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.

April, 2018

Revision History

Date	Document Version	Description of Release
04/23/2018	3.0	Document published for V8 SP2 GA
01/17/2018	2.0	Document published for V8 SP1 GA • Added a note under the Creating a New Enterprise App > Step 1 : App Basics section • Added a note under the Devices 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	Document published for V8 GA • Renaming Enterprise Store Android Binary • Enterprise Store • Device Enrollment • Active Directory and Kony Fabric Identity Users Unlock. • Application Settings > Usage Settings • Users page • App Ratings and App Downloads Report • Enterprise Wipe Enhancements • Search/Filter apps with categories • Enterprise Apps • Self-service Console Apps • Event Log

Date	Document Version	Description of Release
04/23/2018	3.0	Document published for V8 SP2 GA

Date	Document Version	Description of Release
12/29/2017	2.0	Document published for V8 SP1 GA • 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	Document published for V8 GA • Renaming Enterprise Store Android Binary ◦ Enterprise Store ◦ Device Enrollment • Active Directory and Kony Fabric Identity Users Unlock. ◦ Application Settings > Usage Settings ◦ Users page • App Ratings and App Downloads Report • Enterprise Wipe Enhancements • Search/Filter apps with categories ◦ Enterprise Apps ◦ Self-service Console Apps • Default Groups • Default Device Sets • Default Polcies

Table of Contents

1. Introduction

Kony Management Suite's Enterprise mobility management (EMM) software is a policy configuration and management tool for mobile handheld devices and corresponding applications on smartphones and tablets. EMM helps enterprises to manage complex communications between mobile devices by supporting security, network services, and software and hardware management across multiple OS platforms. EMM also supports bring your own device (BYOD) initiatives that has become the focus of many enterprises. It can support corporate and personal devices, and helps to support a more complex and heterogeneous environment.

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

The following is a scenario in which the Kony EMM approaches and handles the problem:

To manage any device, it must be enrolled. The management can choose to manage only a few employee devices or all of them. The employee database can be imported from enterprise systems like Microsoft Active Directory. Once it is enrolled successfully, the EMM Administrator has complete control over the devices.

These devices are grouped together into Device Sets based on rules. Device Sets are usually dynamic, which means all the devices satisfying the rules are part of the set. Device Sets can be created on the basis of several Attribute Types including its location, ownership, OS, hardware, apps installed and many more. To keep the devices in check, device policies are created, which are applied to the device sets. These device policies and settings cover the entire scope of a device functionality. For example, enforcing a passcode policy, removing camera access at certain locations.

A device may belong to multiple groups and hence it can have several policies applicable to it. But, only one policy should be applied to a device. To resolve this, each policy has a Priority associated with it. The policy with highest priority is loaded first on the device. As part of the policy, the administrator also defines Compliance Actions. If devices do not comply with the rules, the administrator can perform the required action. The administrator can prescribe a set of actions such as, sending alerts to administrator and/or the user, Blocking Email, Resetting Passcode, Locking Device, Enterprise Wipe, and a Complete Wipe. Once returning to a compliant state, the EMM server automatically restores the settings and access the device as per the policy is applied.

Similarly, aapplication level policies can also be applied to users and groups. These differ from device level policies because they apply at the application level. 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.

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 Device Management (MDM), 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`	- User input text, system prompts and responses - File path - Commands - Program code - File names
Italic	- Emphasis - Names of books and documents - New terminology
Bold	- Windows - Menus - Buttons - Icons - Fields - Tabs - Folders
URL	Active link to a URL.
Note	Provides helpful hints or additional information.
Important	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 enrollment 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.

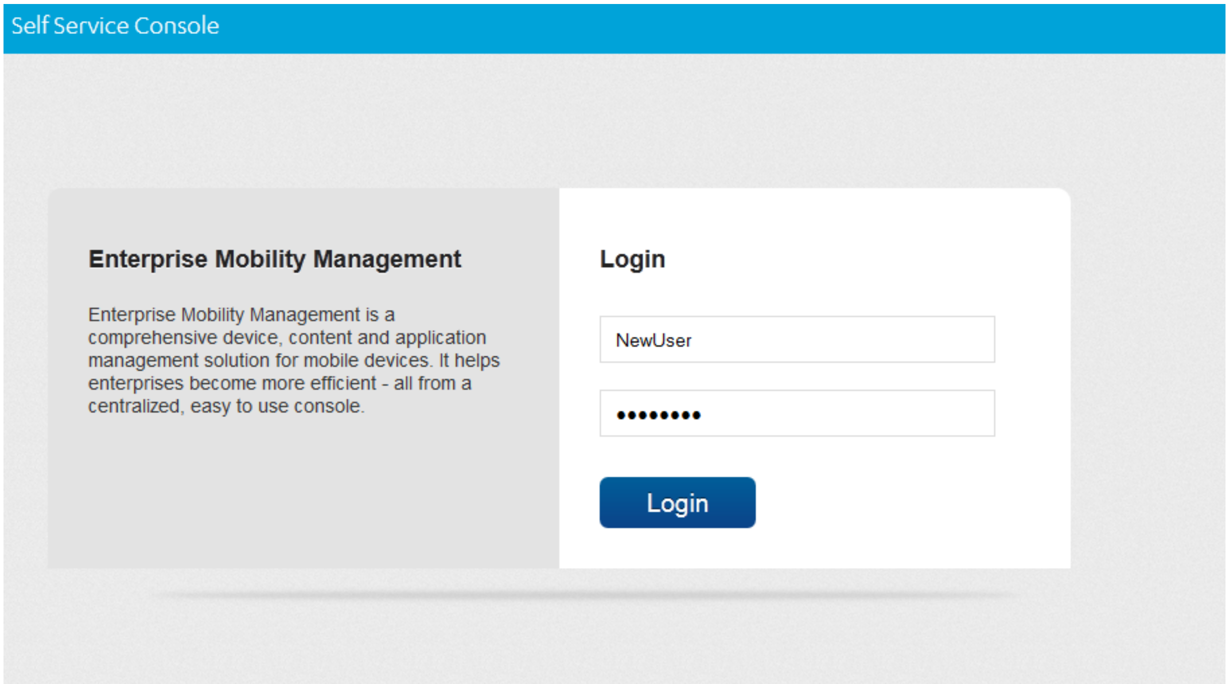
Scenario	If			User need to provide authentication details as follows:
	AD 1	AD 2	Local Directory	
1	YES	NO	NO	**Username and password**: Authentication should directly happen.
2	YES	YES	NO	**Username, password, domain**: Because there are users from different domains, this resolution is necessary. Only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

Enterprise Mobility Management

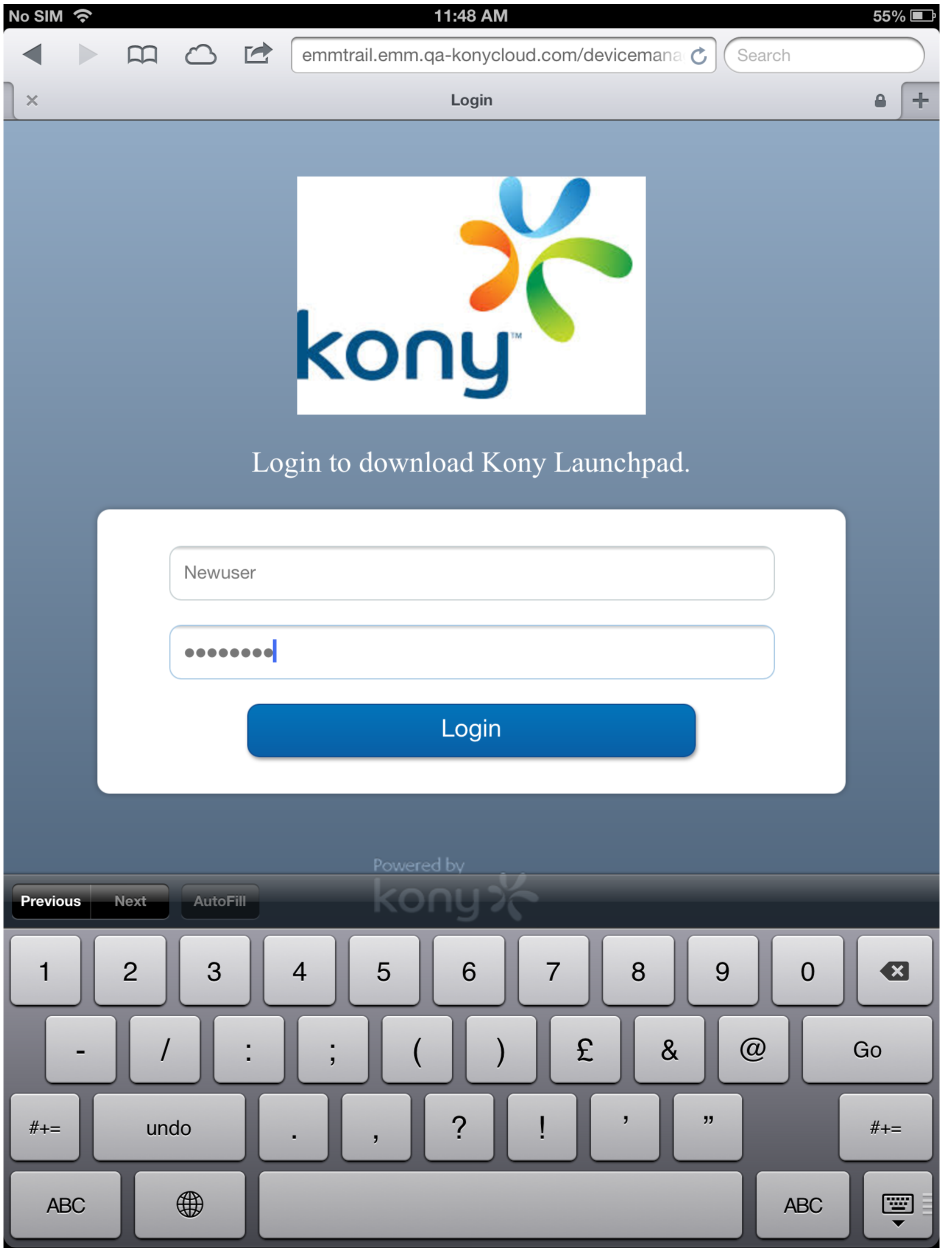
Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

NewUser

••••••••

2.1.2 Device download (device side)

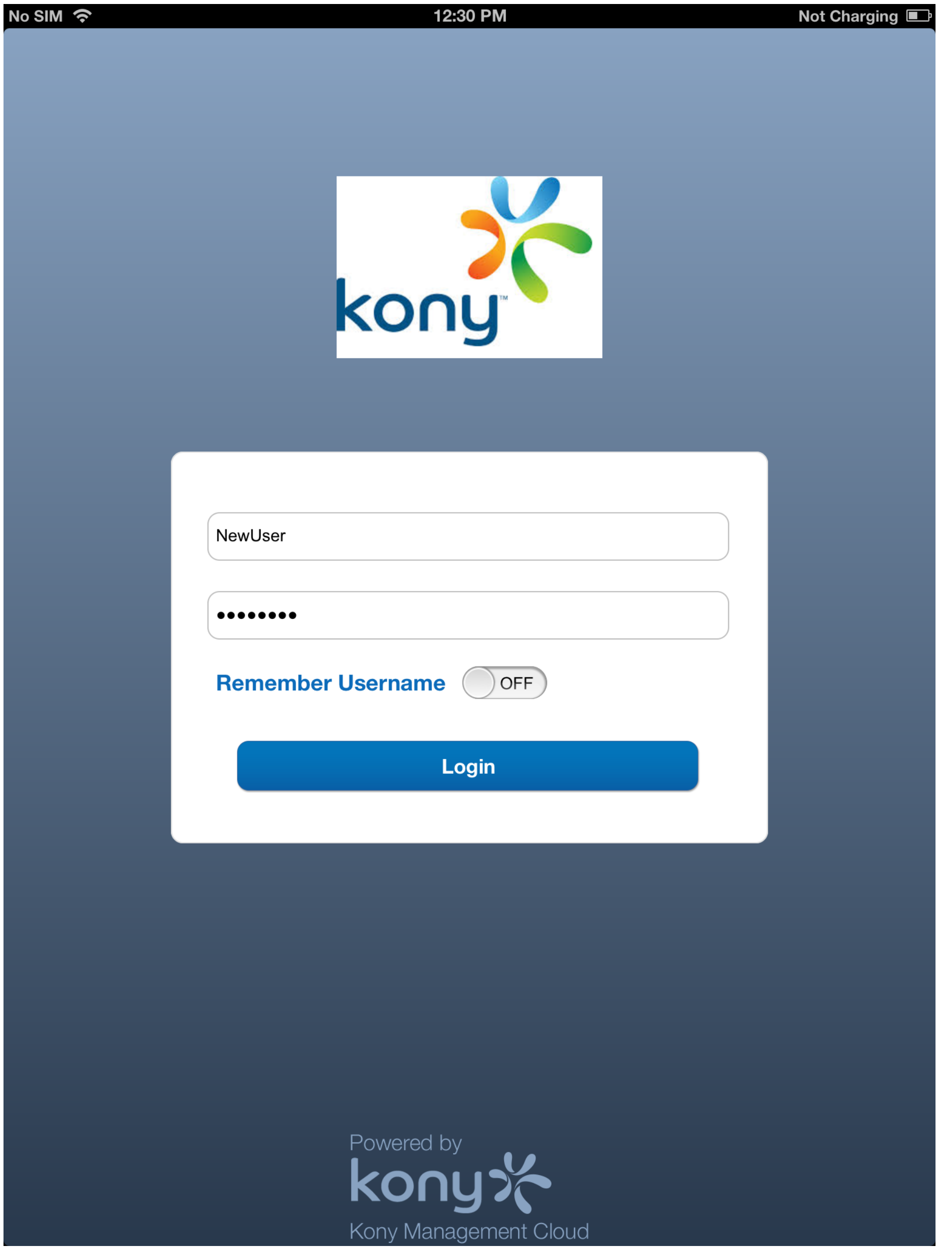


Login to download Kony Launchpad.

Newuser

••••••••

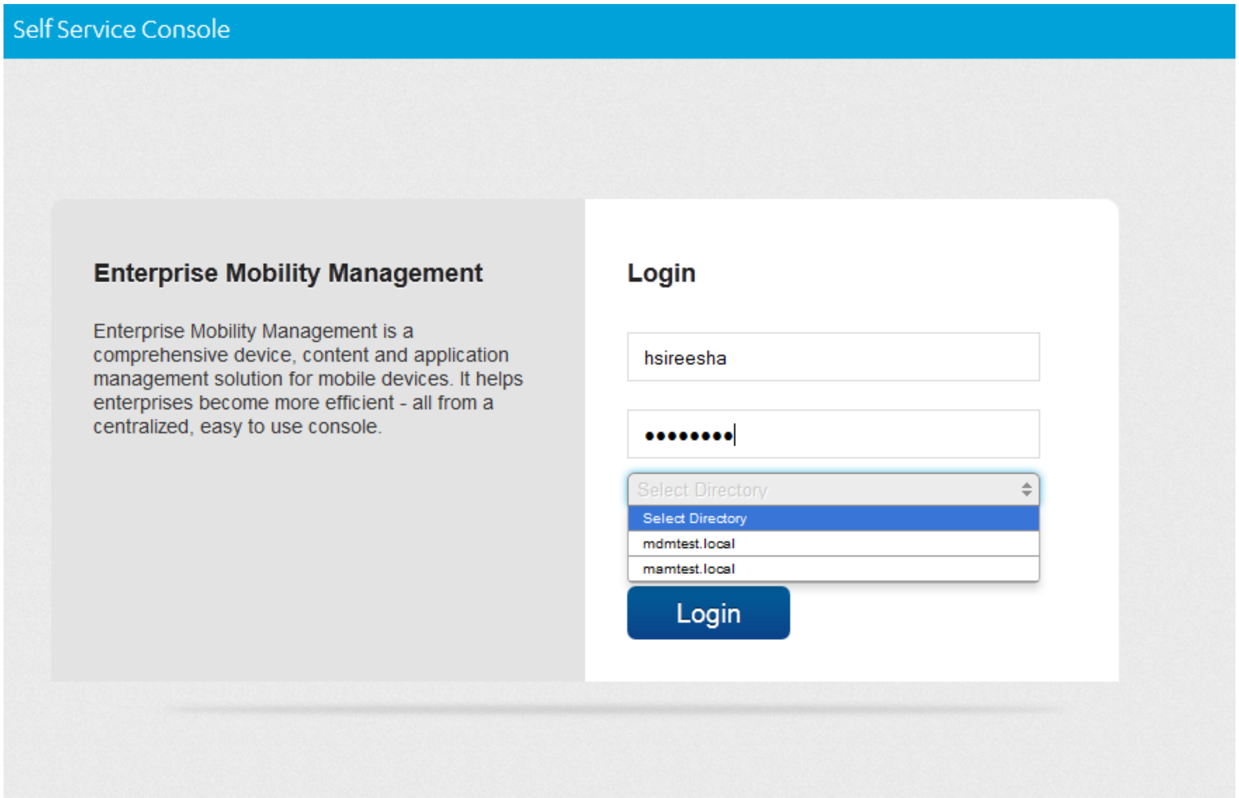
2.1.3 Device log in (device side)



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

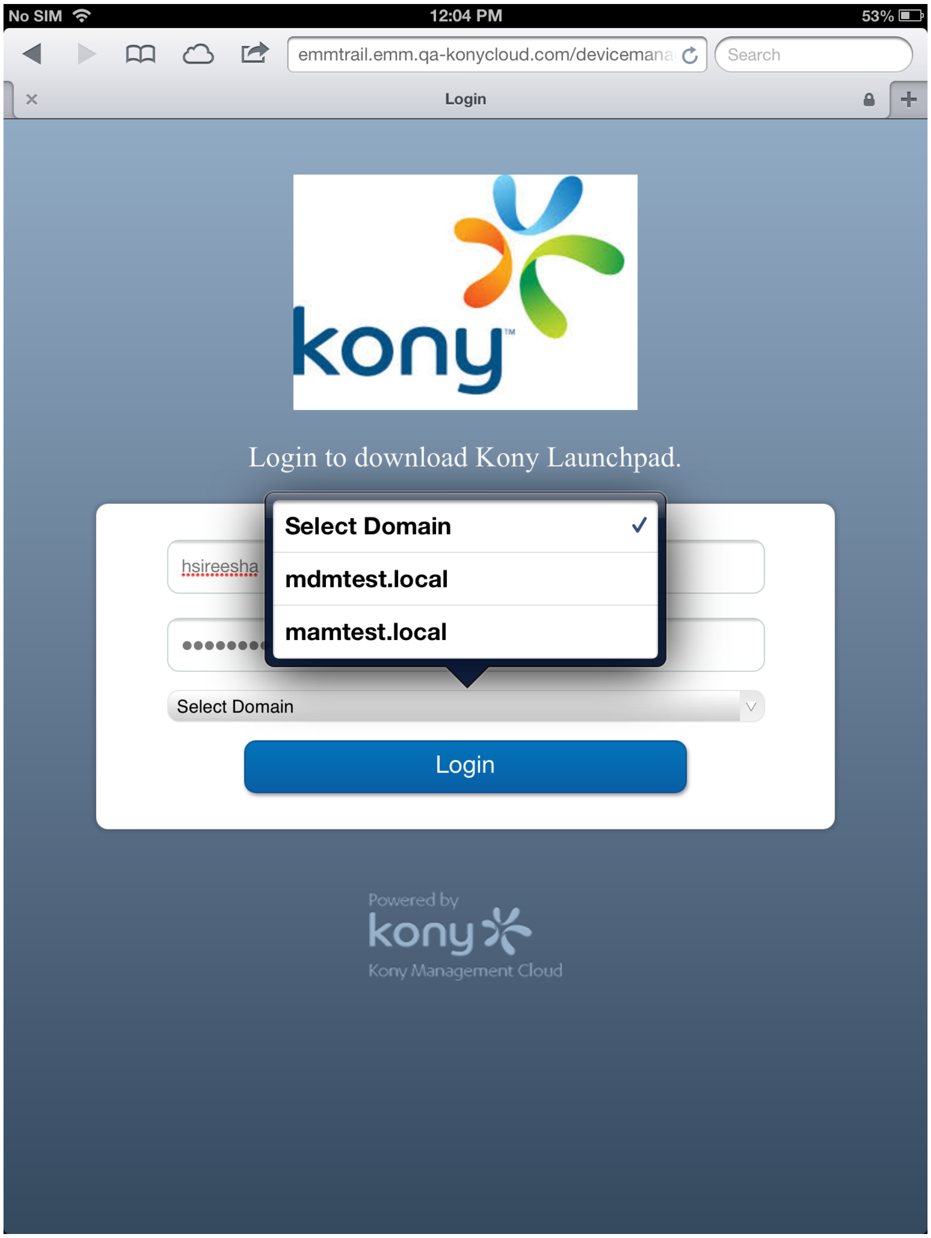
hsireesha

••••••••

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.

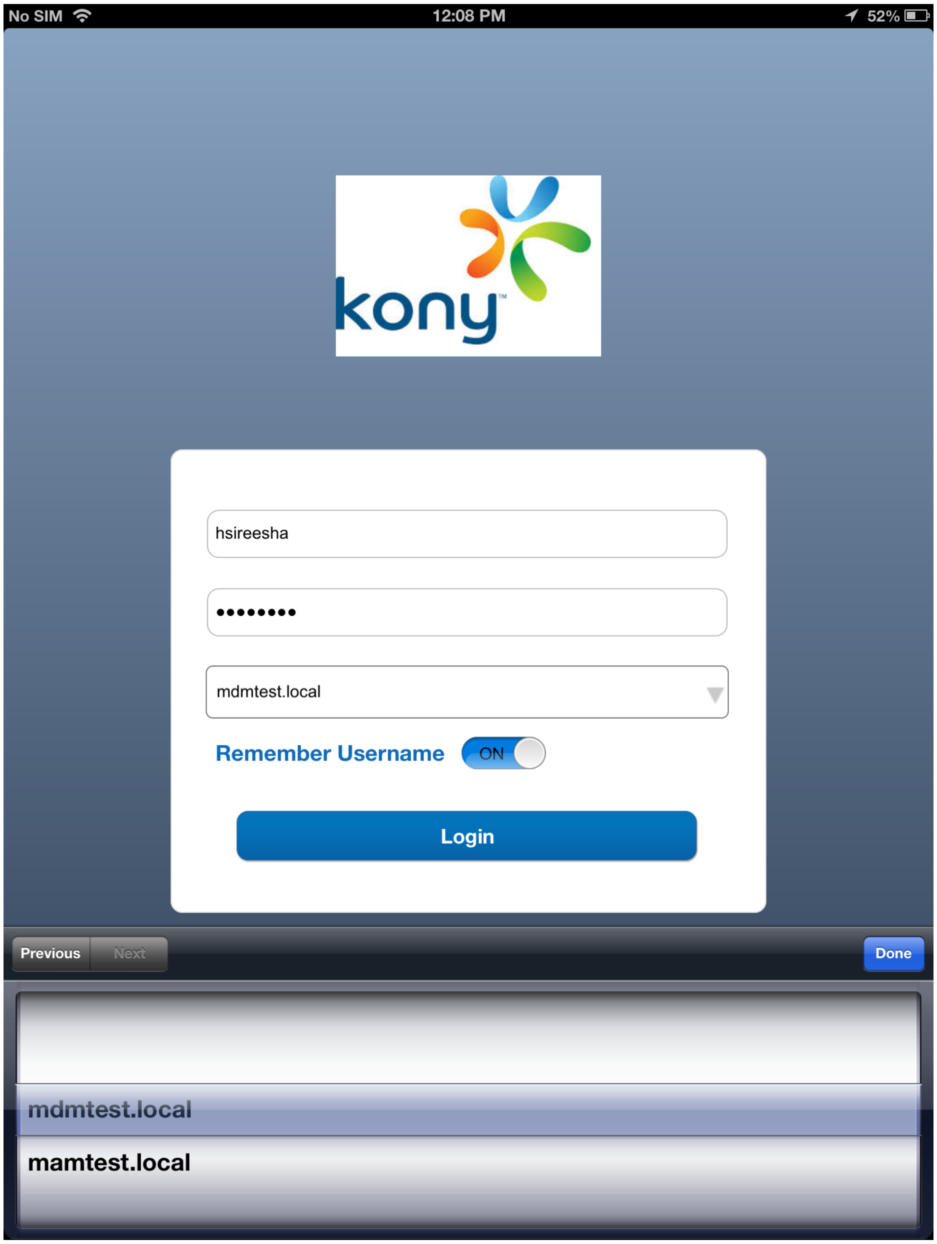
If a user does not choose the remember me option, these fields will be blank the next time the page is loaded in the browser. Only the username and password fields will be displayed.

2.2.2 Device download (device side)



Login to download Kony Launchpad.

2.2.3 Device log in (device side)



No SIM 12:08 PM 52%

hsireesha

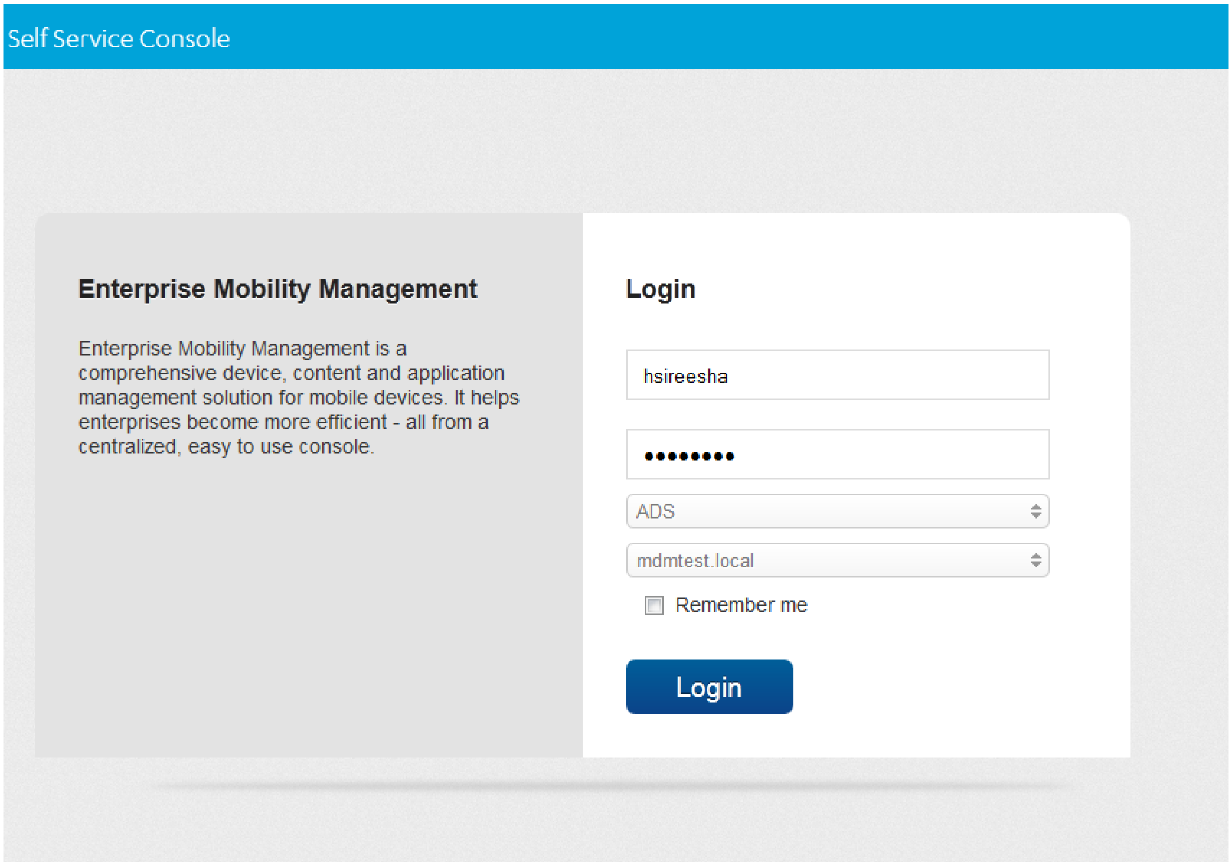
••••••••

mdmtest.local

Remember Username ON

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.



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

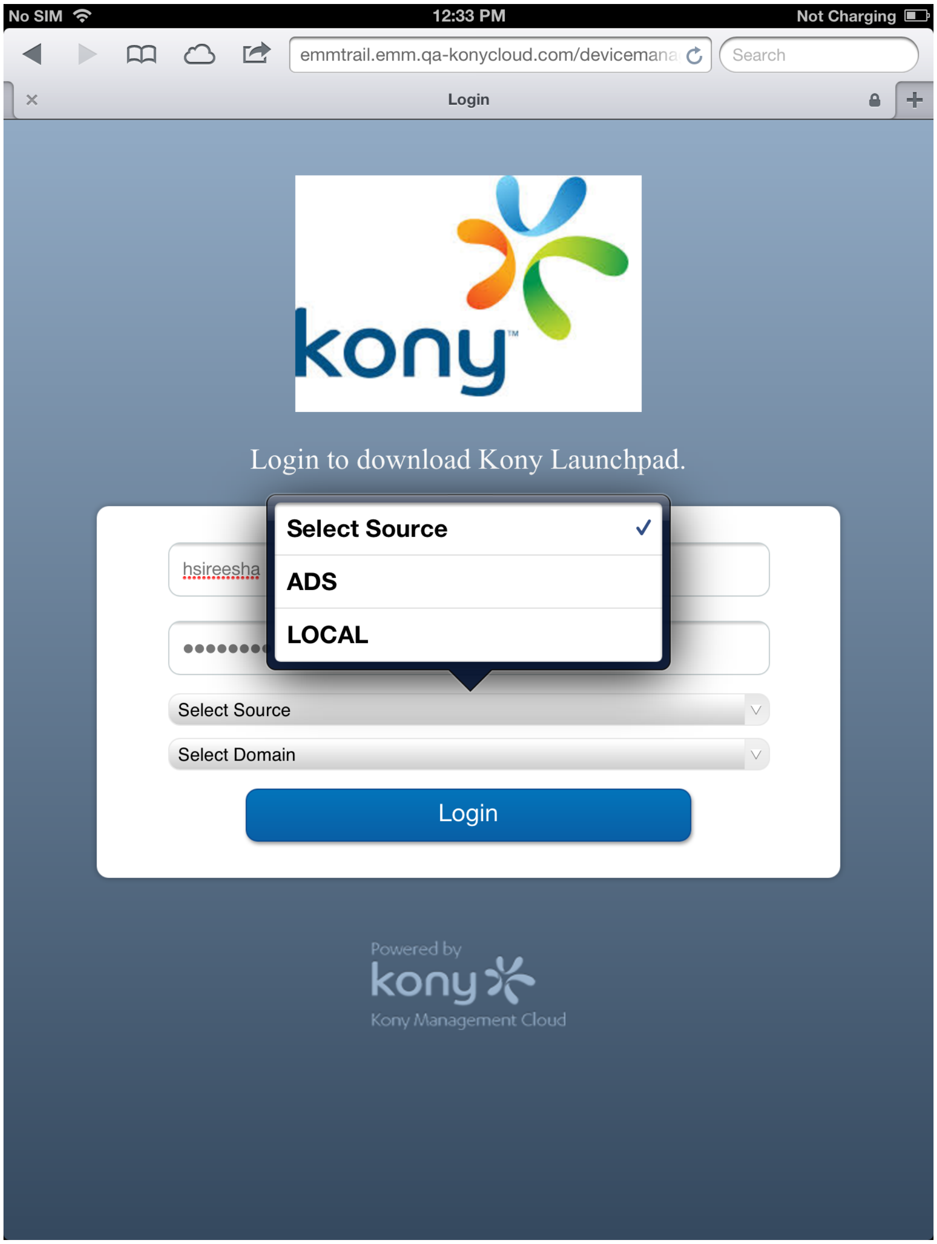
••••••••

ADS

mdmtest.local

☐ Remember me

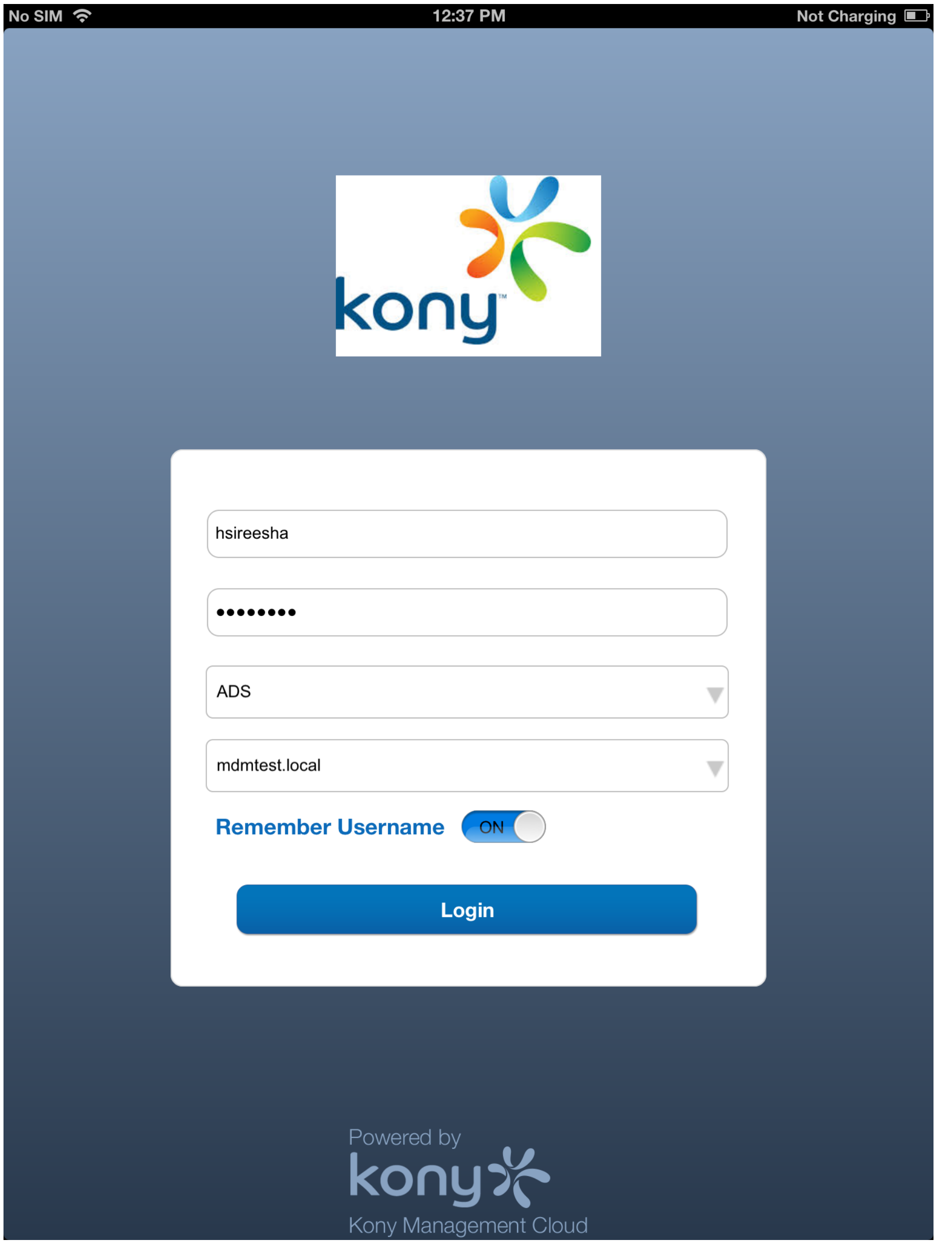
2.3.1 Device download (device side)



Login to download Kony Launchpad.

hsireesha

2.3.2 Device log in (device side)



No SIM 12:37 PM Not Charging

hsireesha

••••••••

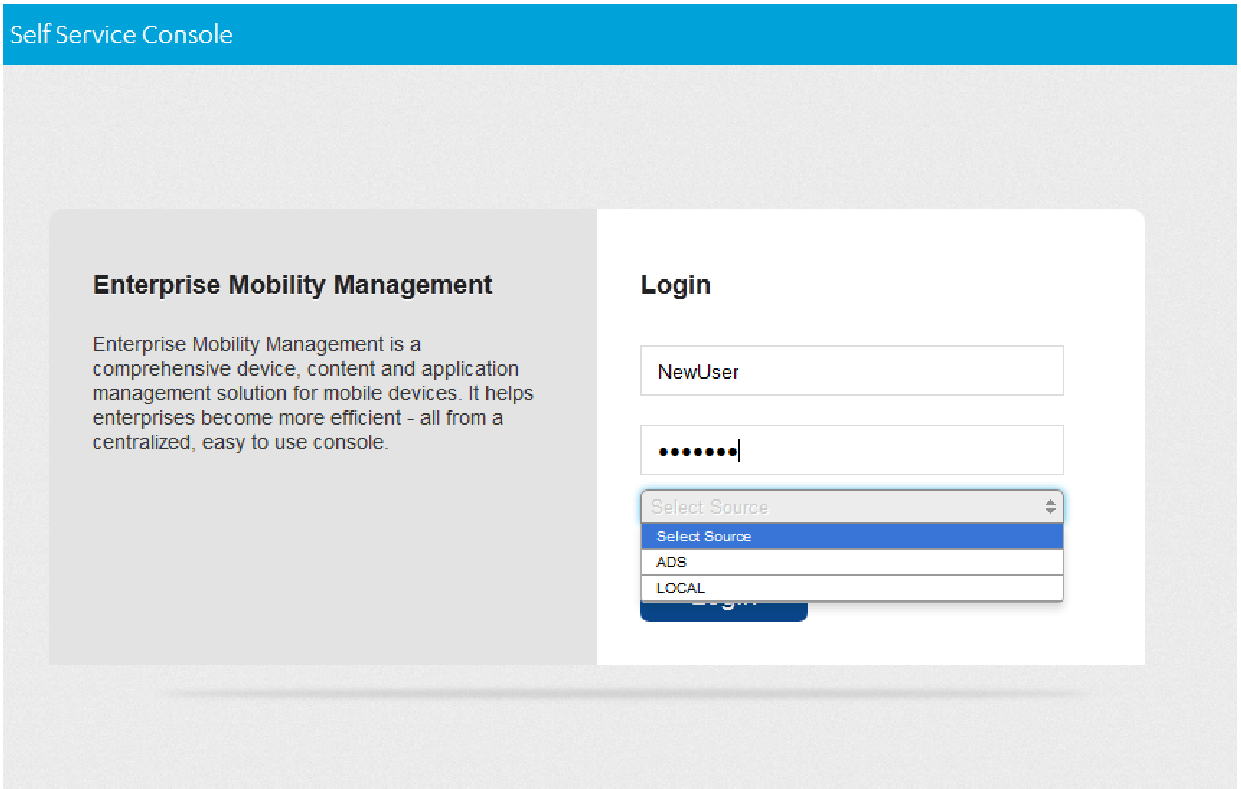
ADS

mdmtest.local

Remember Username: ON

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

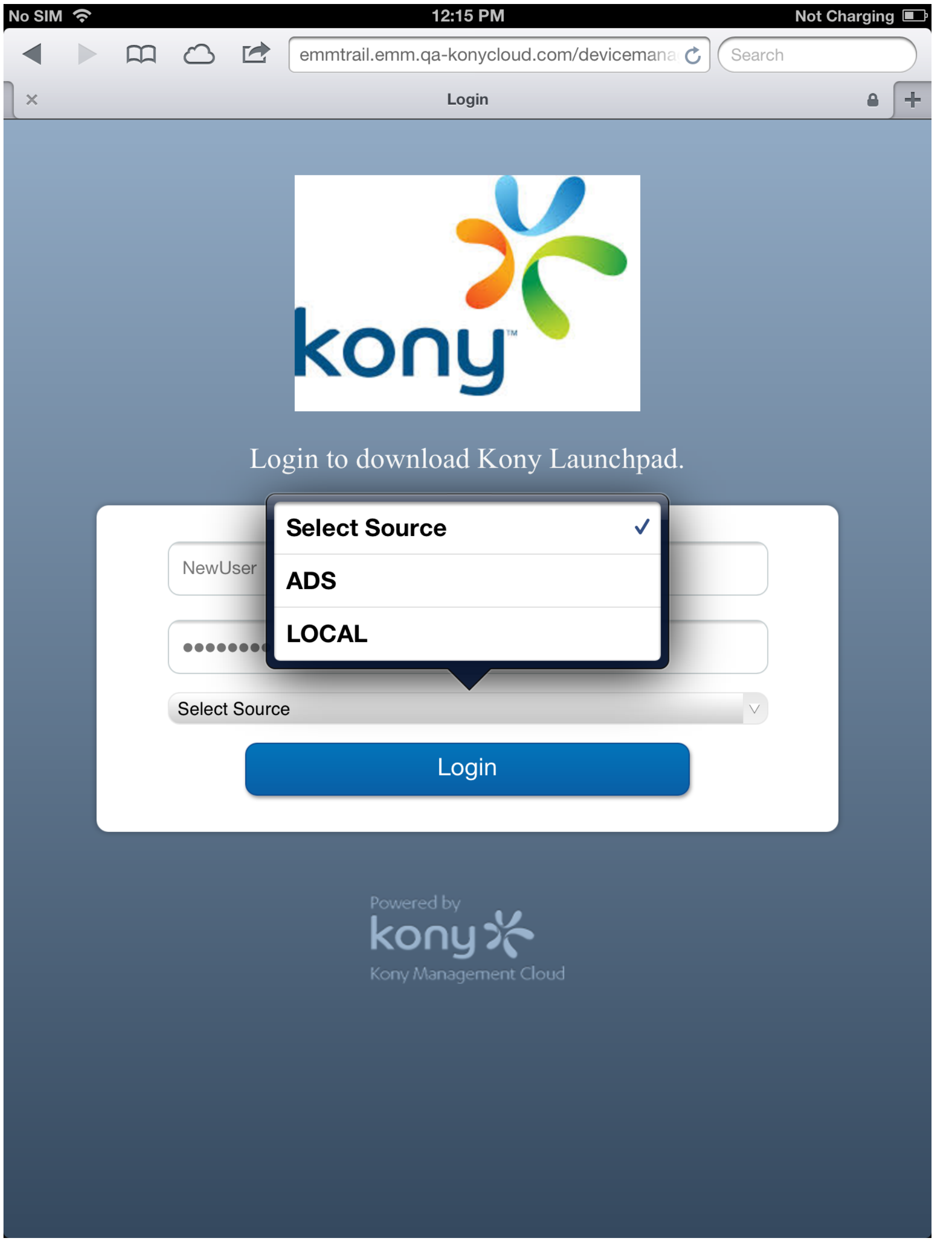
Enterprise Mobility Management is a comprehensive device, content and application management solution for mobile devices. It helps enterprises become more efficient - all from a centralized, easy to use console.

Login

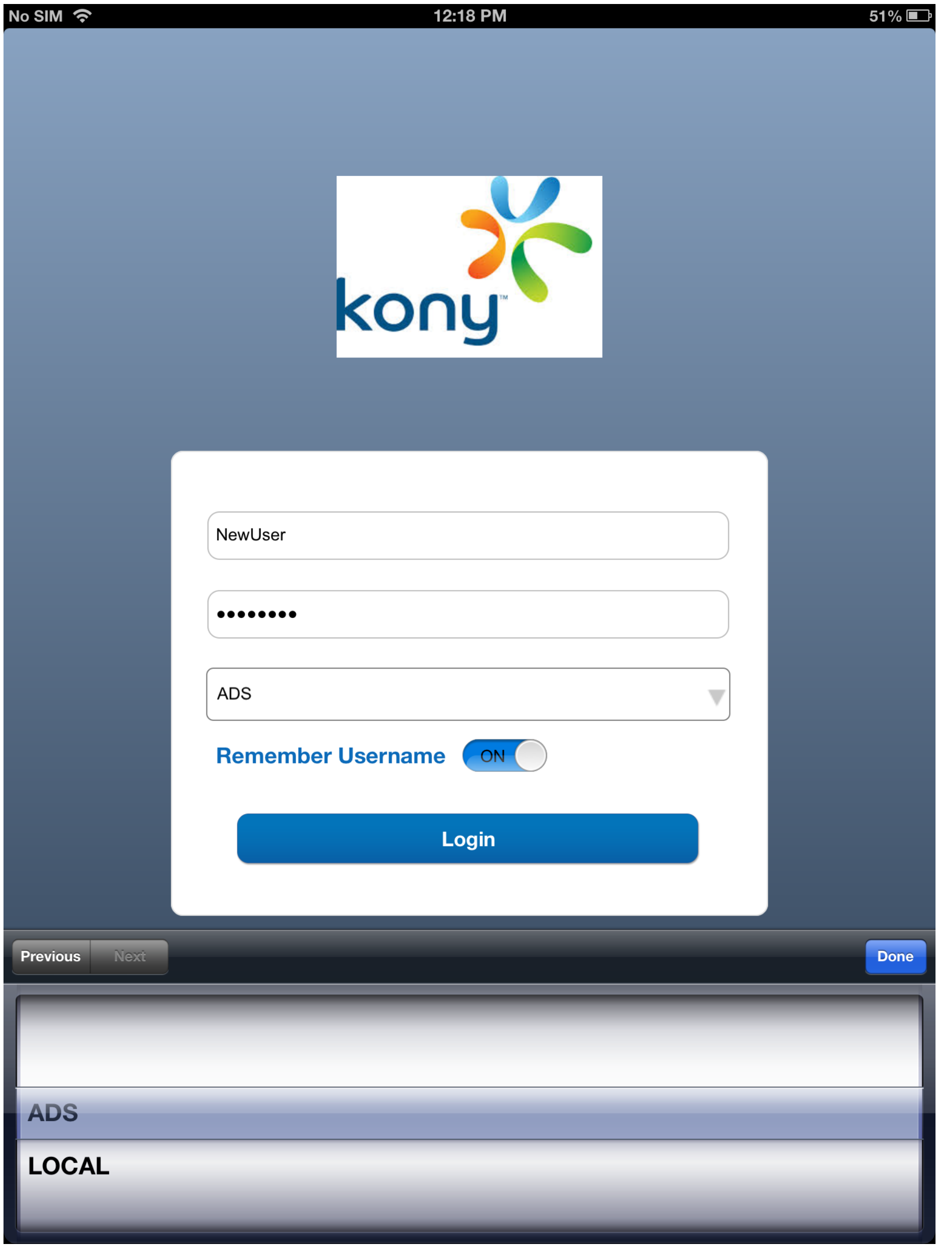
NewUser

•••••••

2.4.1 Device download (device side)



2.4.2 Device log in (device side)



No SIM 12:18 PM 51%

NewUser

••••••••

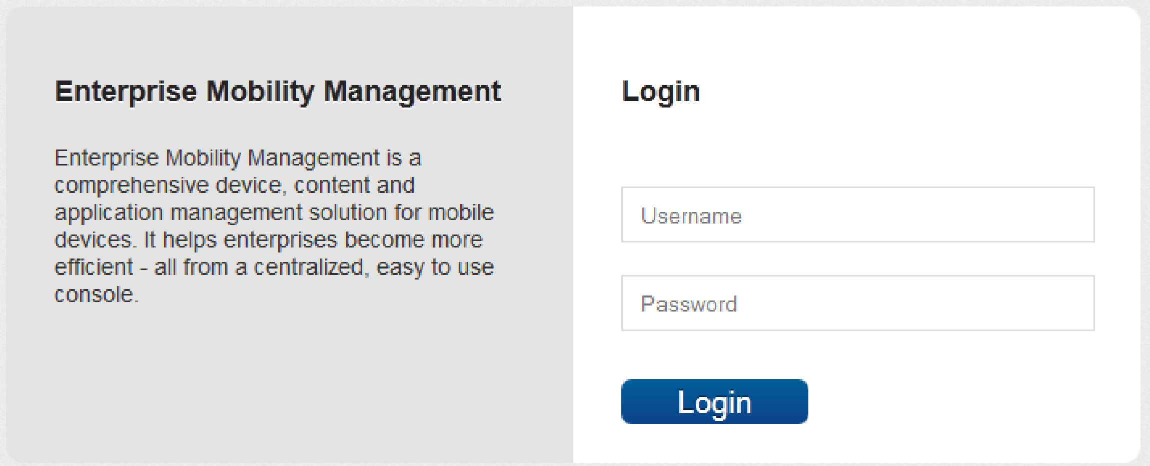
ADS

Remember Username ON

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.

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.

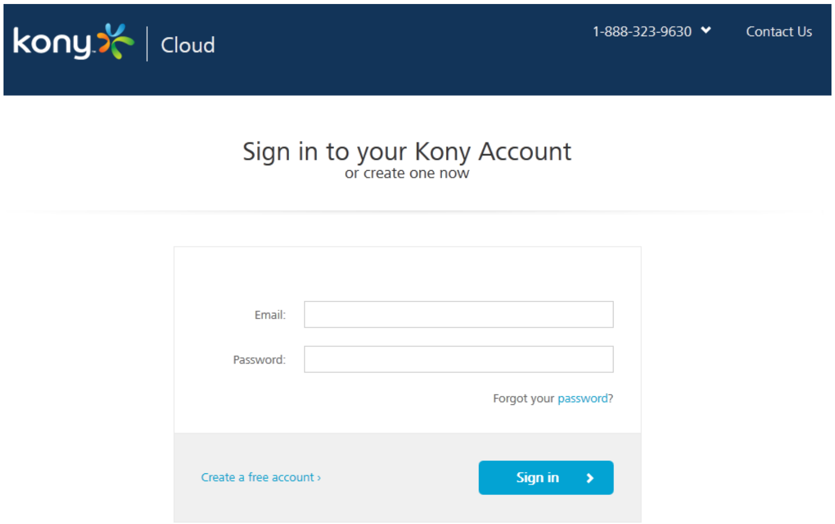
> ***Note:*** It is recommended that the same User should not log in from multiple browsers or computers. Modifying the same page simultaneously may result into an unexpected behavior.

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 authentications or source. Custom Authentication feature provides additional flexibility to you to have all authentication to 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, synching 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. Exchange Settings
6. Enterprise Resources
7. Branding
8. Geo and Time Fence List
9. Event Log
10. System Status
11. 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 enrolling 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 only third party sources 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.

Column	Description
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 ❗	Displays the number of users and groups imported from the Active Directory when you click on the information icon. If no users or groups are imported from a Directory, the information icon turns into a check box. If you want to delete an Active Directory, you must select the desired check box and then click the **Delete** button.
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:

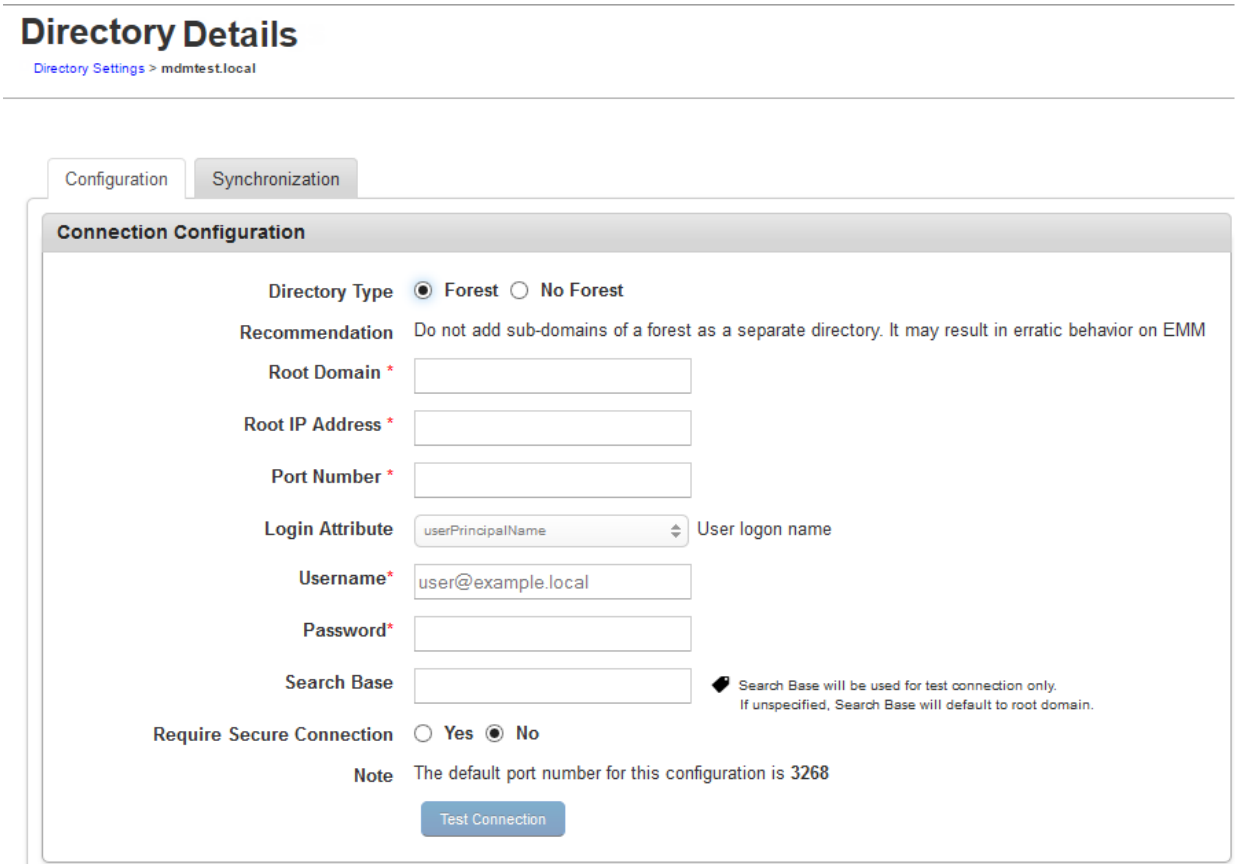
- Configuring Active Directory
- Configuring an AD with a Secured VPN for Management Cloud
- Searching and Filtering Active Directory
- Viewing Number of Users/Groups Imported from AD

- 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

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 userPrincipalName User logon name

Username* user@example.local

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:

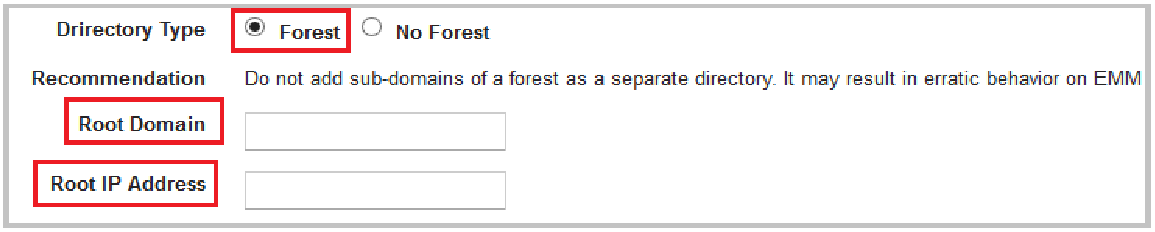
- Forest
- No Forest

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.

   Drirectory 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

   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 form 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

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

   Save status message appears.
7. Click **OK** to return to the main page.

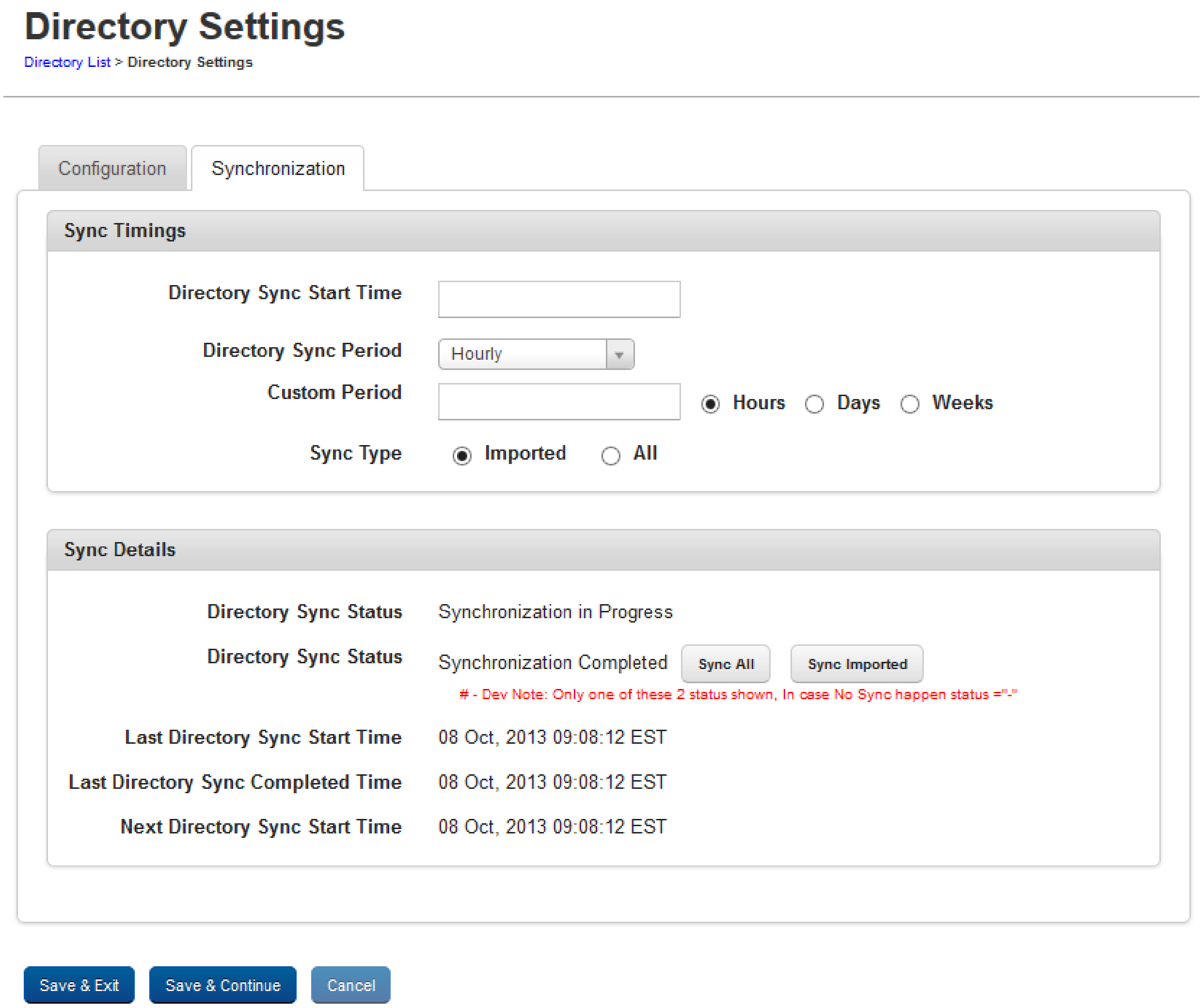
> *Important:* In this application, wherever passwords need to be provided, some browsers may ask to Remember Password. Opt for Never as it is irrelevant. Your enterprise passwords should not be remembered

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

Sync Timings

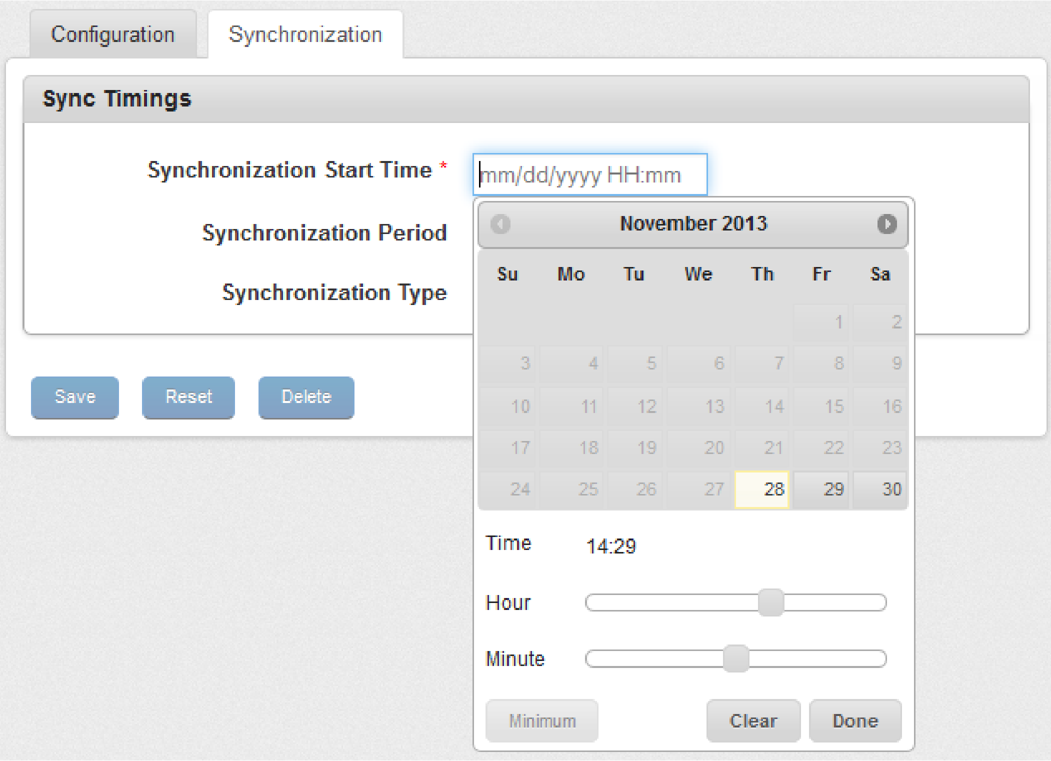
Directory Sync Start Time	
Directory Sync Period	Hourly
Custom Period	● Hours ○ Days ○ Weeks
Sync Type	● Imported ○ All

Sync Details

Directory Sync Status	Synchronization in Progress
Directory Sync Status	Synchronization Completed
	# - Dev Note: Only one of these 2 status shown, In case No Sync happen status ="-"
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:

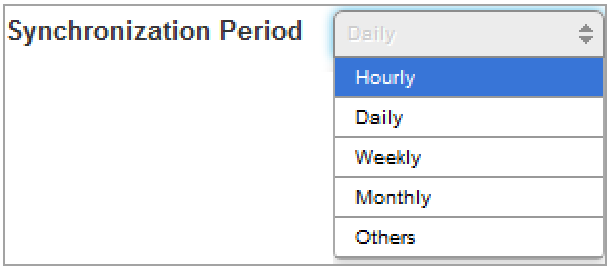
1. **Synchronization Start Time**: Place cursor in **Synchronization Start Time** field.



The Calendar appears.

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

   The selected Date and Time appears in the field.



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 enrolled 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
Created By: ▪ Admin 1 ▪ Admin 2 ▪ Admin 3	The server only displays those directories (rows) that have the filtered entity. • For example, if the directory name is Orlando AD, then all directories named Orlando AD are shown regardless of domains. Filters can be applied for one or more columns. If filters are applied across multiple columns, the system performs AND condition between all filters. • For example, if directory name is Orlando AD and Created By is Mike, then all directories created by Mike are shown.
Created On: ▪ Today ▪ Yesterday ▪ Last 7 days ▪ Last 10 days ▪ Last 30 days ▪ More than 30 days	You can specify dates and time with the Created On filters. The filters represent data based on the following: • 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. 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. All the above ranges are non-overlapping and ensures that no results are double counted.

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.

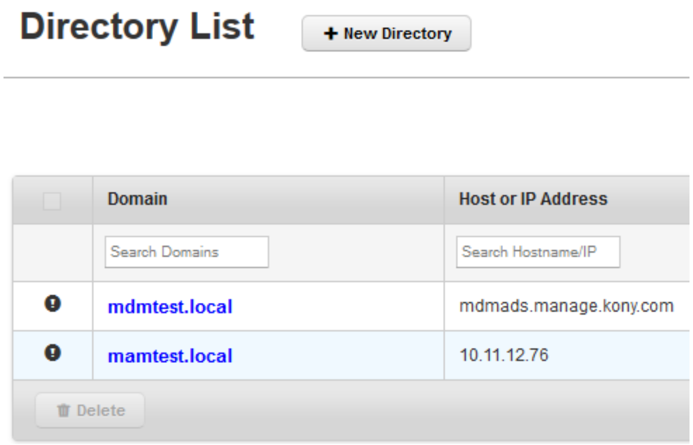
To view the details, click the information icon next to Domain column. The system displays the details of users and groups imported from the AD.

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

□	Domain	Host or IP Address
	Search Domains	Search Hostname/IP
❗	mdmtest.local	mdmads.manage.kony.com
❗	mamtest.local	10.11.12.76

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.

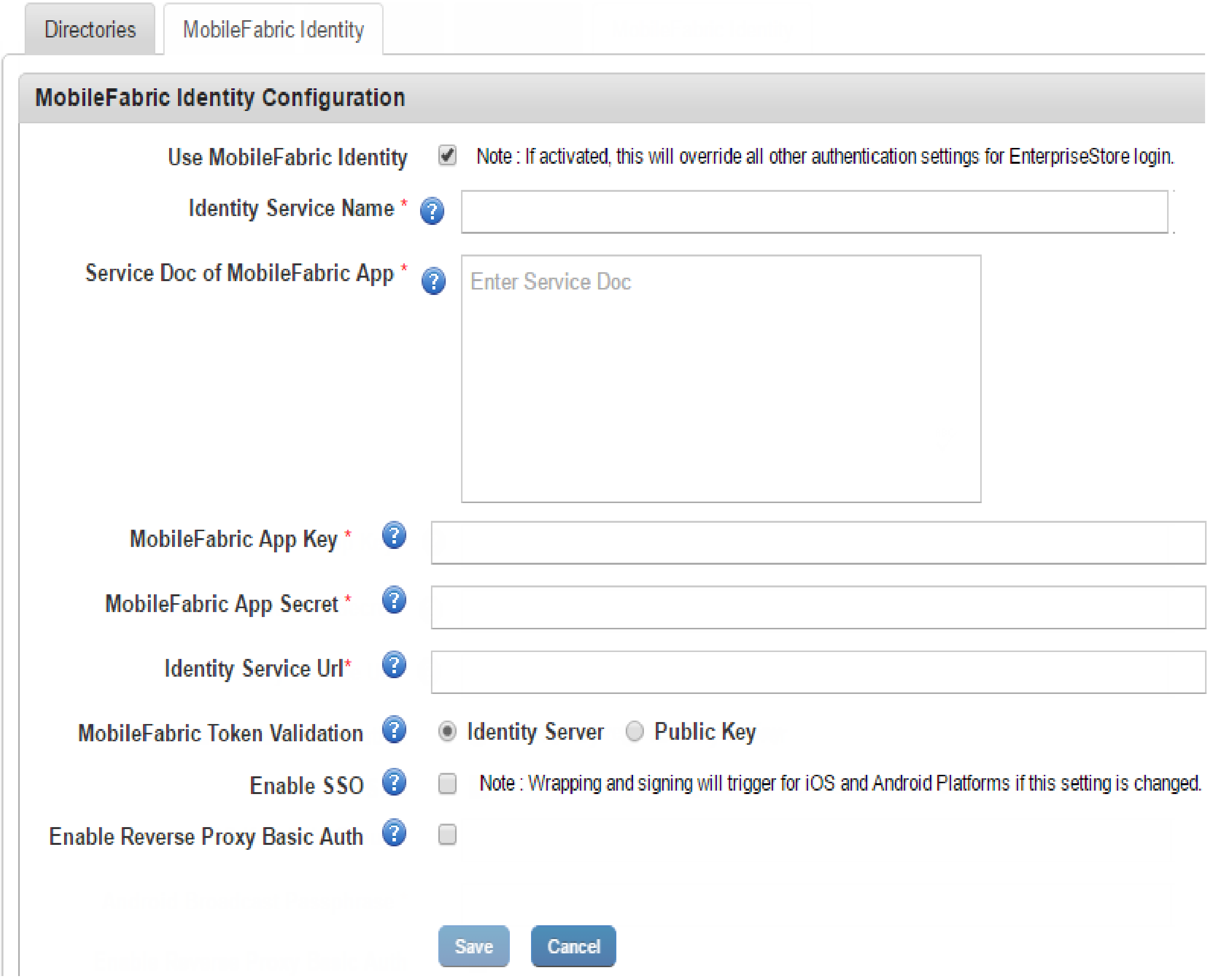
- EMM Management Console
- EMM Self Service Console

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
Identity Service Name *
Service Doc of MobileFabric App *
Enter Service Doc
MobileFabric App Key *
MobileFabric App Secret *
Identity Service Url*
MobileFabric Token Validation
Identity Server
Public Key
Enable SSO
Enable Reverse Proxy Basic Auth
Save
Cancel

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

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**.

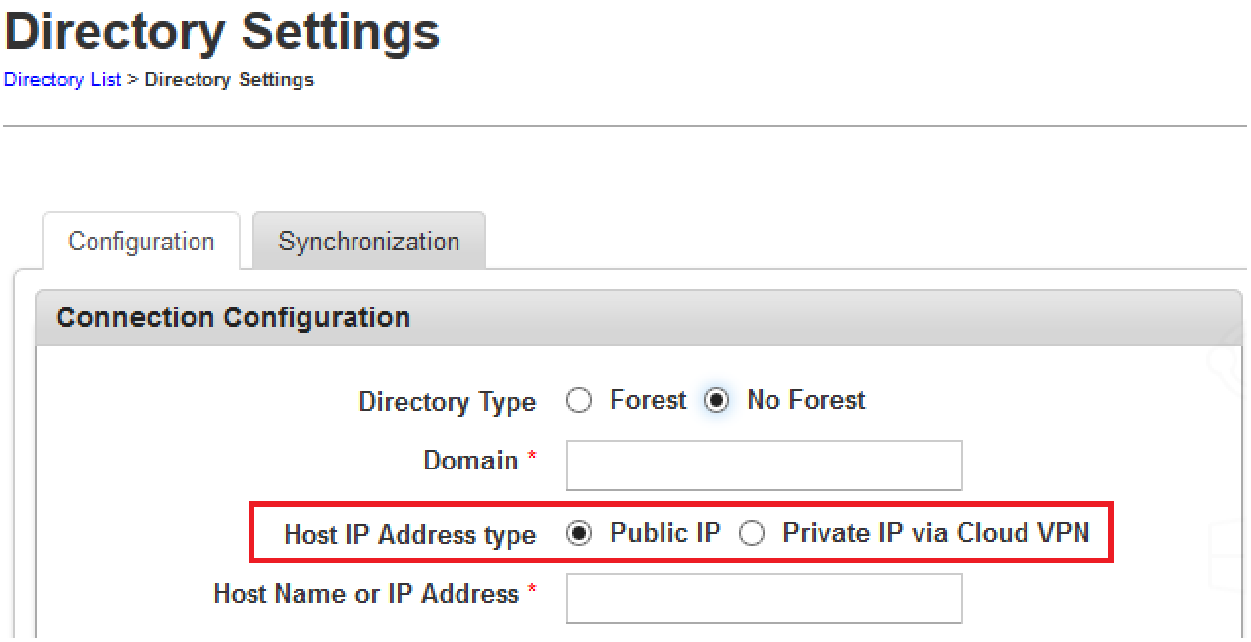
For more information on Kony Fabric Identity service, click here.

For more information on Kony Fabric Identity App Key, App secret, and Service Doc, click here.

6.1.4.2 Configuring an AD With a Secured VPN for Management Cloud

Kony Management offers secure VPN connectivity between Management Cloud and a your Enterprise data center, so that you can connect EMM to an active directory. This ensures that all communications between Management Cloud and an AD are secure.

> *Important:* The **Host IP Address type** option is available only for Management Cloud.



Directory Settings

Directory List > Directory Settings

Connection Configuration

Directory Type ○ Forest ● No Forest

Domain *

Host IP Address type ● Public IP ○ Private IP via Cloud VPN

Host Name or IP Address *

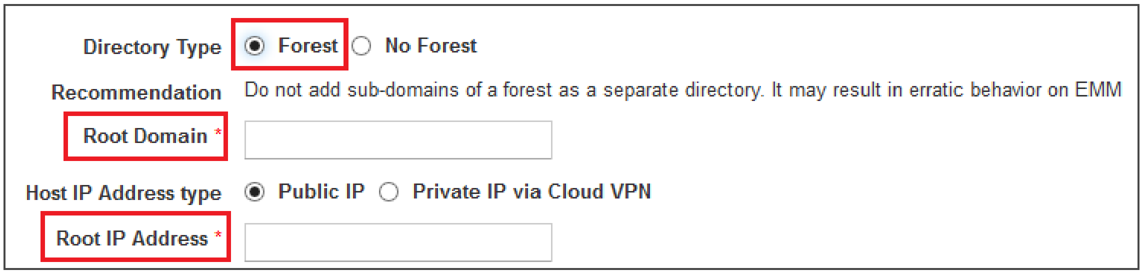
Configuration

You can configure a secured VPN by selecting the **Host IP Address type** as **Private IP via Cloud VPN**.

To configure an AD with secured VPN for could only, follow these steps:

1. Select the **Directory Type**. By default this is set to **No Forest**. You can modify it to **Forest**, as shown below.

The system displays the **Root Domain** and the **Root IP Address** fields. The **Host IP Address type** option is available for both Forest or No Forest Management Cloud.



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 *	
Host IP Address type	● Public IP ○ Private IP via Cloud VPN
Root IP Address *	

2. Type the required domain details.

> *Important:* Do not add sub-domains of a Forest as a separate directory. Such action could result in erratic behavior while synchronizing Users and Groups, if common Users and Groups are found.

For example, if directory type is **Forest AD**, follow these steps:

a. **Root Domain**: Enter the Root Domain name of the Forest AD.

b. **Host IP Address type**: By default this option is set to Public IP. Select one of the following options.

   - **Public IP**: A public IP address accessible directly on the Internet.
   - **Private IP via Cloud VPN**: A private IP address that is accessible only via a VPN connection. IP addresses accessible via a VPN are always within the private IP address range.

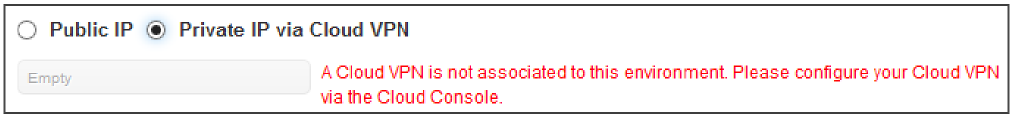
c. **Root Host Name or IP Address**:

   - If you select the option **Public IP** as Host IP Address type, enter a public IP address.

- If you select the option **Private IP via Cloud VPN** as Host IP Address type, only then the **Root IP Address** text field turns into a drop-down list contains Cloud VPNs that are associated to this environment. Select one of the IP addresses from the drop-down list.

  If no VPNs are configured, the system displays the following message:

  A Cloud VPN is not associated to this environment. Please configure your Cloud VPN via the Cloud Console

  ○ Public IP ● Private IP via Cloud VPN

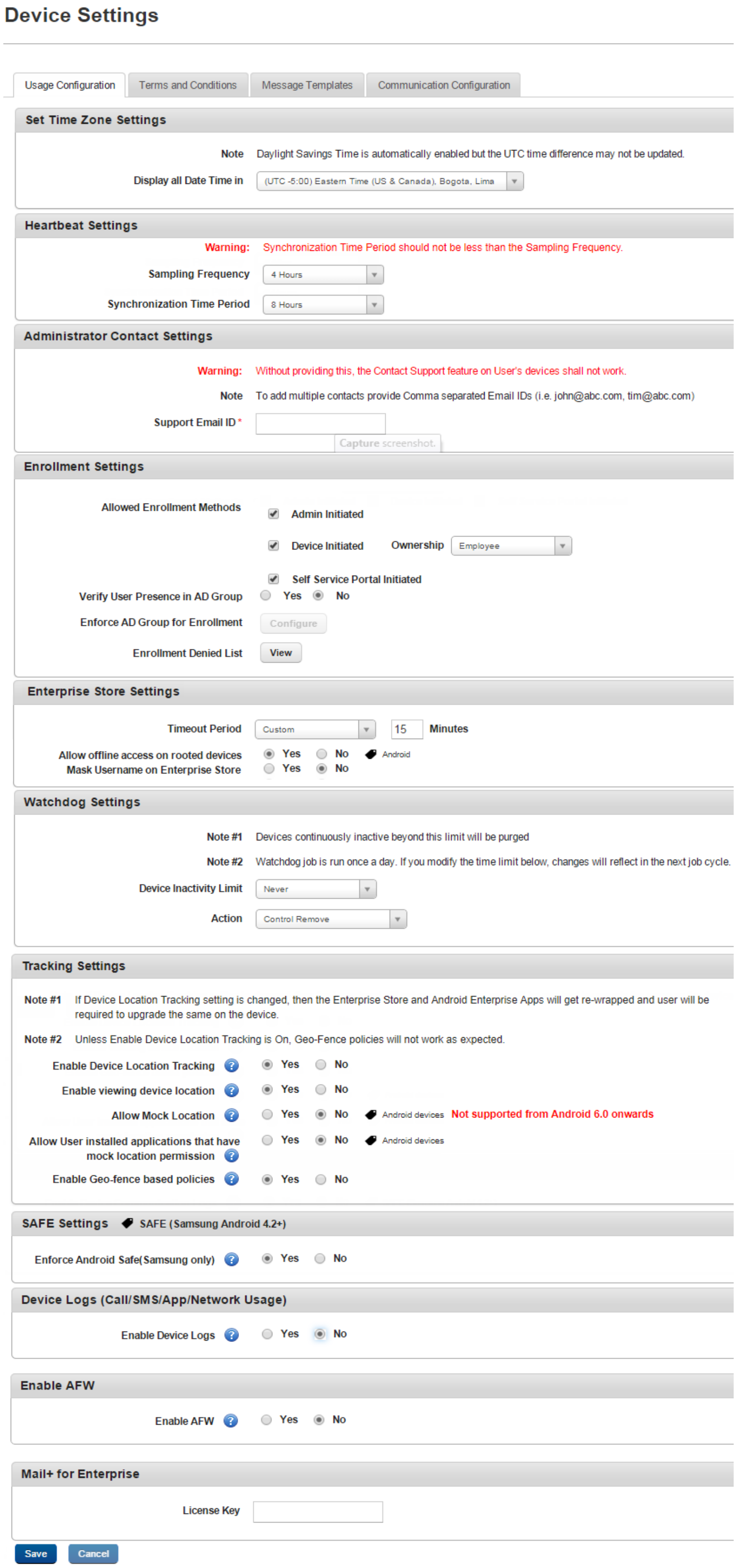
  Empty

  A Cloud VPN is not associated to this environment. Please configure your Cloud VPN via the Cloud Console.

3. Continue Step 4 through Step 7 in the Configuring Active Directory Settings section.

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

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 *

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)

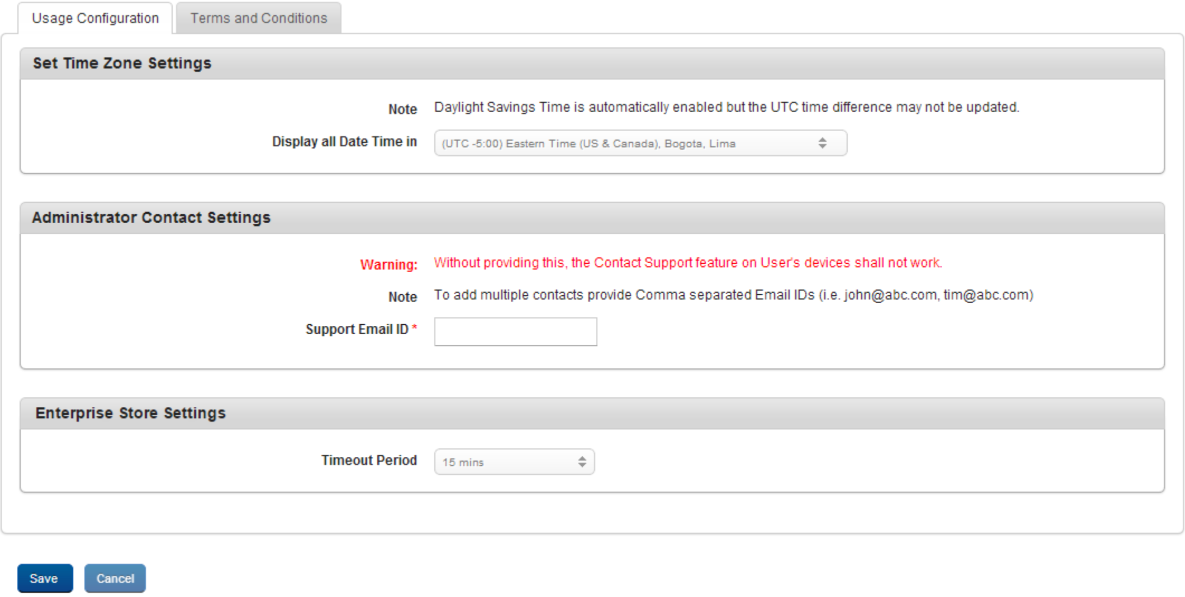
Enable Device Logs ?: ○ Yes ● No

Enable AFW

Enable AFW ?: ○ Yes ● No

Mail+ for Enterprise

License Key



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

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 *

Timeout Period 15 mins

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.

- **Message Templates**: You can use message templates to send messages to an administrator or to the user. Administrators can use messages as is or can edit them. Administrators can build on top of templates to send messages to specific devices or device sets. There are two modes of sending messages - push notifications and email. You can create separate templates for each messaging mode.

- **Communication Configuration**: This feature helps the administrator to create a device certificate to enable managing the device through Enterprise Mobility Management (EMM). Without this certificate, EMM application cannot manage devices. EMM application cannot send any commands such as Lock, Locate, Wipe, and Push profiles to adhere to the rules. Following are the Communication Configurations provided for each device.

Device Settings page is used:

- To set Usage Configuration
- To set Terms and Conditions
- To set Message Template
- To set Communication Configuration

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.
Synchronization Time-Period	To set the time period to sync between device and the EMM server, select the value from the drop-down list. Heartbeat configured in EMM applies only to iOS, Android, Windows 6.x, and Windows Phone 8 devices. *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.
Administrator Contact Settings	
Support Email ID	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.
Enrollment Settings	
Allowed Enrollment Methods	Select the required check boxes to set device enrollment.
Admin initiated	If selected, the Admin can initiate the enrollment process. Single Device enrollment and Bulk Enrollment are allowed. Else they are not.

Feature	Description
Device Initiate	If selected, the device can initiate itself without administrator intervention. Selecting the Device Initiated field will enable the following option: **Ownership**: Using the ownership field, you can globally flag all devices enrolling into EMM. Options are **Corporate**, **Employee**, and **Shared**.
Self Service Portal	If selected, the users can send requests to enroll their devices through the Self Service Portal.
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 Enrollment	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

Feature	Description
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	
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.

Feature	Description
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	
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.

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

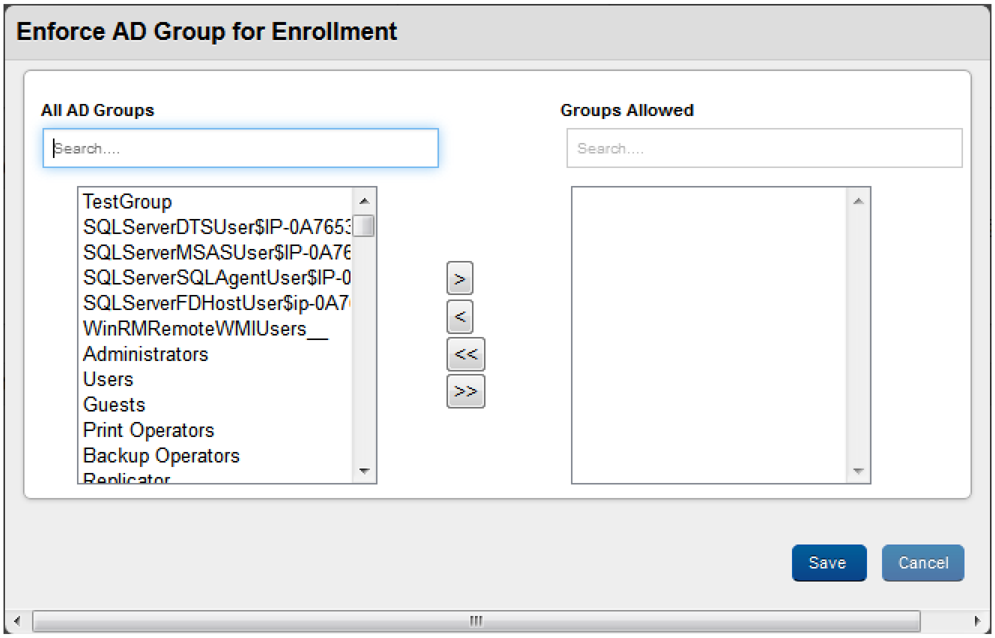
iii. From the drop-down list, select an option. For example, Corporate.

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**.

4. To enforce active directory group for enrollment, click **Configure**. The Enforce AD Group for Enrollment window appears.

5. 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.

6. Once you finish adding your groups, click **Save**. A success message appears.

7. Click **OK**.

8. 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.

9. Click **Save**. A confirmation message appears.

10. 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 date 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.

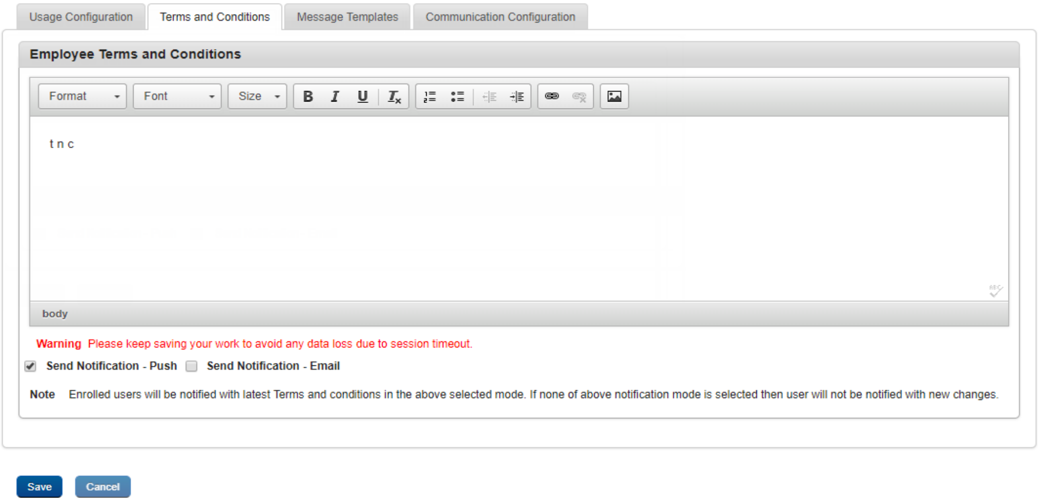
2. Under the **Mail + for Enterprise Device** heading, in the **License key** text box, enter your license key for Mail + for enterprise.

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 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.



Employee Terms and Conditions

t n c

Warning Please keep saving your work to avoid any data loss due to session timeout.

☑ Send Notification - Push ☐ Send Notification - Email

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.

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.

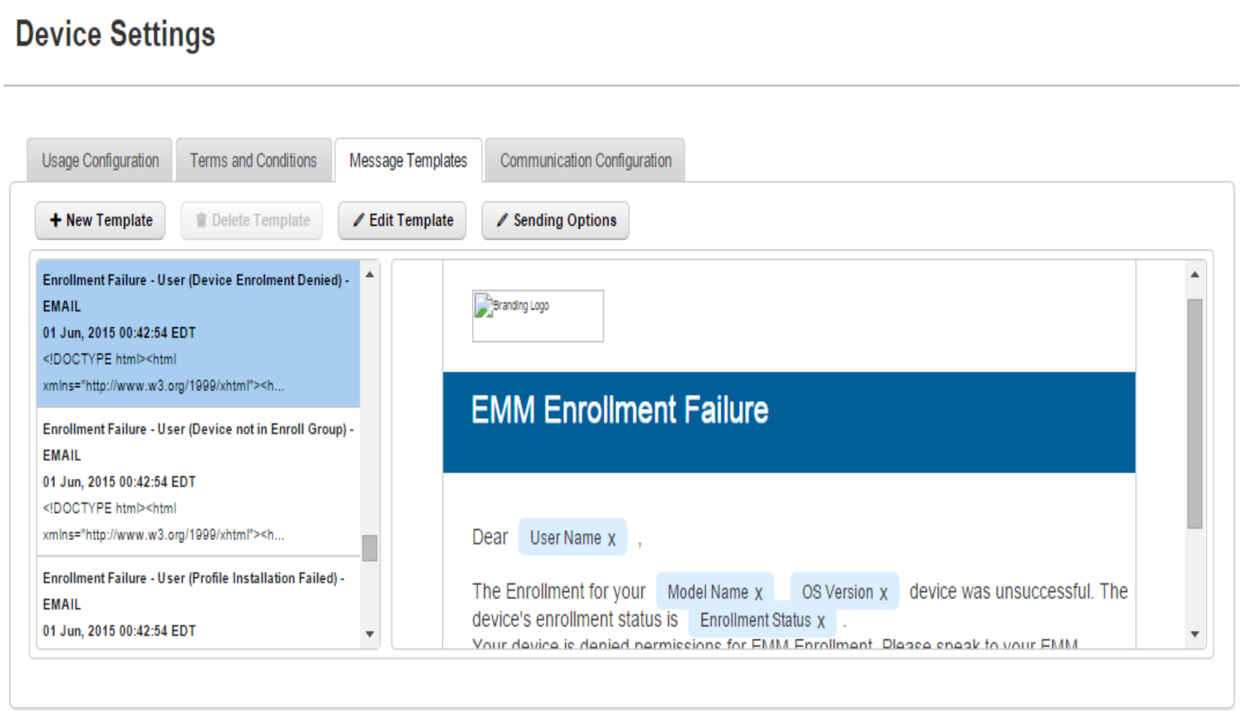
4. Click **OK** to return to the terms and conditions page.

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.

6.2.3 Message Templates

Using Message Templates, you can messages to an administrator or to a user. Administrators can use messages directly or can use message templates after edit them. Administrators can build on top of existing templates to send messages to specific devices or device sets. There are two modes of sending messages - push notifications and email. You can create separate templates for the two modes.



Enrollment Failure - User (Device Enrolment Denied) - EMAIL
01 Jun, 2015 00:42:54 EDT
<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml"><h...

Enrollment Failure - User (Device not in Enroll Group) - EMAIL
01 Jun, 2015 00:42:54 EDT
<!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml"><h...

Enrollment Failure - User (Profile Installation Failed) - EMAIL
01 Jun, 2015 00:42:54 EDT

EMM Enrollment Failure

Dear User Name x ,

The Enrollment for your Model Name x OS Version x device was unsuccessful. The device's enrollment status is Enrollment Status x .

Your device is denied permissions for EMM Enrollment. Please speak to your EMM

You can perform the following activities from the **Message Template** tab.

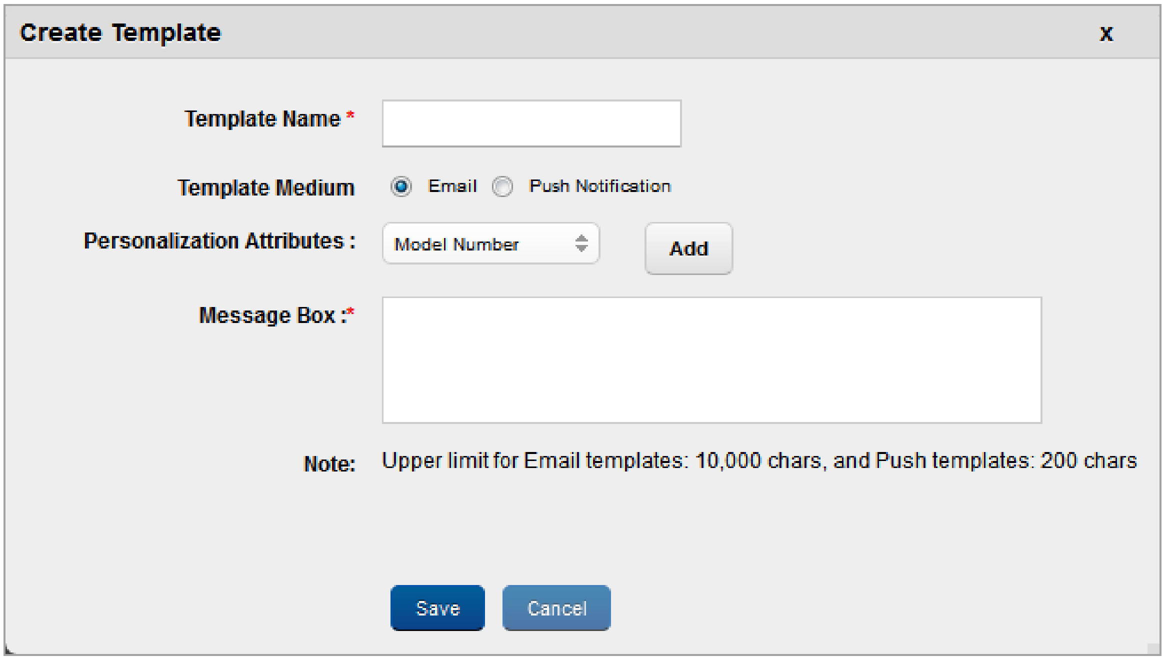
- Creating a New Template
- Editing a Template
- Configure Sending Options
- Deleting a Template

6.2.3.1 Creating a New Template

An administrator uses this template to tailor a message to each individual user or device. The administrator can create templates where certain attributes are populated at runtime based on a recipient. This ensures consistent messages to all recipients.

To create a new template, follow these steps:

1. Click the **+New Template** button under the **Message Template** tab.

   Note: Upper limit for Email templates: 10,000 chars, and Push templates: 200 chars

   The **Create Template** dialog box appears.

2. Enter the following fields:

   i. **Template Name**: Enter your desired name for the template.

   ii. **Template Medium**: Select the medium as email or push notification.

   iii. **Personalization Attributes**: Personalization attributes are pieces of information pertaining to a specific device or a user. Select the personalization attributes from the drop-down list and click **Add.** The following attributes are provided:

   - User ID
   - Company Name
   - Device IMEI
   - Device Model Name

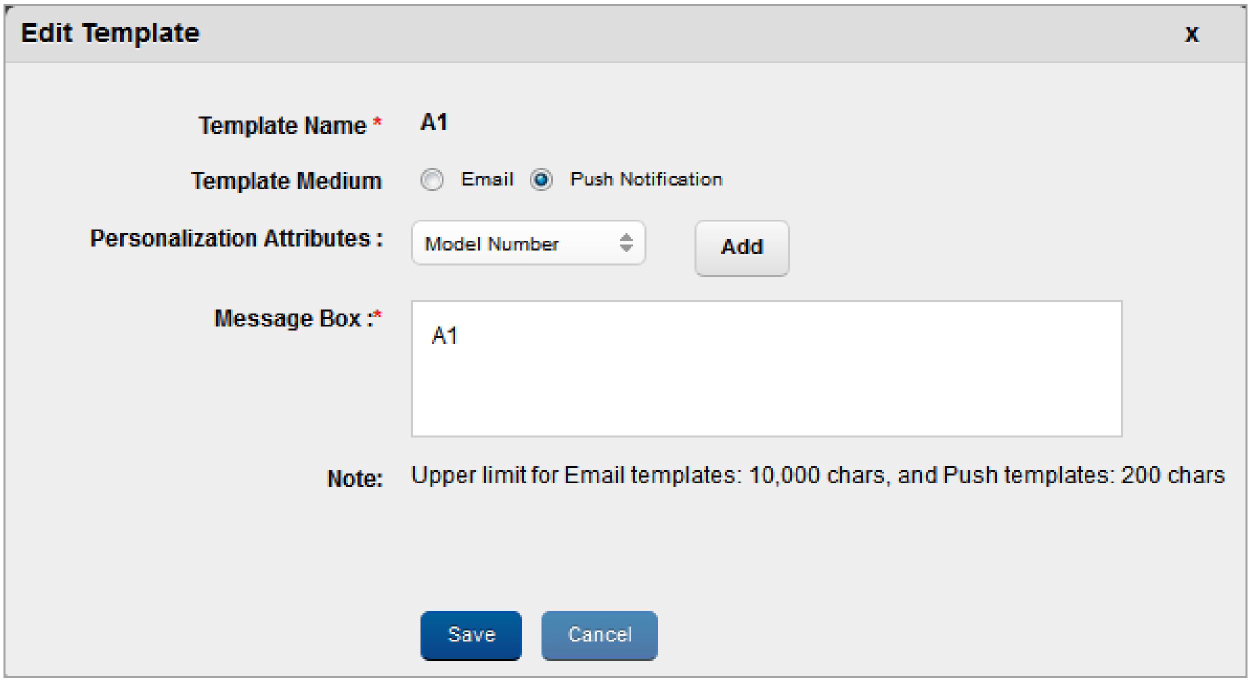
- Device Model No
- Device Name
- Device OS
- Email
- Enrollment Rules
- Enrollment Status
- First Name
- Last Name
- Policy Name
- Time Limit
- Wipe Type

iv. Enter your message in the **Message Box**. Formatting toolbar appears on top of the editor to modify your look and feel of the text. Currently, HTML is not supported. Only plain text is supported.

3. Click the **Save** button. The saved template details appear in the list view.

6.2.3.2 Editing a Template

To modify or edit a template, follow these steps:



Template Name * A1

Template Medium ○ Email ● Push Notification

Personalization Attributes : Model Number

Message Box :* A1

Note: Upper limit for Email templates: 10,000 chars, and Push templates: 200 chars

1. Select the template from the list view and click the **Edit Template** button.

   The Edit Template window appears.

2. Enter details for the following fields:

   i. **Template Medium**: Select the option as email or push notification.

   ii. **Personalization Attributes**: Select the personalization attributes from the drop-down list. You cannot change the **Template Name**.

   iii. Enter your message in the **Message Box**.

3. Click the **Save** button. The saved template details appear in the list view.

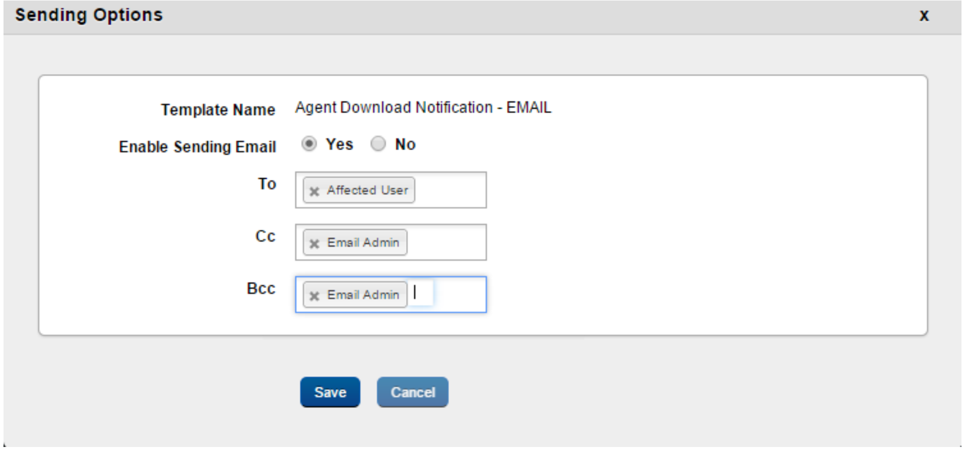
6.2.3.3 Configure Sending Options

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.



Sending Options

Template Name: Agent Download Notification - EMAIL

Enable Sending Email: ● Yes ○ No

To: Affected User

Cc: Email Admin

Bcc: Email Admin

To configure Sending Options, follow these steps:

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**.

6.2.3.4 Deleting a Template

To delete a Template, follow these steps:

1. Select the template from the list view, and click the **Delete Template** button.

   The system displays the warning message (Delete Template) asking if you are sure you want to delete the template.

2. Click the **Yes** button.

   The template is removed from the list view.

   > ***Note:*** There is a known issue with the TextArea Widget in the Chrome Browser. The backspace may not always function properly.

6.2.4 Communication Configuration

This feature helps the administrator to create a device certificate to enable managing the device through Kony Management. Without this certificate, Kony Management cannot manage devices. Kony Management cannot send any commands such as Lock, Locate, Wipe, and Push profiles to adhere to the rules. Following are the Communication Configurations provided for each device:

- Organization Details
- Configure APNS for iOS
- Configure Windows 6.x for Windows Phone 6.x
- Configure Windows Phone 8.x and Windows 8.1 for Windows Phone 8.x and Windows 8.1

6.2.4.1 Organization Details

The user must provide the details of the organization in this section.

Company Name: You must enter the name of your Company.

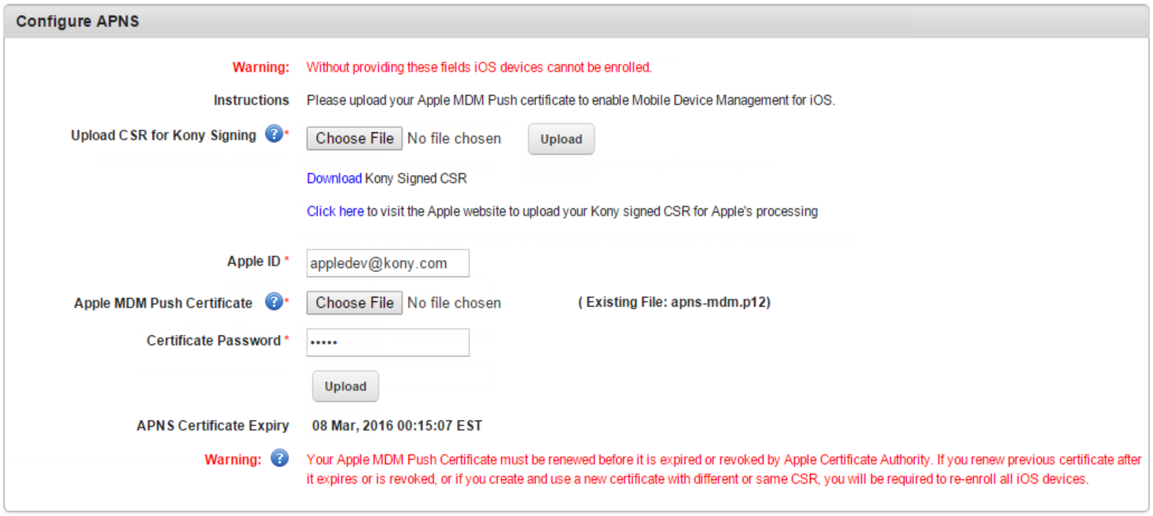
> ***Note:*** Company name changes will only affect new devices enrolled. There is no change on devices already enrolled. This is mandatory for Windows Phone 8.x and Windows 8.1 device enrollments.

6.2.4.2 Configure APNS

The Apple Push Notification Service (APNS) feature helps the administrator to create an Apple MDM certificate to enable mobile management through Kony Management. Without an APNS certificate, Kony Management cannot manage iOS devices. Kony Management cannot send any commands such as Lock, Locate, Wipe or Push profiles onto the iOS device. For more information on APNS, refer Apple Documentation.

To configure APNS, follow these steps:

1. **Upload CSR for Kony Signing**: Browse the file from its location. Select it and click **Open**. The file details appear. Click the **Upload** button to upload the CSR file.



Configure APNS

Warning: Without providing these fields iOS devices cannot be enrolled.

Instructions Please upload your Apple MDM Push certificate to enable Mobile Device Management for iOS.

Upload CSR for Kony Signing *: No file chosen

Download Kony Signed CSR

Click here to visit the Apple website to upload your Kony signed CSR for Apple's processing

Apple ID *: appledev@kony.com

Apple MDM Push Certificate *: No file chosen (Existing File: apns-mdm.p12)

Certificate Password *: •••••

APNS Certificate Expiry: 08 Mar, 2016 00:15:07 EST

Warning: Your Apple MDM Push Certificate must be renewed before it is expired or revoked by Apple Certificate Authority. If you renew previous certificate after it expires or is revoked, or if you create and use a new certificate with different or same CSR, you will be required to re-enroll all iOS devices.

2. **Apple ID:** Enter your email ID.

3. **Apple MDM Certificate**: upload your Apple MDM push certificate. Browse the file from its location. Select it and click **Open**. The file details appear.

4. **Certificate Password**: Enter the certificate password.

5. Click the **Upload** button.

> *Note:* The **APNS Certificate Expiry** field displays the expiry date of the APNS certificate.

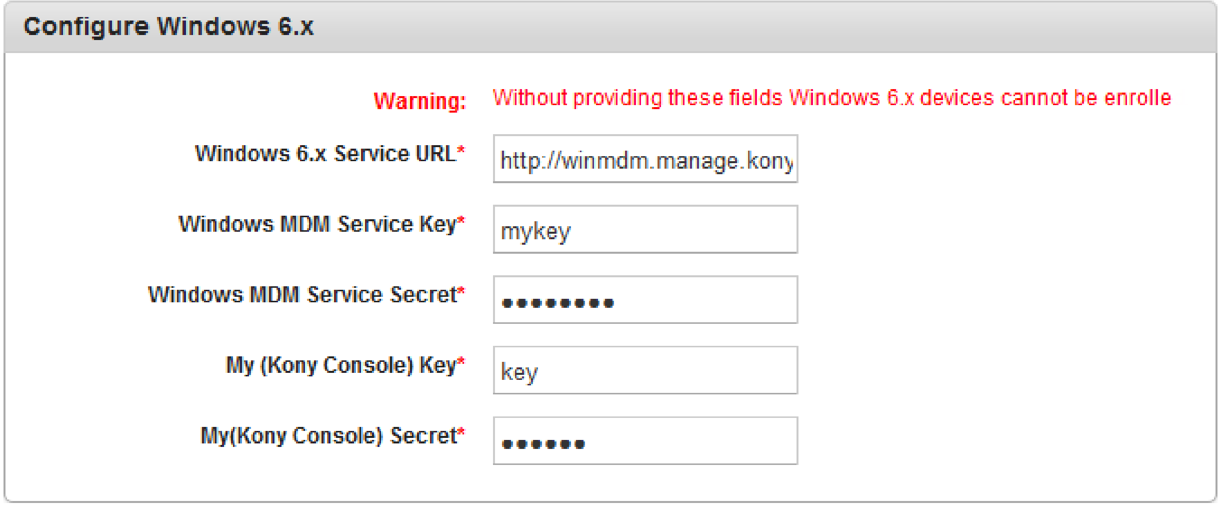
6. Click **Save**. A success message appears.

7. Click **OK**.

6.2.4.3 Configure Windows 6.x

To know how to install Windows Server, refer the installation document. Two services: MDM setup and Group Policy setup

To configure Window 6.x, follow these steps:



Configure Windows 6.x

Warning: Without providing these fields Windows 6.x devices cannot be enrolle

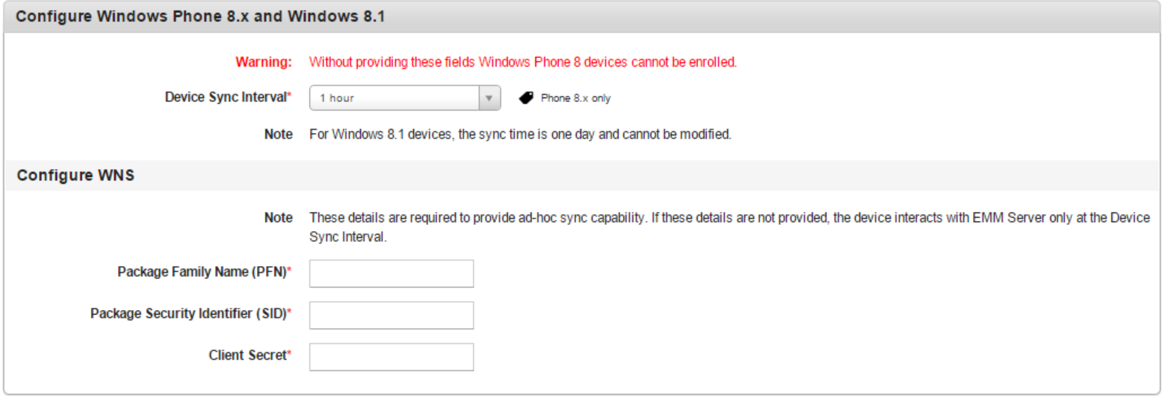
Windows 6.x Service URL*	http://winmdm.manage.kony
Windows MDM Service Key*	mykey
Windows MDM Service Secret*	●●●●●●●●●
My (Kony Console) Key*	key
My(Kony Console) Secret*	●●●●●●

1. **Windows 6.x Service URL**: Enter the URL where you have set up your Windows Server.
2. **Windows MDM Service Key**: Enter the key that you provided while performing the installation process of MDM.
3. **Windows MDM Service Secret**: Enter the secret password that you provided while performing the installation process of MDM.
4. **My (Kony Console) key**: Use the same key that is used for MDM Service Key.
5. **My (Kony Console) Secret**: Use the same Secret password that is used while installing process of MDM.
6. Click **Save**. A success message appears.
7. Click **OK**.

> *Important:* Do not use the WinMDM server directly to send commands to devices or to configure policies. Use Kony EMM server only.

6.2.4.4 Configure Windows Phone 8.x and Windows 8.1

To configure Window 8.x and Windows 8.1, follow these steps:



Configure Windows Phone 8.x and Windows 8.1

Warning: Without providing these fields Windows Phone 8 devices cannot be enrolled.

Device Sync Interval* 1 hour ▾ Phone 8.x only

Note For Windows 8.1 devices, the sync time is one day and cannot be modified.

Configure WNS

Note These details are required to provide ad-hoc sync capability. If these details are not provided, the device interacts with EMM Server only at the Device Sync Interval.

Package Family Name (PFN)*

Package Security Identifier (SID)*

Client Secret*

1. **Device Sync Interval (in minutes)**: Enter the duration in hours. Device Sync Interval should be at least one hour. For Windows 8.1 devices, the sync time is one day and cannot be modified.

   If you want to use Windows Notification Service, you must enter details in the Configure WNS section. For more information on PFN, see the Pre-Install guide.

2. **Package Family Name (PFN)**: Enter the Package Family Name. The package family name you enter here will be validated during the device enrollment stage. Once you enroll a Windows 8.1 or Windows Phone 8.x device, a validation takes place. If the PFN you entered is not correct, a warning appears prompting you to enter a correct PFN.

   Once a valid PFN is provided, it is valid until it expires (one year). Before the PFN expires, if it is replaced with another valid PFN, the new PFN is honored.

   > *Note:* If PFN is not provided, after device (Windows Phone 8.x and Windows 8.1) enrollment, MDM push will not work on the enrolled device. The enrolled device will communicate with the server only at scheduled intervals and not on demand. MDM policies will apply only at scheduled intervals. Once PFA is provided, when the device pings the server, MDM push will be enabled.

3. **Package Security Identifier (SID)**: Enter the package security identifier of the PFN.

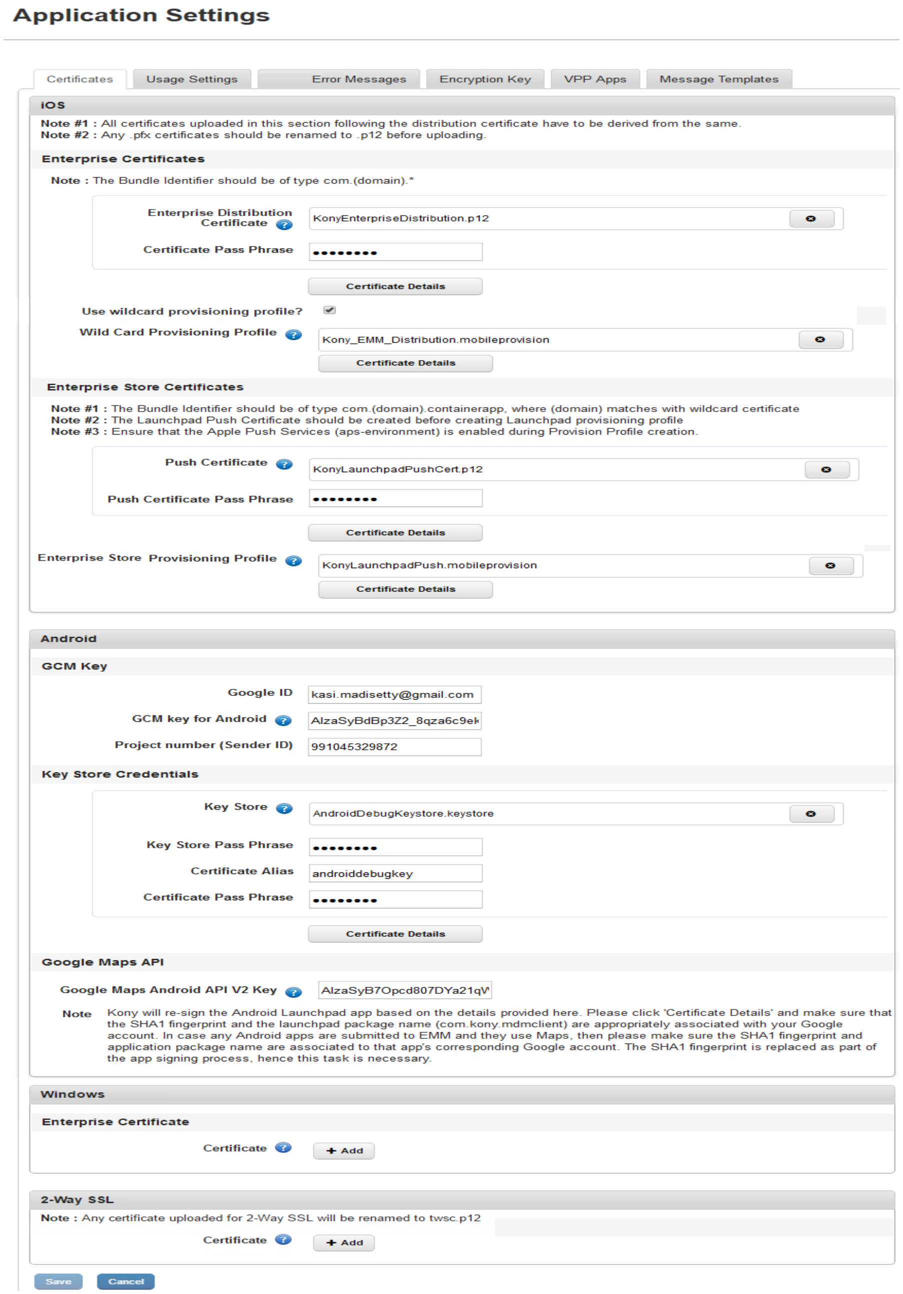
4. **Client Secret**: Enter the client secret of the PFN.

5. Click **Save**. A success message appears.

6. Click **OK**.

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

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: KonyEnterpriseDistribution.p12
Certificate Pass Phrase: ●●●●●●●●●

Use wildcard provisioning profile? ☑
Wild Card Provisioning Profile: Kony_EMM_Distribution.mobileprovision

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: KonyLaunchpadPushCert.p12
Push Certificate Pass Phrase: ●●●●●●●●●

Enterprise Store Provisioning Profile: KonyLaunchpadPush.mobileprovision

Android

GCM Key

Google ID: kasi.madisetty@gmail.com
GCM key for Android: AlzaSyBdBp3Z2_8qza6c9ek
Project number (Sender ID): 991045329872

Key Store Credentials

Key Store: AndroidDebugKeystore.keystore
Key Store Pass Phrase: ●●●●●●●●●
Certificate Alias: androiddebugkey
Certificate Pass Phrase: ●●●●●●●●●

Google Maps API

Google Maps Android API V2 Key: AlzaSyB7Opcd807DYa21qV

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.mdmclient) 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

2-Way SSL

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

Certificate

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

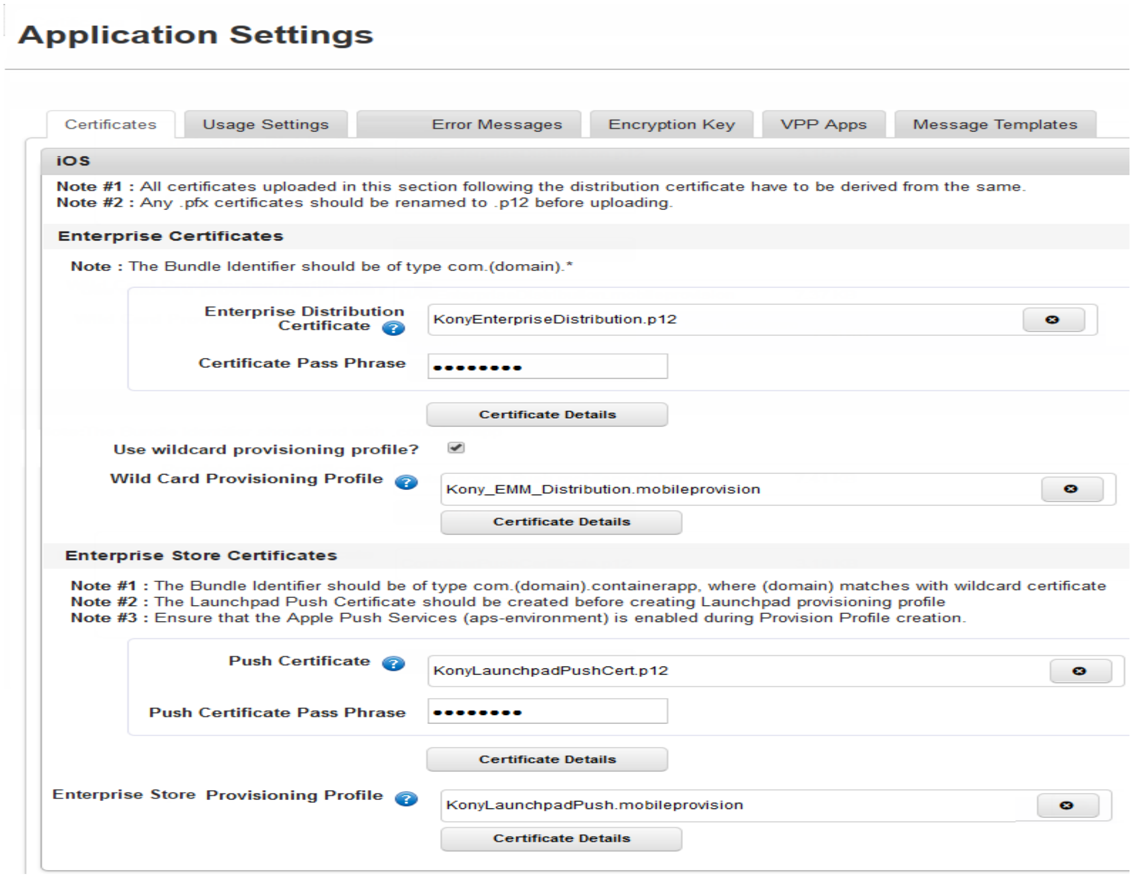
6.3.1 Certificates

The primary purpose to have certificates for iOS, Android, and Windows is to enroll 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

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: KonyEnterpriseDistribution.p12

Certificate Pass Phrase: ••••••••

Use wildcard provisioning profile? ☑

Wild Card Provisioning Profile: Kony_EMM_Distribution.mobileprovision

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: KonyLaunchpadPushCert.p12

Push Certificate Pass Phrase: ••••••••

Enterprise Store Provisioning Profile: KonyLaunchpadPush.mobileprovision

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	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**. 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.
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.

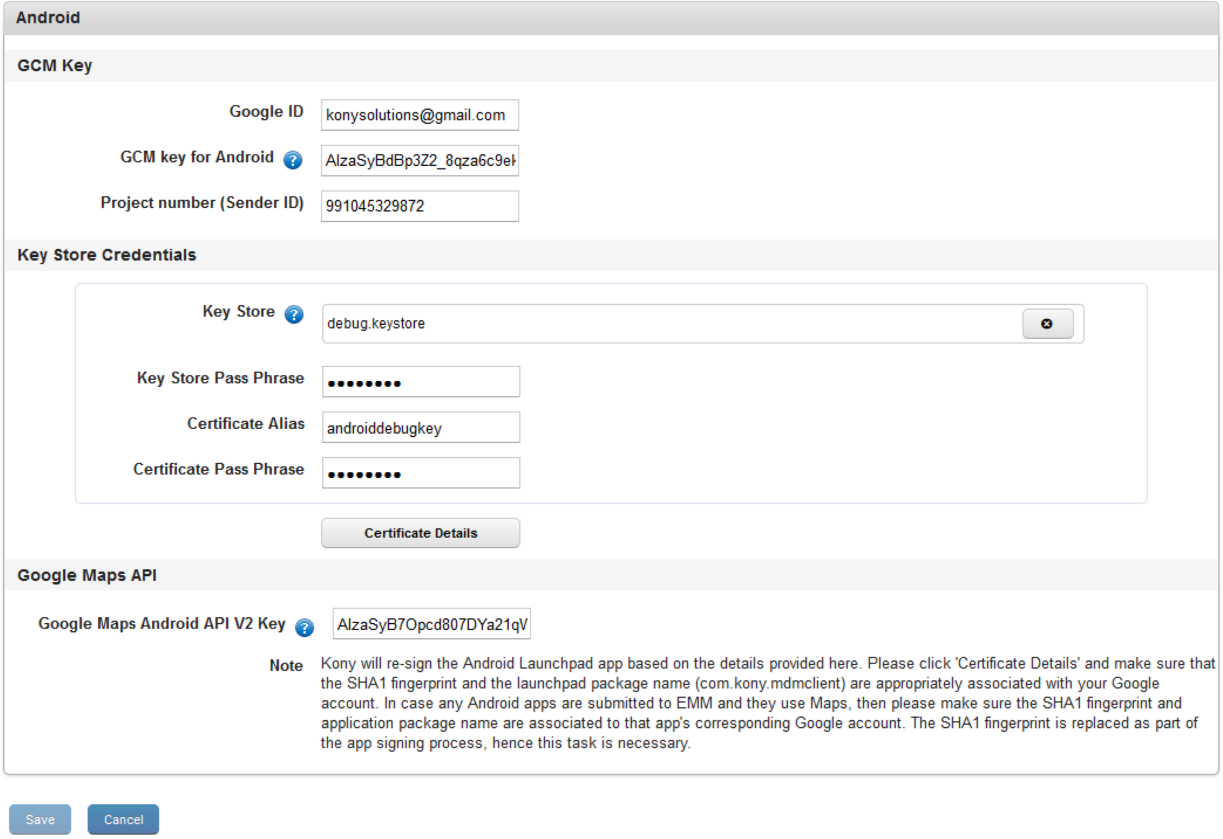
Ensure that you have the following information before you configure the Android certificates:

- 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	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 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.

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	konysolutions@gmail.com
GCM key for Android	AlzaSyBdBp3Z2_8qza6c9ek
Project number (Sender ID)	991045329872

Key Store Credentials

Key Store	debug.keystore
Key Store Pass Phrase	••••••••
Certificate Alias	androiddebugkey
Certificate Pass Phrase	••••••••

Google Maps API

Google Maps Android API V2 Key	AlzaSyB7Opcd807DYa21qV

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.mdmclient) 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 IDGoogle ID**: Enter your email account ID.

   ii. **GCM Key for Android**: Enter your GCM Key for Android.

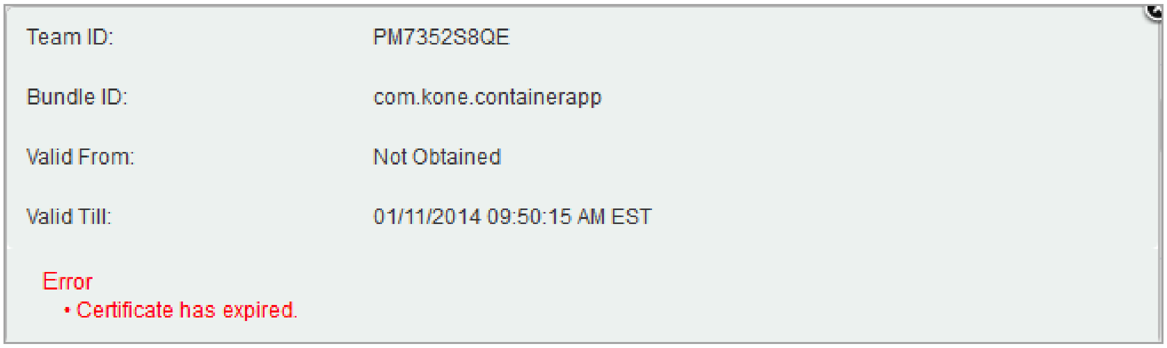
   iii. **Project Number (Sender ID)**: Enter the Sender ID.
3. In the **Key Store Credentials** section, enter the following:
   i. **Key Store**: Click **+Add** to select the certificate from its location and then click **Open**. The selected certificate with size in KB appears next to the Key Store label.
      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.



Team ID:	PM7352S8QE
Bundle ID:	com.kone.containerapp
Valid From:	Not Obtained
Valid Till:	01/11/2014 09:50:15 AM EST

Error
- Certificate has expired.

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.

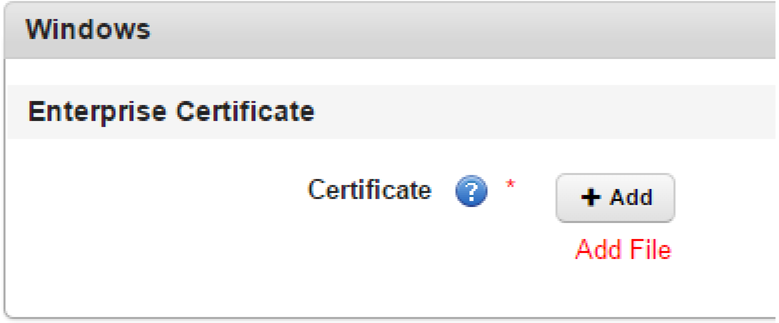
5. Click **Save** to save the entered details.In the confirmation message that appears, click **OK** to return to the main page.

6.3.1.3 Windows Phone 8.x

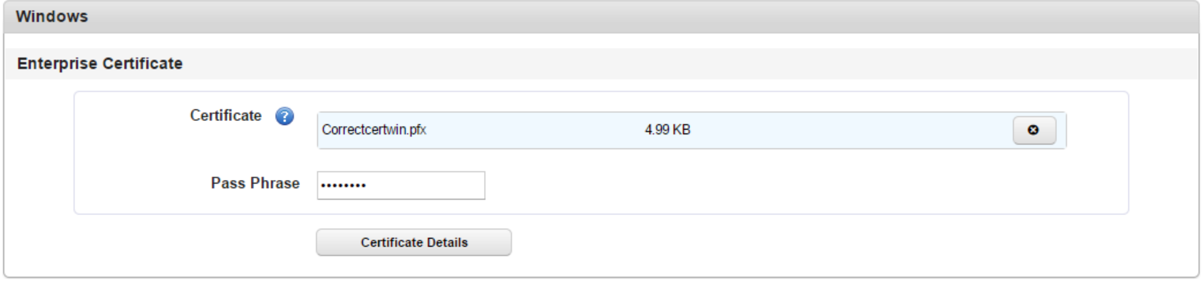
Windows Phone 8.x devices require a Symantec Code Signing Certificate. Symantec is the only provider of code signing certificates for the Windows Phone Private Enterprise program. You can use this certificate to enable and distribute your windows applications within your organization. This certificate 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**.



Certificate: Correctcertwin.pfx 4.99 KB

Pass Phrase: ••••••••

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.

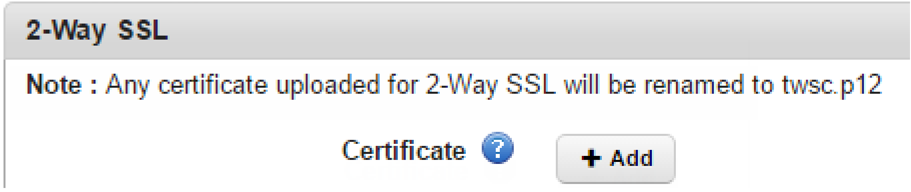
The SSL certificate is used to contact any server resource inside a customer's network that requires mutual authentication - for example, f5 load balancer. You must provide an x509 client side certificate (.p12 supported) for two-way SSL authentication, for the Enterprise Store to authenticate to a back-end. 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.

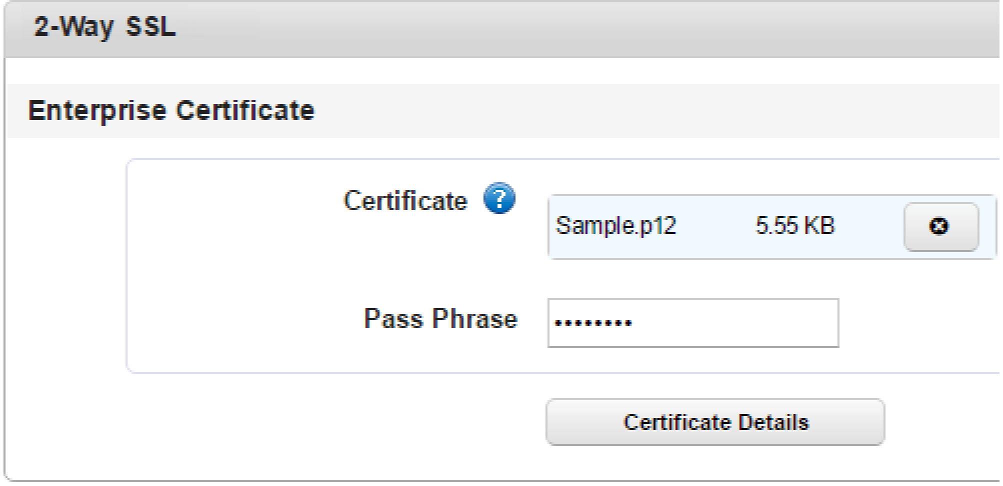
To upload an enterprise certificate for two-way SSL, follow these steps:


2-Way SSL

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

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: ••••••••

> *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	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. For Android devices, if the user exceeds the maximum number of allowed attempts, enterprise wipe will be initiated on the device.
Trigger Enterprise Wipe on Device after Failed Attempts Offline	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.
Device Limit	
Maximum number of Devices Per User	Admin can limit the number of devices per user to be enrolled. Select one of the options from the list. Once the limit is reached, all subsequent device enrollments will fail.
Local EMM User Password Settings	
Reset Password on First Log-in	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.

Feature	Description
Complexity of Password	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. 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. 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: 1. Email notifications cannot be sent to the user. These notifications include user enrollment, device actions, app updates, and others. 2. Email policies cannot be applied. 3. The user cannot participate in the iOS Volume Purchasing Program.

Feature	Description
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: • 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 A user with limited administrator permissions will not get Reset password information notifications.	
Enterprise App Licenses	
Enable Enterprise App Licenses	By default, this is set to **No**. Configuring this to **Yes** will enable restricting enterprise app distribution through licenses.

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:
   1. 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.
   2. Overwrite Local Group with Imported Group. If this is configured to yes, the local group will get overwritten with the first imported group.
   3. Sync Groups for AD Users after Login. If this is configured to yes,
   4. 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.

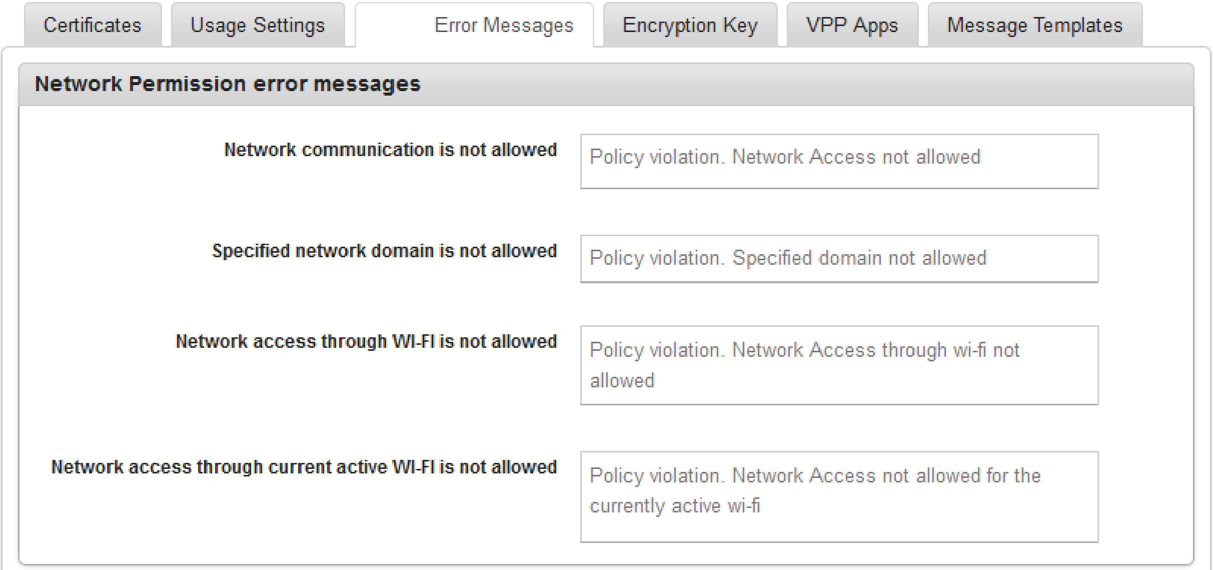
6.3.3 Error Messages

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

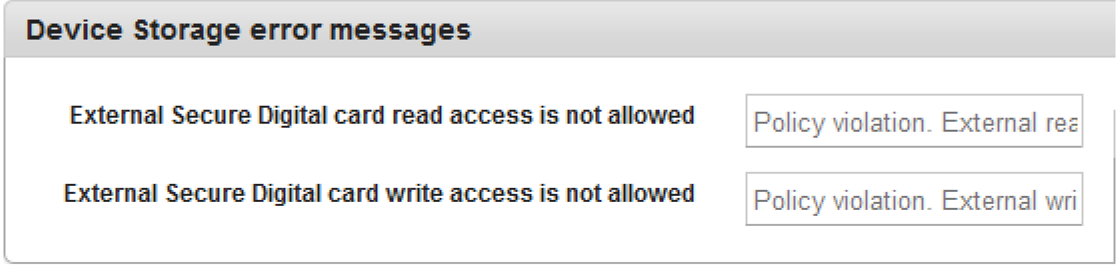


Network Permission error messages

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



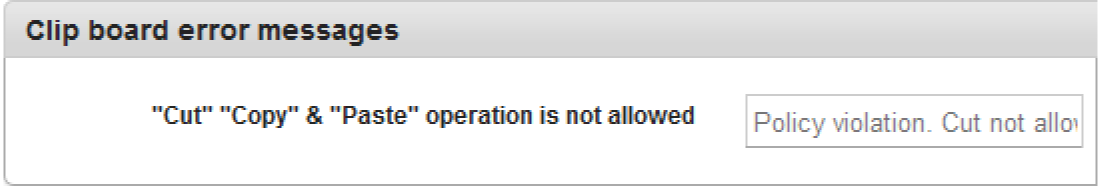
Device Storage error messages

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

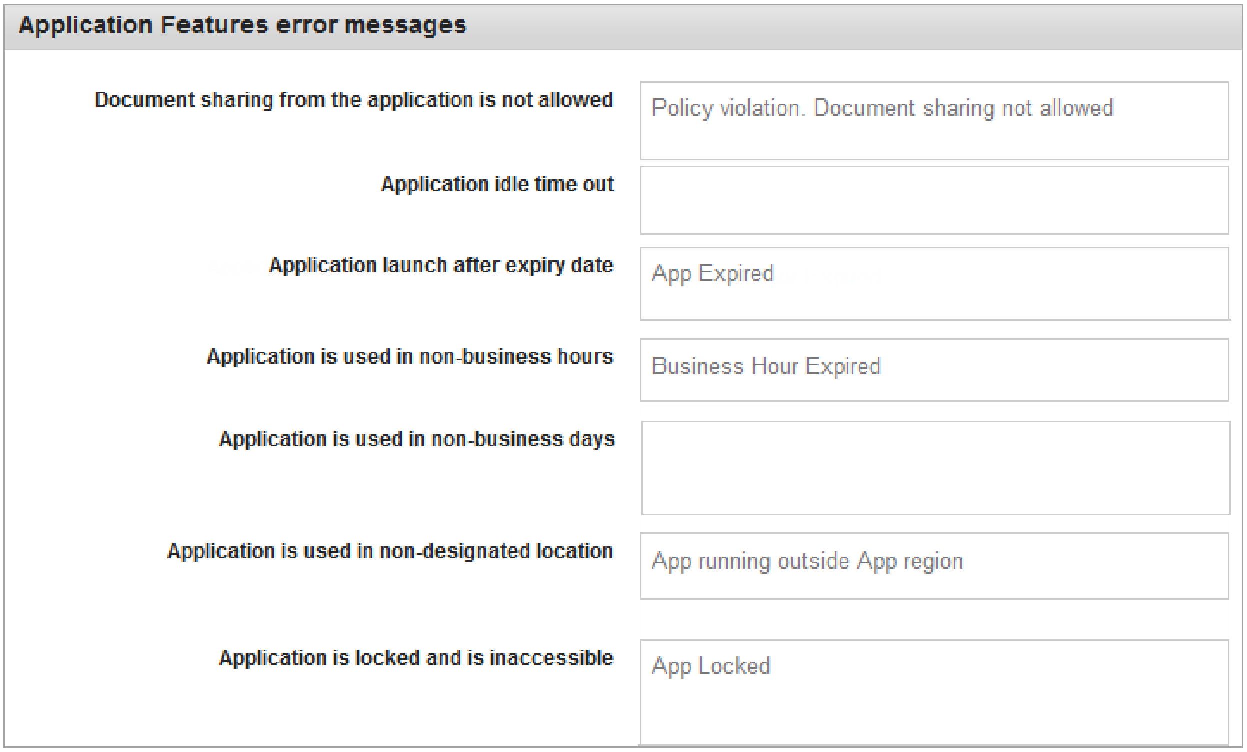


Clip board error messages

"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

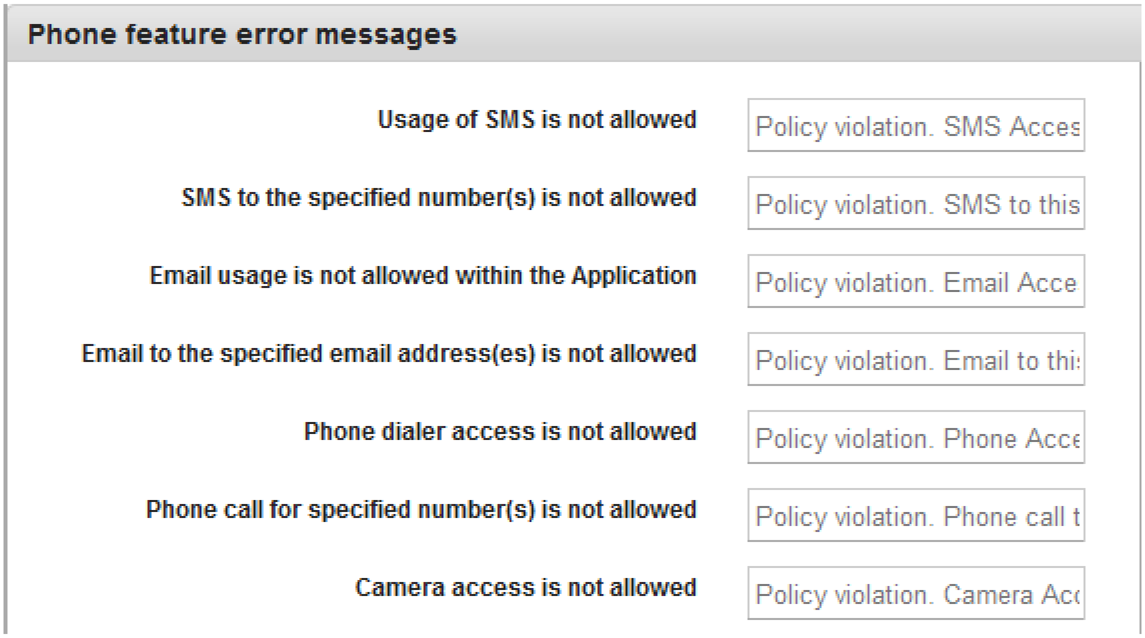


Application Features error messages

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:
   1. Document sharing from the application is not allowed
   2. Application idle timeout
   3. Application launch after expiry date
   4. Application is used in non-business hours
   5. Application is used in non-business days
   6. Application is used in non-designated location
   7. Application is locked and is inaccessible

Phone Features Error Messages

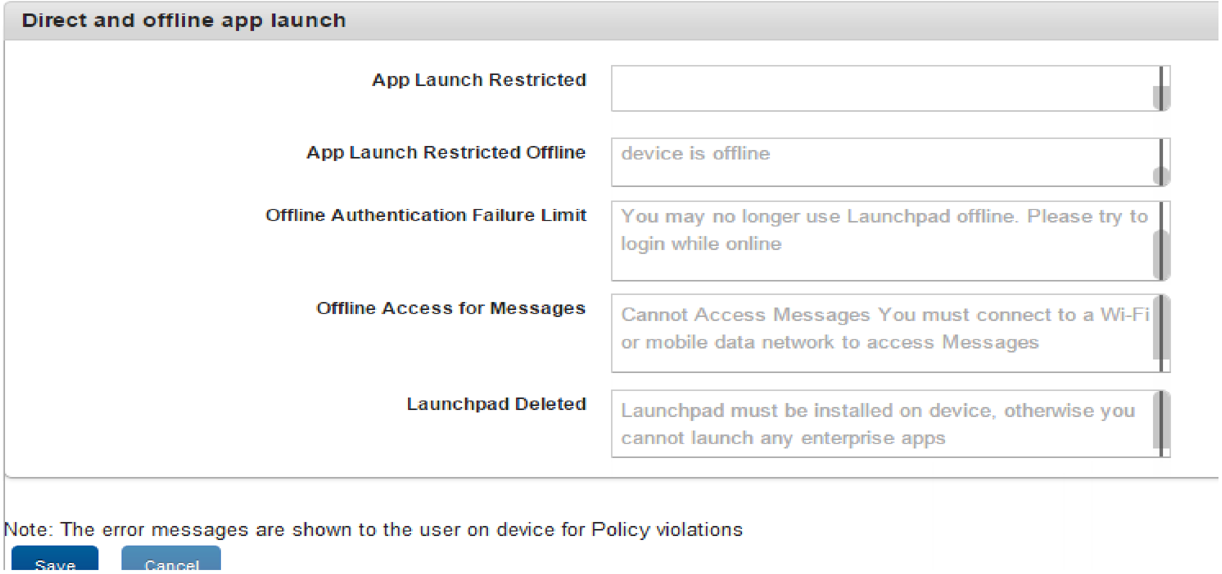


Phone feature error messages

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	
App Launch Restricted Offline	device is offline
Offline Authentication Failure Limit	You may no longer use Launchpad offline. Please try to login while online
Offline Access for Messages	Cannot Access Messages You must connect to a Wi-Fi or mobile data network to access Messages
Launchpad Deleted	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

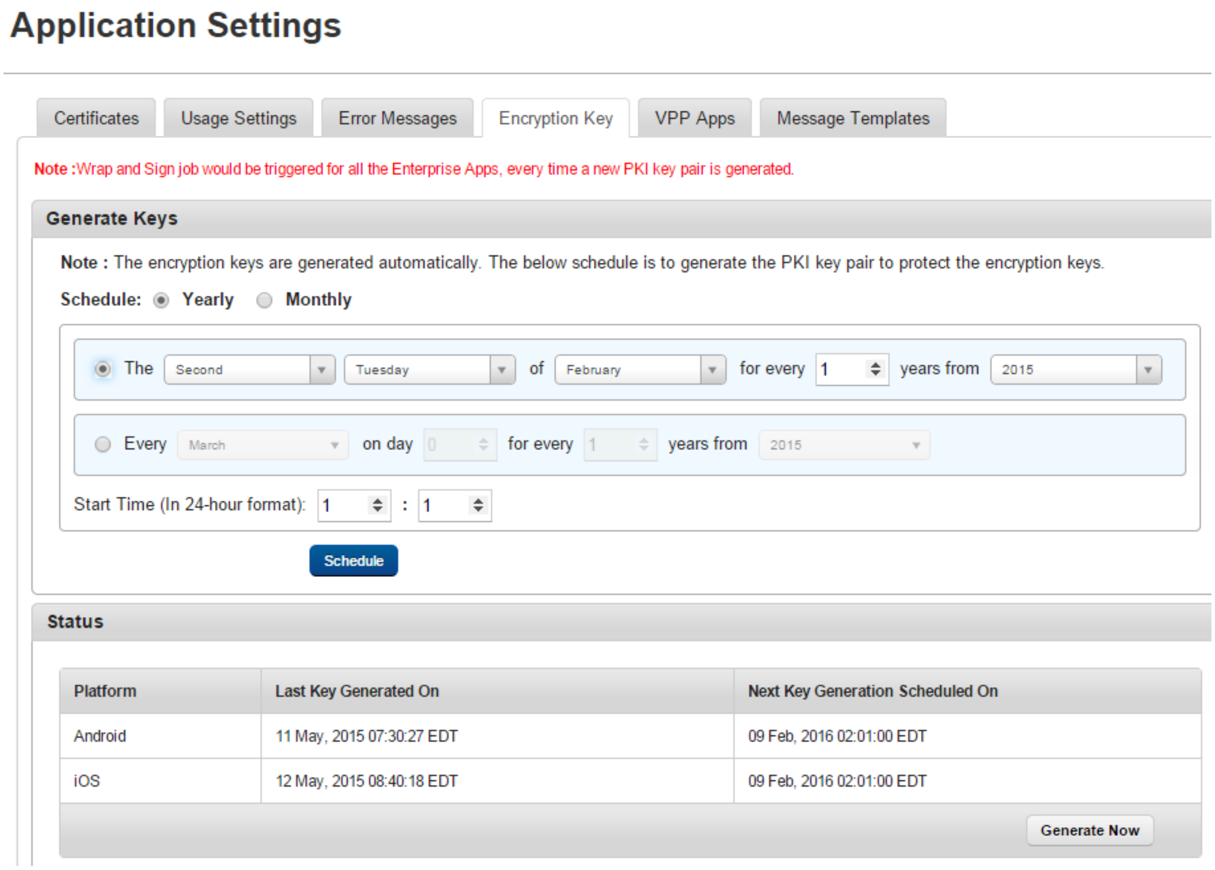
1. Enter the customized error messages for the following fields:
   a. App Launch Restricted
   b. App Launch Restricted Offline
   c. Offline Authentication Failure Limit
   d. Offline Access for Messages
   e. Enterprise Store Deleted

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

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

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

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.

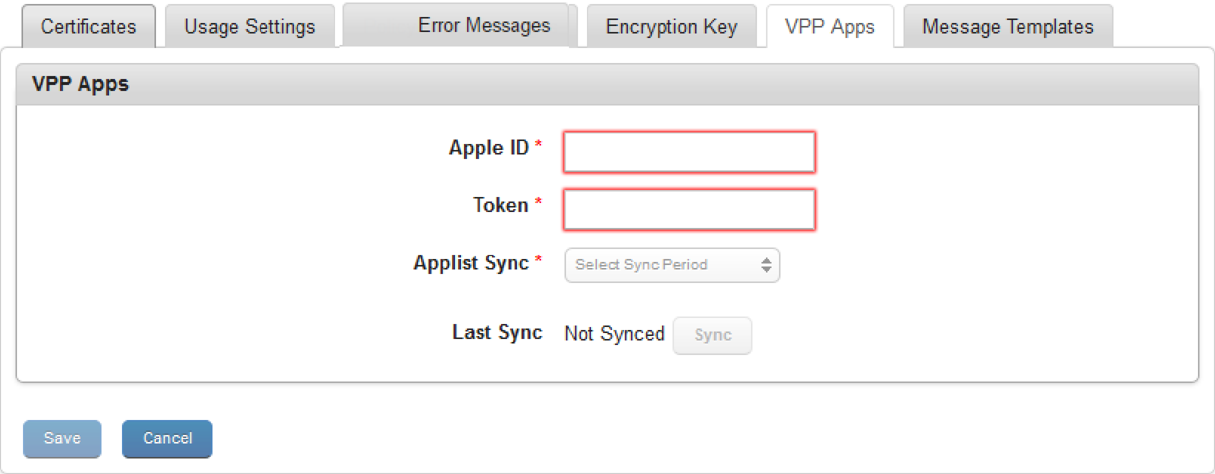
  - **Last Key Generated On**: Displays the time the encryption key was generated.

  - **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.



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/

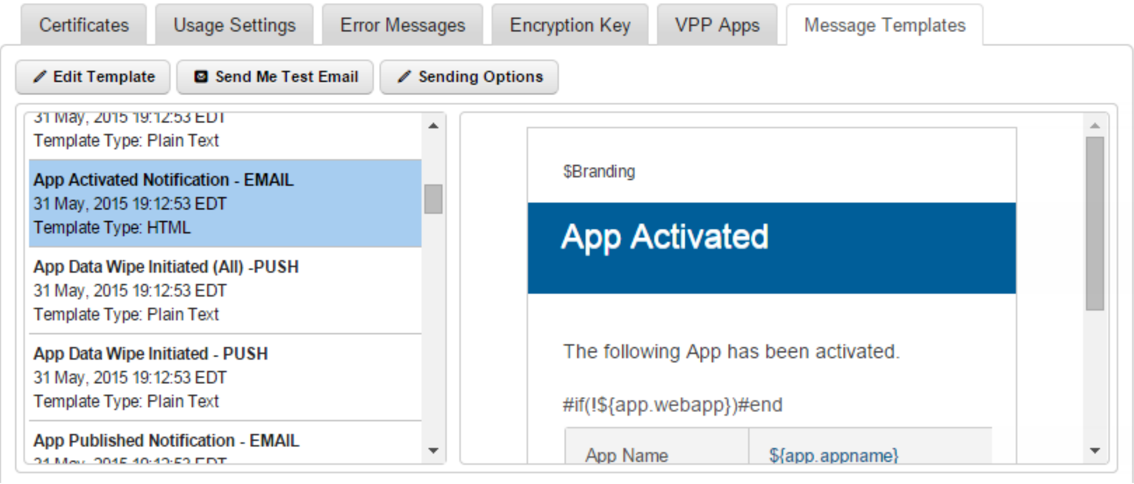
   Each token is valid for one year from the time it is generated.

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 the 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.



31 May, 2015 19:12:53 EDT
Template Type: Plain Text

App Activated Notification - EMAIL
31 May, 2015 19:12:53 EDT
Template Type: HTML

App Data Wipe Initiated (All) -PUSH
31 May, 2015 19:12:53 EDT
Template Type: Plain Text

App Data Wipe Initiated - PUSH
31 May, 2015 19:12:53 EDT
Template Type: Plain Text

App Published Notification - EMAIL
31 May, 2015 19:12:53 EDT

$Branding

App Activated

The following App has been activated.

#if(!${app.webapp})#end

App Name	${app.appname}

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.

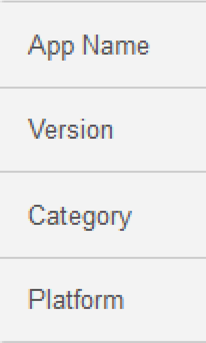
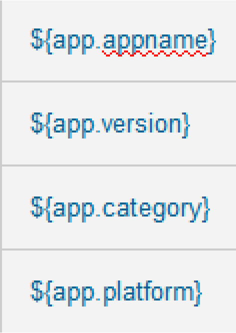
6.3.6.1 Pre-Defined Templates

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

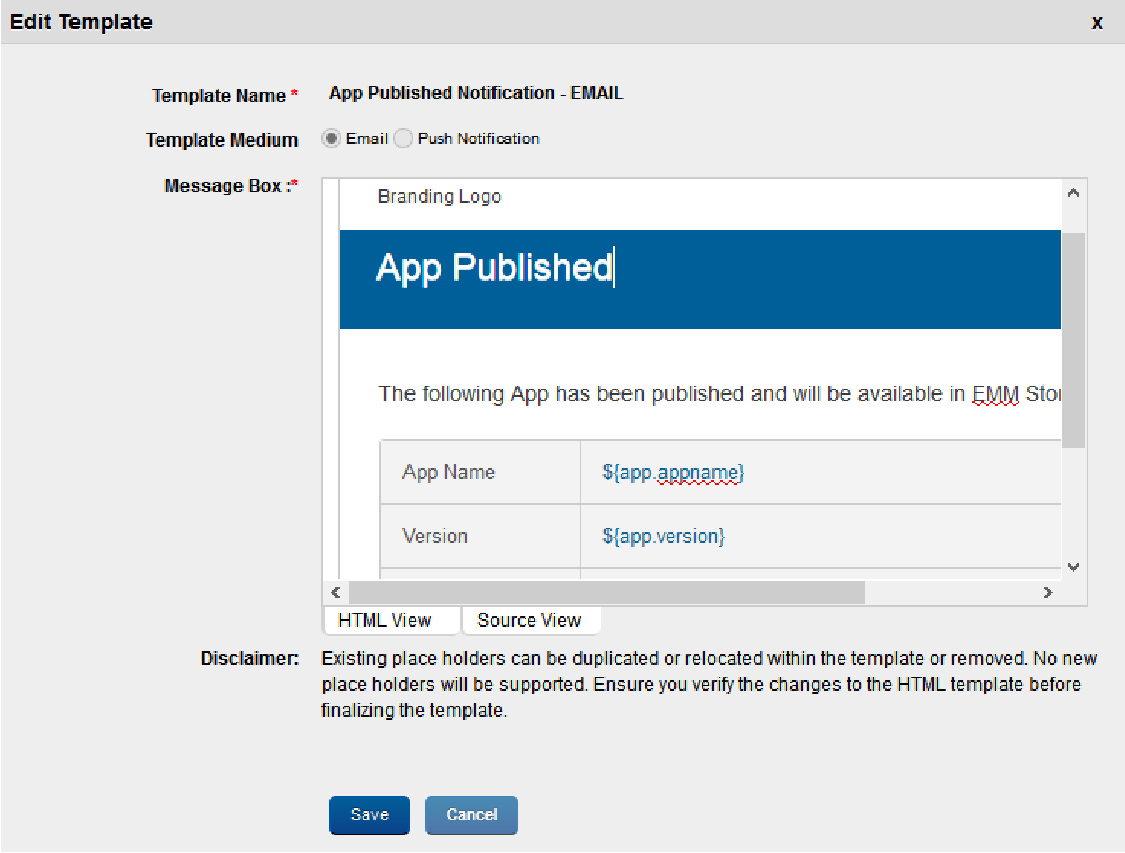
The Admin can edit pre-defined templates. The placeholder tags must not modified, but can be shifted from one place to another. If tags are modified, the system can not fetch the data for that tag. Ensure that you only modify tags labels if required.

For example:

Tag Labels	Placeholders
 App Name Version Category Platform	 ${app.appname} ${app.version} ${app.category} ${app.platform}

To edit a template, follow these steps:

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



Edit Template

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 Sto

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.

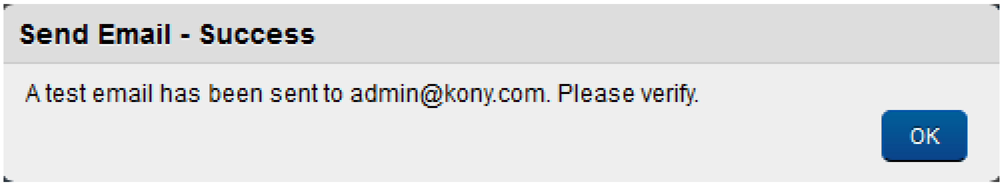
6.3.6.3 Sending a Test Email

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.*"

   Send Email - Success

   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

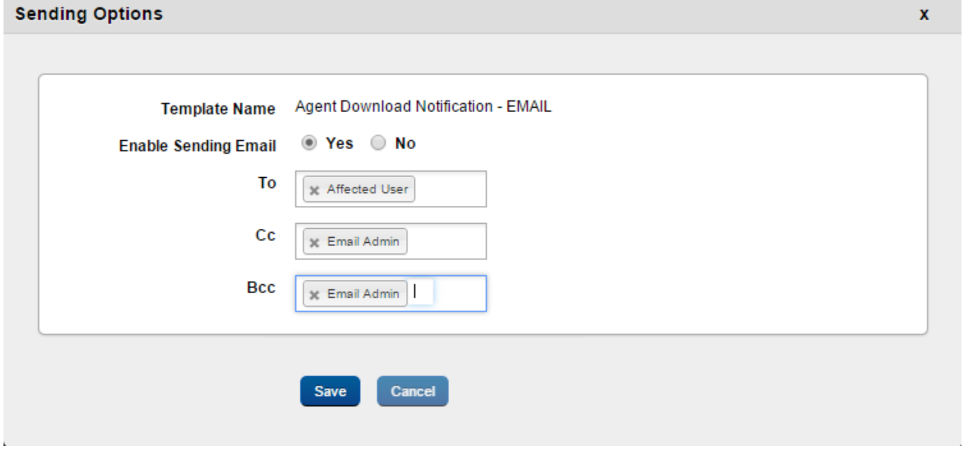
This feature helps you enable or disable message-template notifications to users. If you send notifications, you can customize the audience for these notifications. You can customize sending options for each message templates based on the required audience. Messages can be specific to affected users,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



Sending Options

Template Name Agent Download Notification - EMAIL

Enable Sending Email ● Yes ○ No

To: Affected User

Cc: Email Admin

Bcc: Email Admin

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**.

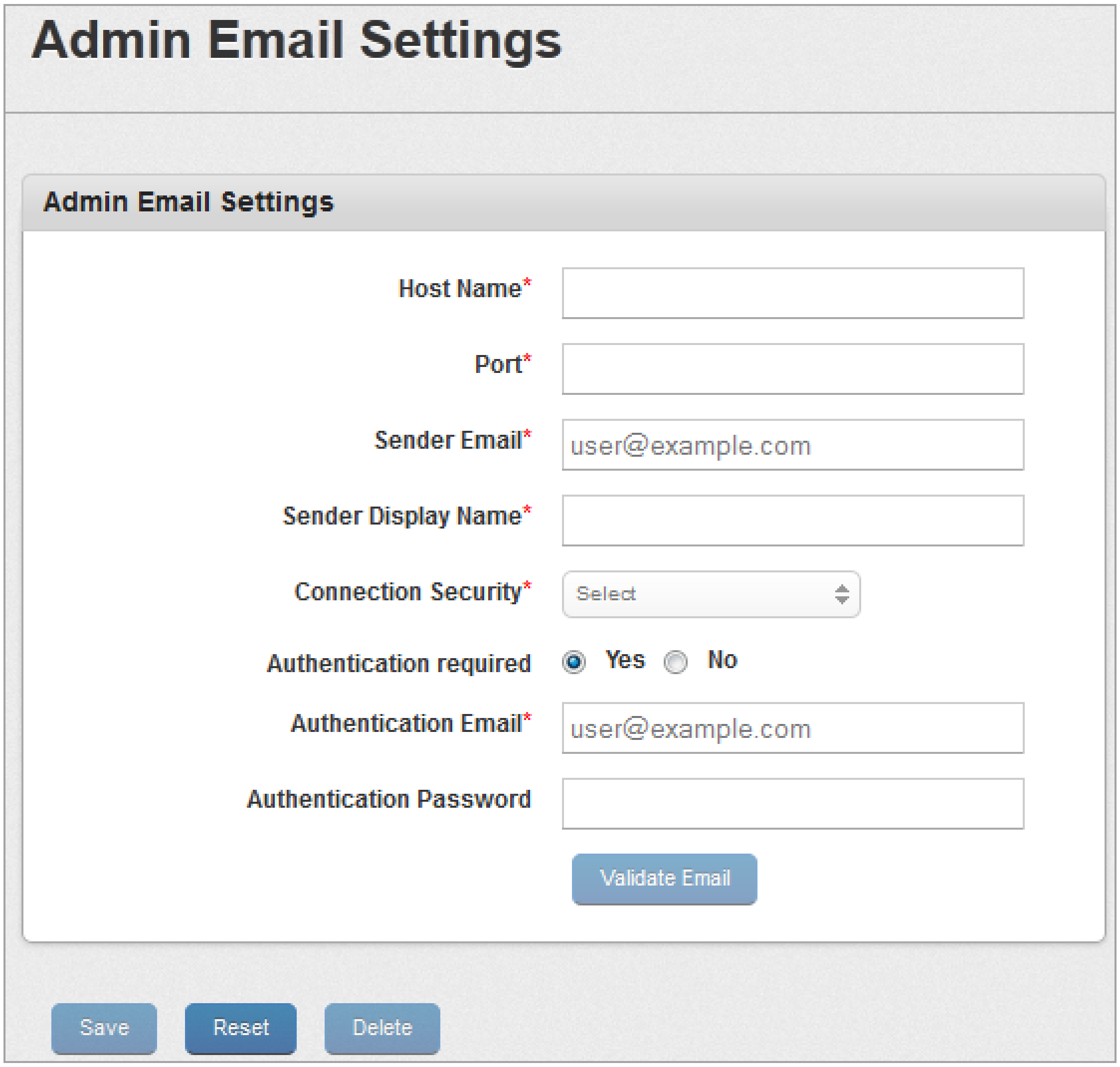
6.3.6.5 Deleting a Template

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*	user@example.com
Sender Display Name*	
Connection Security*	Select
Authentication required	● Yes ○ No
Authentication Email*	user@example.com
Authentication Password	

To configure Admin Email Settings, follow these steps:

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

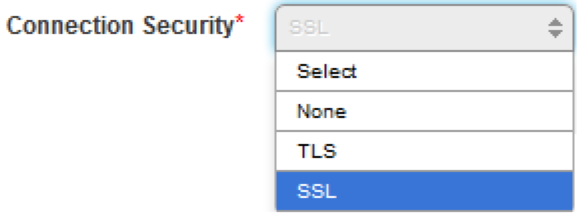
   Hostname is the domain name that absolutely and uniquely identifies every computer hooked up to the Internet through the Domain Name Service (DNS) naming hierarchy. You use host name to communicate with the enrolled devices to EMM.

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.



Connection Security* SSL

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?

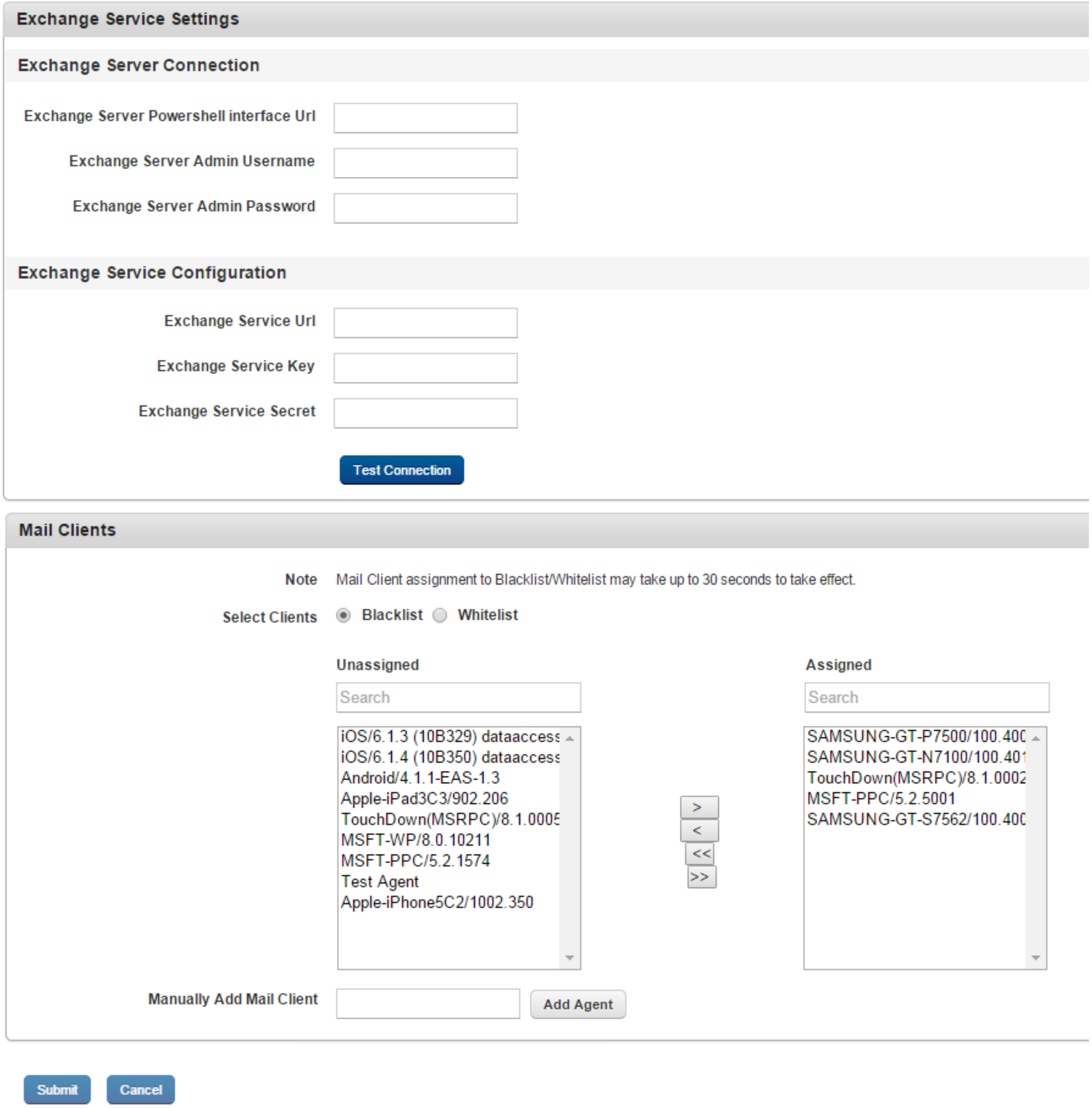
12. Click **Yes** to continue.

13. In the success message that appears, click **OK** to return to the main page. The deleted Admin Email Settings is removed.

6.5 Exchange Services

The current settings depend upon the Kony Exchange service. To know more details about How to install Kony Exchange service, see Exchange Service Document.

Based on the credentials provided in the Kony Exchange service configuration the current settings values have to be entered. Only one Exchange Server is supported by EMM currently.



Exchange Service Settings

Exchange Server Connection

Exchange Server Powershell interface Url

Exchange Server Admin Username

Exchange Server Admin Password

Exchange Service Configuration

Exchange Service Url

Exchange Service Key

Exchange Service Secret

Mail Clients

Note Mail Client assignment to Blacklist/Whitelist may take up to 30 seconds to take effect.

Select Clients ● Blacklist ○ Whitelist

Unassigned

iOS/6.1.3 (10B329) dataaccess
iOS/6.1.4 (10B350) dataaccess
Android/4.1.1-EAS-1.3
Apple-iPad3C3/902.206
TouchDown(MSRPC)/8.1.0005
MSFT-WP/8.0.10211
MSFT-PPC/5.2.1574
Test Agent
Apple-iPhone5C2/1002.350

Assigned

SAMSUNG-GT-P7500/100.400
SAMSUNG-GT-N7100/100.401
TouchDown(MSRPC)/8.1.0002
MSFT-PPC/5.2.5001
SAMSUNG-GT-S7562/100.400

Manually Add Mail Client

From the **Settings** section, click **Exchan**ge **Services** from the left panel. The Email Exchange Settings page appears with two sections:

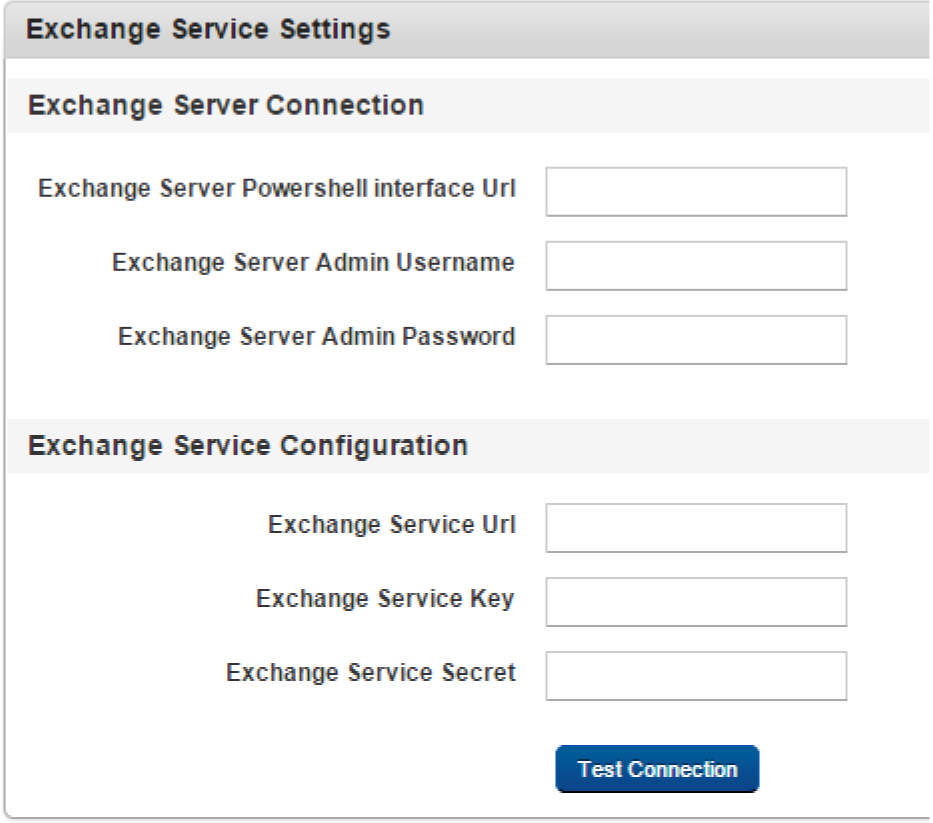
- Exchange Service Settings
- Mail Clients

Email Exchange Settings is specifically for AD Users. From this section, you can blacklist or whitelist specific email clients. The blacklisted clients cannot communicate with your device.

If you have configured Mail Clients setting, then Block Email button is available under Device List> Block Email section.

To configure Email Exchange Settings, follow these steps:

1. Exchange Server Settings: Enter details for the following fields:



Exchange Service Settings

Exchange Server Connection

Exchange Server Powershell interface Url

Exchange Server Admin Username

Exchange Server Admin Password

Exchange Service Configuration

Exchange Service Url

Exchange Service Key

Exchange Service Secret

   a. **Exchange Server Powershell interface URL**: Enter the Exchange Server powershell URL. It is usually similar to "https://< hostname >/powershell/" where hostname is the hostname of the Exchange Server.

   b. **Exchange Server Admin Username**: Enter the name of the Administrator.

c. **Exchange Server Admin Password**: Enter the password for Administrator to access Exchange Server.

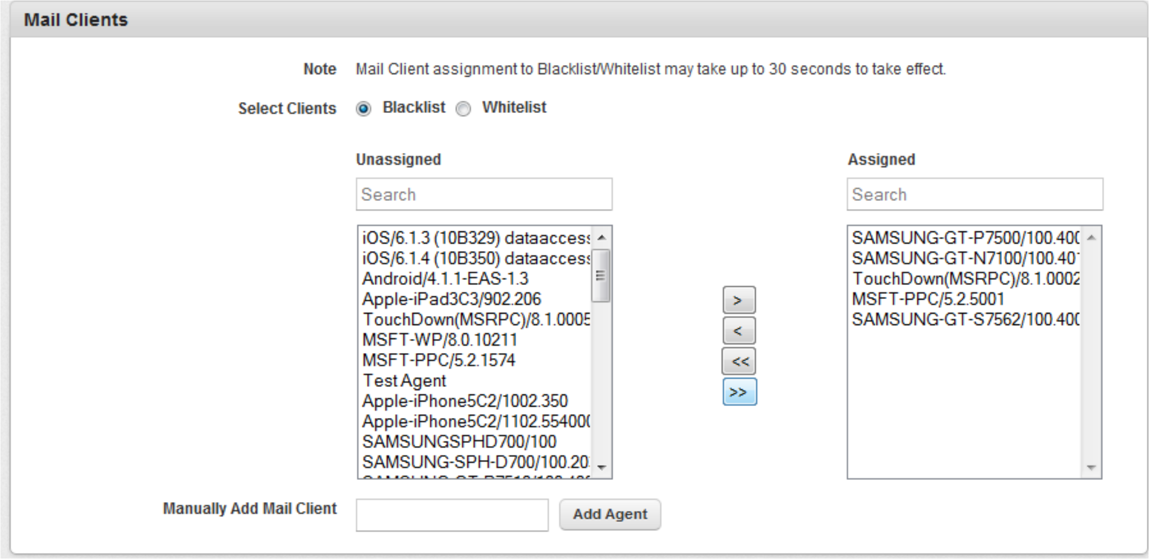
d. **Exchange Service URL**: Enter the Kony Exchange Service URL.

e. **Exchange Service Key**: Enter the Kony Exchange Service Key.

f. **Exchange Service Secret**: Enter the Kony Exchange Service Secret.

These are the Email clients used by the devices to connect to the Exchange Server. The administrator can choose to allow or deny specific mail clients from interacting with the Exchange Server.

2. **Mail Clients**:To set mail clients, do the following:



Mail Clients

Note Mail Client assignment to Blacklist/Whitelist may take up to 30 seconds to take effect.

Select Clients ● Blacklist ○ Whitelist

Unassigned

Search

iOS/6.1.3 (10B329) dataacces
iOS/6.1.4 (10B350) dataacces
Android/4.1.1-EAS-1.3
Apple-iPad3C3/902.206
TouchDown(MSRPC)/8.1.0005
MSFT-WP/8.0.10211
MSFT-PPC/5.2.1574
Test Agent
Apple-iPhone5C2/1002.350
Apple-iPhone5C2/1102.55400
SAMSUNGSPHD700/100
SAMSUNG-SPH-D700/100.20

Assigned

Search

SAMSUNG-GT-P7500/100.40
SAMSUNG-GT-N7100/100.40
TouchDown(MSRPC)/8.1.0002
MSFT-PPC/5.2.5001
SAMSUNG-GT-S7562/100.40

Manually Add Mail Client

If a device email client syncs with the Exchange Service, then the user agent is captured automatically but if a user agent never syncs with Exchange, then you need to add user agent using **Manually Add Mail Client**.

a. **Select Clients**:

   - **Blacklist** indicates that the selected user agents are not allowed. By default, **Blacklist** is selected.
   - **Whitelist** indicates that the selected user agents are allowed.

b. **Manually Add Mail Client**: Enter the Activesync mail client user agent name in the text field and click the **Add Agent** button to add the new clients into the list. In the confirmation message (Add Agent) that appears, click **OK** to continue.

   The added mail client appears in the Unassigned Mail client list. Use the Single right and the Single left- arrow icons to move individual entry from left to right and right to left columns respectively. Use the Double right-arrow icon and the Double left- arrow icon to move complete list from right to left and left to right columns respectively.
   The Email Client User Agent that is provided by '**Manually Add Mail Client**' in Exchange Settings should match exactly with the User Agent retrieved from the device.

   For example:

   a. Android NitroDesk TouchDown Email Client User Agent is TouchDown(MSRPC) /8.3.00036/. If the format matches exactly, the blacklisting works. If anything is missed in the same does not block the email client for devices having that email client user agent.

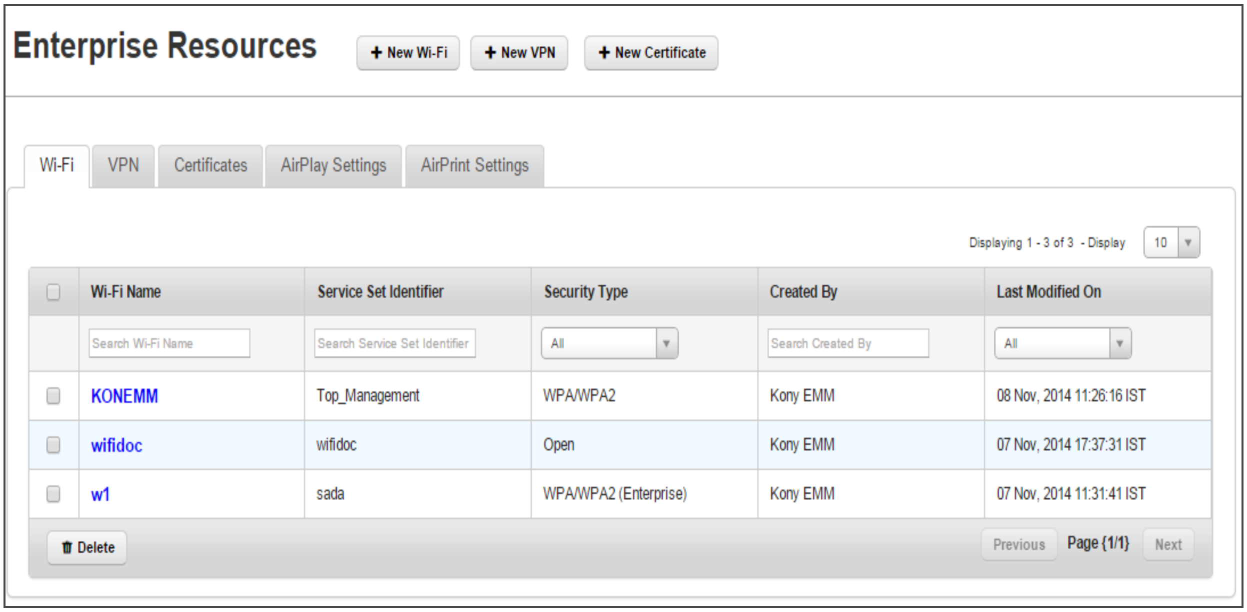
      Some email clients do not share User Agent ids and in that scenario the same cannot be blacklisted (example: NitroDesk TouchDown iOS).

3. Click the **Submit** button to save the configuration. In the confirmation message (Save Exchange Service Settings) that appears, click **OK** to return to the main page. A confirmation message appears at the bottom of the page above Submit.

6.6 Enterprise Resources

The Enterprise Resources settings in the Management Console configure Wi-Fi and VPN access for devices enrolled in your domain. There are three types of enterprise resources that you can configure: Wi-Fi, VPN and Certificates. These resources are made available to devices through the Network Policy and Certificate Distribution policy respectively.

From the **Settings** section, click **Enterprise Resources List** from the left panel. The Enterprise Resources page appears with a list of the enterprise resources details.



□	Wi-Fi Name	Service Set Identifier	Security Type	Created By	Last Modified On
	Search Wi-Fi Name	Search Service Set Identifier	All	Search Created By	All
□	KONEMM	Top_Management	WPA/WPA2	Kony EMM	08 Nov, 2014 11:26:16 IST
□	wifidoc	wifidoc	Open	Kony EMM	07 Nov, 2014 17:37:31 IST
□	w1	sada	WPA/WPA2 (Enterprise)	Kony EMM	07 Nov, 2014 11:31:41 IST

The Enterprise Resources List Page includes five tabs:

- Wi-Fi
- VPN
- Certificates
- AirPlay Settings
- AirPrint Settings

By default, Wi-Fi tab is set to active.

6.6.1 Wi-Fi

The list view displays a list of all the Wi-Fi networks along with other details. You can search Wi-Fi networks based on each column and also sort on each column.

The Wi-Fi List page displays the following columns:

Columns	Description
Wi-Fi Name	The name of this Wi-Fi network entry. This field is for your reference and should not match the SSID of the network
Service Set Identifier	The Wi-Fi network's SSID. This is the name that a network broadcasts to identify itself, and that computers use to join it. SSIDs are case-sensitive.
Security Type	Displays the types of security.
Created By	Displays the names of the Administrators.
Last Modified on	Displays when the Wi-Fi connection was last modified.

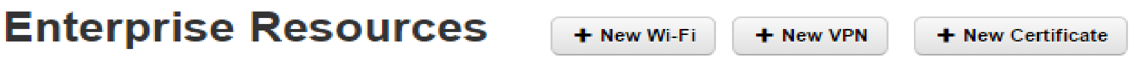
You can scroll the list view through the **Previous** and the **Next** buttons.

You can perform the following activities from the Wi-Fi page:

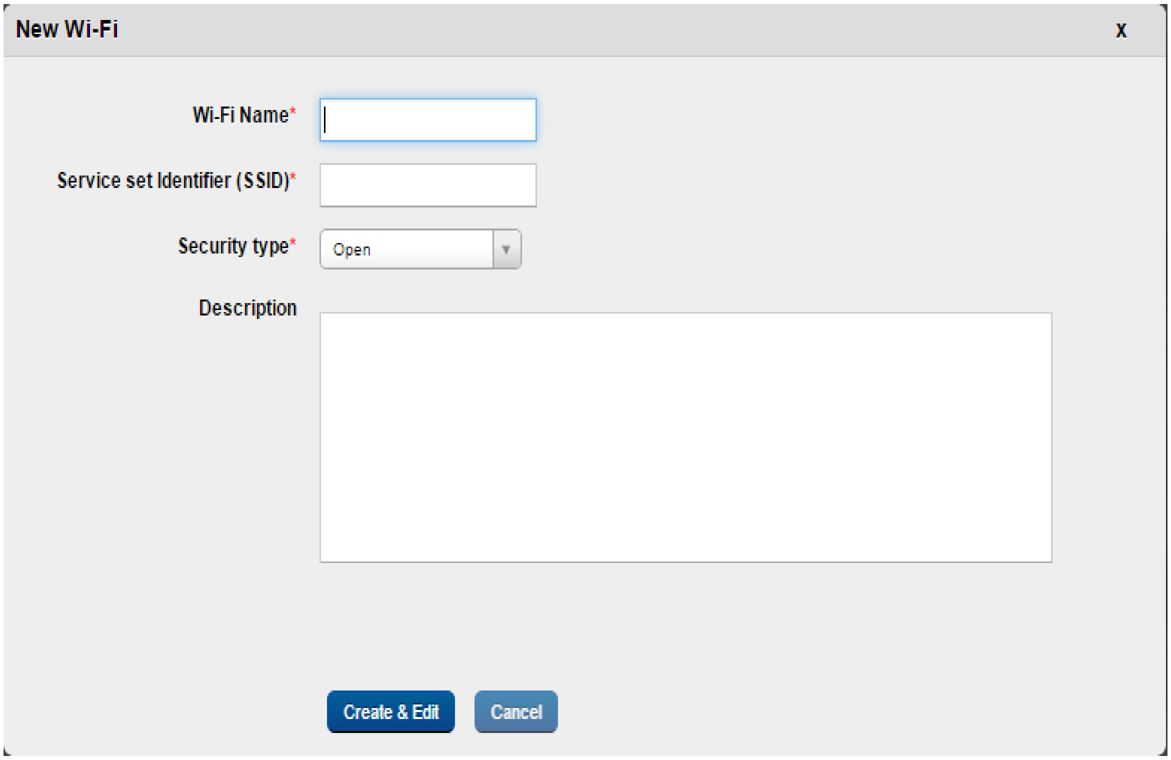
- Creating a Wi-Fi Connection
- Updating a Wi-Fi Connection
- Searching for Wi-Fi
- Deleting a Wi-Fi Connection

6.6.1.1 Creating a Wi-Fi Connection

To create a new Wi-Fi connection, follow these steps:



1. To open the **New Wi-Fi** window, click the **+ W- Fi button** next to the Enterprise Resources label at the top of the page.



Security type* Open

The **New Wi-Fi** window appears.

2. Enter the following details:

    a. **Wi-Fi Name**: Enter a valid name.

    b. **Service Set Identifier (SSID)**: Enter a unique name for the SSID.

c. **Security Type**: Select the required security type from the drop-down menu.

d. **Description**: Enter a brief and appropriate description.

3. Click the **Create** button.

   The newly created Wi-Fi appears in the list view.

4. Click the **Create and Edit** button to open the newly created Wi-Fi network.

   The Wi-Fi details page appears.

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

> *Important:* When an Android device is applied with a Wi-Fi policy that is a hidden network type, then the same hidden network is not configured on the device of a user.

Not all WiFi types are supported on all platforms. Based on the WiFi you select, features available for each platform may vary. See the table below for more information.

WiFi Type	Platform	Features/Fields
Open	iOS	Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Is this WiFi a hotspot.
	Android	No configuration required
	Windows	Security, Encryption type, Network Security Key, Key Index, Connect automatically, Connect even if non-broadcasting.

WiFi Type	Platform	Features/Fields
WEP	iOS	Password, Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Is this WiFi a hotspot.
	Android	Password
	Windows	This security type is not supported on the Windows platform.
WPA/WPA2	iOS	Password, Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Is this WiFi a hotspot.
	Android	Password
	Windows	Security, Encryption type, Network Security, Key, Key Index, Connect automatically, Connect even if non broadcasting, Enable FIPS (Federal Information Processing Standard).
Any (Personal)	iOS	Password, Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Is this WiFi a hotspot.
	Android	This security type is not supported on the Android platform.
	Windows	This security type is not supported on the Windows platform.

WiFi Type	Platform	Features/Fields
WEP (Enterprise)	iOS	Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Accepted EAP types, Identity Certificate, Username, Use per connection password, Password, Inner Authentication, Outer identity, Trusted certificates, Trusted certificate names, Is this WiFi a hotspot.
	Android	This security type is not supported on the Android platform.
	Windows	This security type is not supported on the Windows platform.

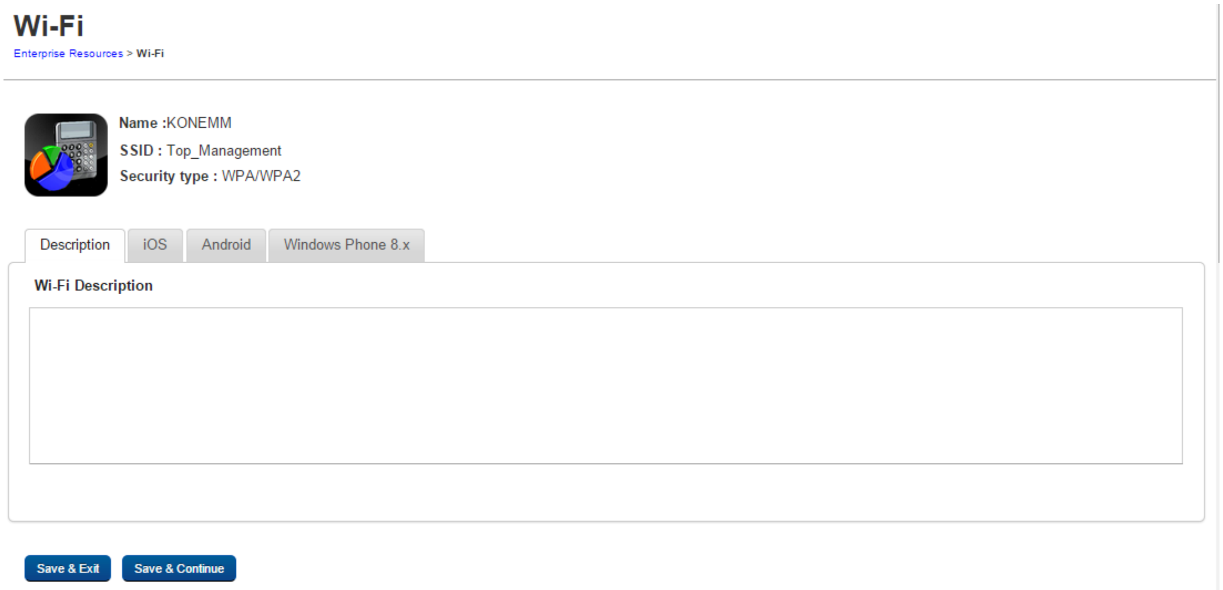
WiFi Type	Platform	Features/Fields
WPA/WPA2 (Enterprise)	iOS	Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Accepted EAP types, Identity Certificate, Username, Use per connection password, Password, Inner Authentication, Outer identity, Trusted certificates, Trusted certificate names, Is this WiFi a hotspot.
	Android	This security type is not supported on the Android platform.
	Windows	Security Type, Encryption Type, Connect Automatically Connect even if non-broadcasting, Network Authentication Method, Validate Server's identity certificate, Connect to these servers, Servers, Trusted Root CAs, Notifications before Connecting, Use Windows Log On Name, Enable Fast Reconnect, Enforce Network Access Protection, Crypto-Binding, Enable Identity, Privacy Anonymous Identity, Use EAP, Client Authentication Type, Enable Single Sign On, Single Sign On Type, Maximum Delay, Allow additional dialogs, Use Separate virtual LANs for Machine and User Authentication, PMK Caching, PMK Time to Live (minutes), Number of entries in PMK Cache, Use Pre-Authentication, Number of pre-auth attempts, Enable FIPS.

WiFi Type	Platform	Features/Fields
Any (Enterprise)	iOS	Auto Join, Proxy Type, Proxy Server Username, Proxy Server Address, Proxy Server Port, Proxy Server Password, Accepted EAP types, Identity Certificate, Username, Use per connection password, Password, Inner Authentication, Outer identity, Trusted certificates, Trusted certificate names, Is this WiFi a hotspot.
	Android	This security type is not supported on the Android platform.
	Windows	This security type is not supported on the Windows platform.

WiFi Type	Platform	Features/Fields
802.1X EAP	iOS	This security type is not supported on the iOS platform.
	Android	Use Two Factor Authentication, EAP Method, Phase 2 Authentication, CA Certificate, Identity Certificate, Identity, Anonymous Identity, Password. Your Android device must have a screen lock (Pin, password or pattern) for this WiFi type to function. If your device does not have a screen lock, this WiFi setting will be parked in the Messages section.
	Windows	Security Type, Encryption Type, Connect Automatically Connect even if non-broadcasting, Network Authentication Method, Use Strong Cipher Kets, Don't reveal permanent ID if pseudonym present, Enable usage of Realms, Realms, Use Simple Certificate Selection, Use a different Username for Connection, Cache User settings, Validate Server’s identity certificate, Connect to these servers, Servers, Trusted Root CAs, Don't prompt user if unable to authorize server. Notifications before Connecting, Use Windows Log On Name, Enable Fast Reconnect, Enforce Network Access Protection, Crypto-Binding, Enable Identity, Privacy Anonymous Identity, Use EAP, Client Authentication Type, Enable Fast Re authentication, Enable Single Sign On.

6.6.1.2 Updating a Wi-Fi Connection

To update a Wi-Fi, follow these steps:



Wi-Fi

Enterprise Resources > Wi-Fi

Name :KONEMM

SSID : Top_Management

Security type : WPA/WPA2

You can update details under four tabs, **Description**, **iOS**, **Android**, and Windows Phone 8.x. By default the **Description** tab is set to active.

- Description - Tab
- iOS - Tab
- Android - Tab
- Windows Phone 8.x

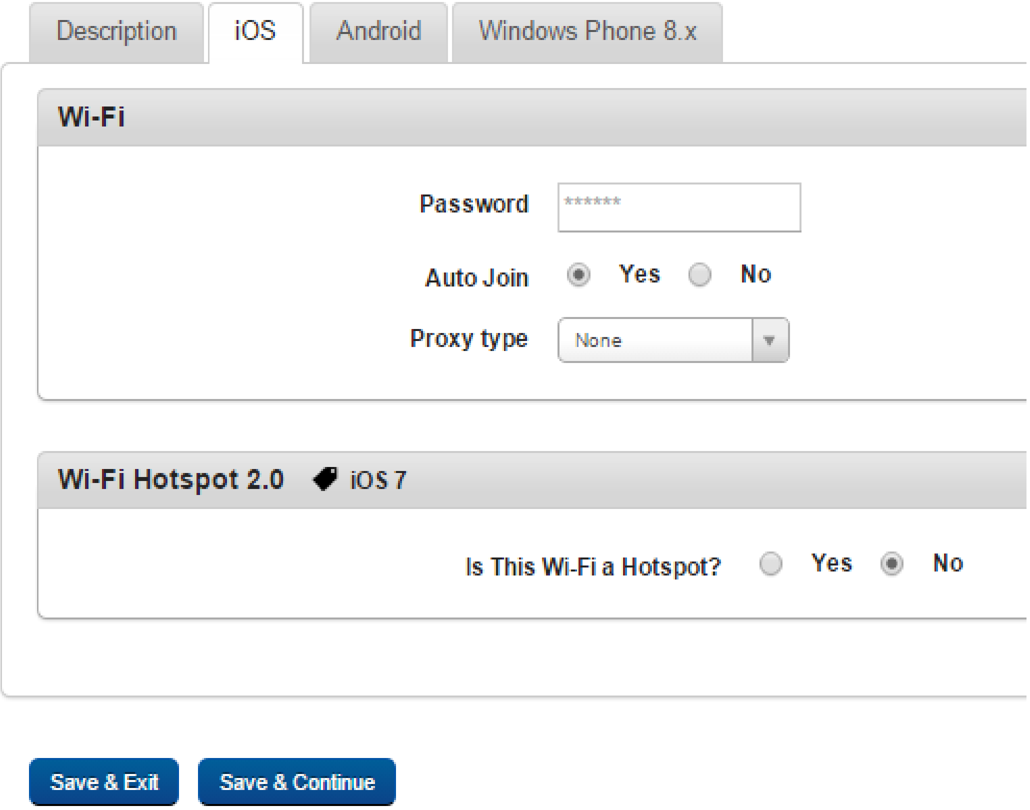
Description - Tab

1. Enter the appropriate description for the Wi-Fi or if required, update the existing content.

iOS - Tab

1. Set Wi-Fi configuration for iOS platform.

   Wi-Fi settings enhanced support for enabling the device to become a Wi-Fi hot spot using the device’s data connection.



Wi-Fi

Password ******

Auto Join ● Yes ○ No

Proxy type None

Wi-Fi Hotspot 2.0 iOS 7

Is This Wi-Fi a Hotspot? ○ Yes ● No

a. **Password**: Enter the password.

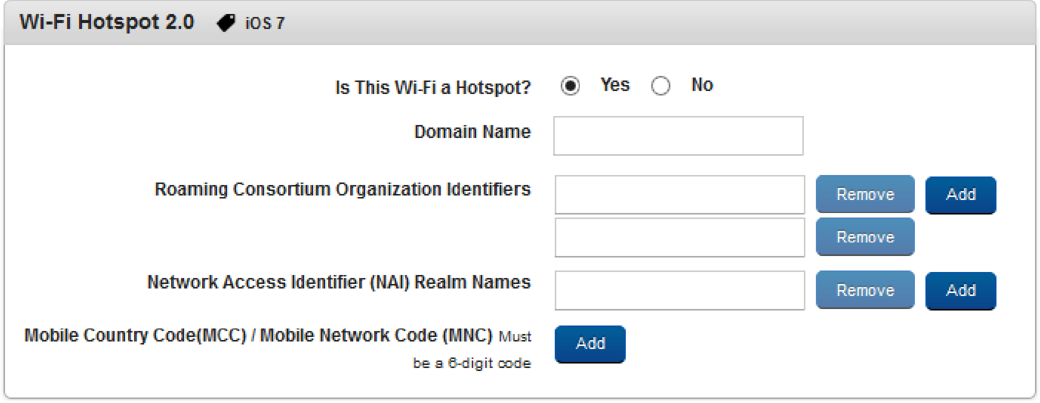
b. **Auto Join**: Based on prerequisite, select the option as Yes or No.

c. **Hidden Network**: If Auto Join is set toNo, this field is enabled. You can select Yes or No.

d. **Proxy Type**: Select the required option as None, Manual or Automatic from the drop-down menu.

2. **Wi-Fi Hot spot 2.0**

You can enable a Wi-Fi hot spot on your device by configuring the fields shown below.



Wi-Fi Hotspot 2.0 iOS 7

Is This Wi-Fi a Hotspot? ● Yes ○ No

Domain Name
Roaming Consortium Organization Identifiers
Remove
Add
Remove
Network Access Identifier (NAI) Realm Names
Remove
Add
Mobile Country Code(MCC) / Mobile Network Code (MNC) Must be a 6-digit code
Add

- **Is This Wi-Fi a Hot spot?**: By default this option is set to No. You can modify it to Yes. If it is yes, only then will the following fields above become active.

- **Domain Name**: Enter the domain name.

- **Roaming Consortium Organization Identifiers**: Click the **Add** button to add identifiers.

  Click the **Remove** button if you wish to remove added entries.

- **Network Access Identifier (NAI) Realm Names**: Click the **Add** button to add NAIs. Click the **Remove** button if you want to remove entries.

- **Mobile Country Code(MCC) / Mobile Network Code (MNC) Must be a 6-digit code**: Click the **Add** button to add MCC or MNC. Click the **Remove** button if you want to remove entries.

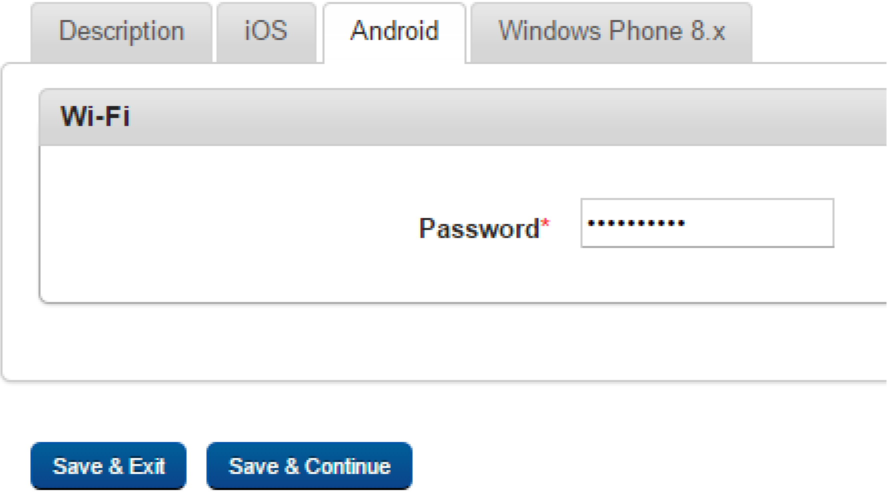
3. Click the **Save and Exit** button to save the changes and exit the page. The updated Wi-Fi network appears in the list view on the main page.

4. Click the **Save and Continue** button to save the details and update other details immediately.

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

Android - Tab

1. Set Wi-Fi configuration for the Android platform for the following fields:

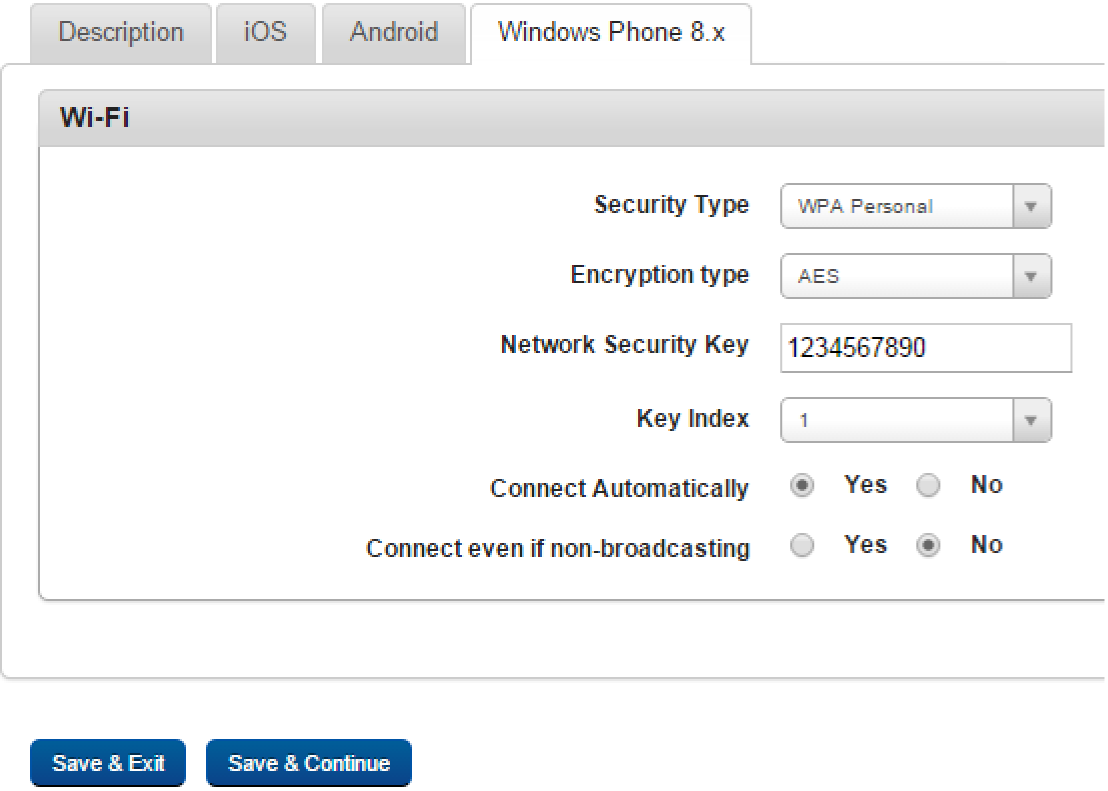


2. **Password**: Enter the password.
3. Click the **Save and Exit** button to save the changes and exit the page. The updated Wi-Fi network appears in the list view on the main page.
4. Click the **Save and Continue** button to save the details and update other details immediately.

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

Windows Phone 8.x Tab

Set Wi-Fi configuration for Windows Phone 8.x platform for the following fields.



Wi-Fi

Security Type: WPA Personal

Encryption type: AES

Network Security Key: 1234567890

Key Index: 1

Connect Automatically: ● Yes ○ No

Connect even if non-broadcasting: ○ Yes ● No

1. **Security Type**: Select a security type from the dropdown list.

2. **Encryption type**: Select an encryption type from the dropdown list.

3. **Network Security Key**: Enter a network security key.

4. **Key Index**: Select a key index value from the dropdown list.

5. **Connect Automatically**: By default this option is set to **No**. You can modify it to **Yes**.

6. **Connect even if non-broadcasting**: By default this option is set to **No**. You can modify it to **Yes**.

7. Click the **Save and Exit** button to save the changes and exit the page. The updated Wi-Fi network appears in the list view on main page.

8. Click the **Save and Continue** button to save the details and update other details immediately.

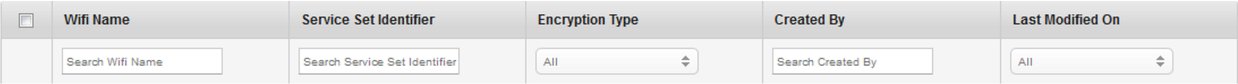
   Click the **Cancel** button to close the window.

You can access the newly added Wi-Fi for both the operating systems through following links:

- Device Policy>Network Policy>Set Network Policy for iOS.
- Device Policy>Network Policy>Set Network Policy for Android
- Device Policy>Network Policy>Set Network Policy for Windows 6.x devices
- Device Policy>Network Policy>Set Network Policy for Windows Phone 8.x devices

6.6.1.3 Searching for Wi-Fi

You can search for a desired Wi-Fi through the available search filters. You can apply a single filter or a combination of search filters to define the search criteria.



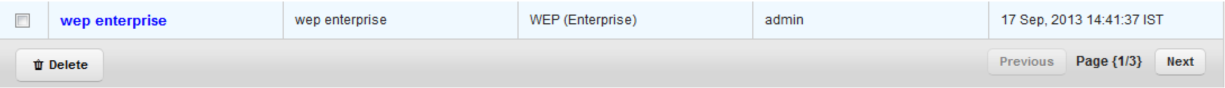
□	Wifi Name	Service Set Identifier	Encryption Type	Created By	Last Modified On
	Search Wifi Name	Search Service Set Identifier	All	Search Created By	All

To search for a Wi-Fi, follow these steps:

1. **Wi-Fi Name**: Enter a partial or complete name of the Wi-Fi in the **Search Wi-Fi Name** field.
2. **Service Set Identifier:** Enter a partial or complete name of the Service Set Identifier in the **Search Service Set Identifier** field.
3. **Encryption Type**: Select the required encryption type from the drop-down list.
4. **Created By**: Enter a partial or complete name of the administrator in the Created By field.
5. **Last Modified On**: Select the required time period from the drop-down menu when the Wi-Fi was last modified.
6. According to your search filters criteria, the list view is updated with the Wi-Fi connection details. By default, the list view displays 10 Wi-Fi connections according to the Display settings. You can modify the Display settings through the Display drop-down list. You can also scroll the list view through Previous and the Next button.

6.6.1.4 Deleting a Wi-Fi Connection

To delete a Wi-Fi connection, follow these steps:



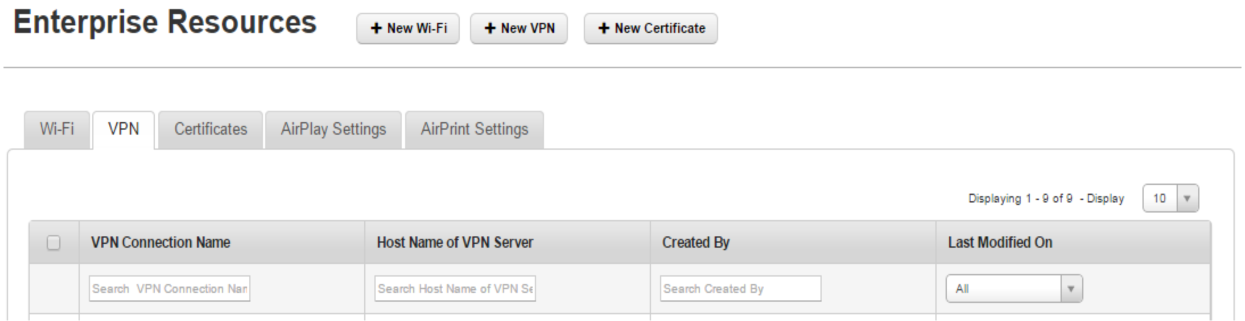
□	wep enterprise	wep enterprise	WEP (Enterprise)	admin	17 Sep, 2013 14:41:37 IST

1. Select the required Wi-Fi from the list view.

2. Click the **Delete** button. The deleted Wi-Fi is removed from the list view.

6.6.2 Virtual Private Network (VPN)

The list view displays a list of all VPN configurations along with other details. You can search VPN configurations based on each column and also sort the configurations based on each column.



□	VPN Connection Name	Host Name of VPN Server	Created By	Last Modified On
	Search VPN Connection Nar	Search Host Name of VPN Se	Search Created By	All

The Enterprise Resources List page displays the following columns:

Columns	Description
VPN Connection Name	Displays name for the VPN network entry
Host Name of VPN Server:	Displays full server host name of the server that provides access to the VPN
Created By	Displays the names of the administrators
Last Modified On	Displays when the VPN connection was last modified

You can scroll the list view through **Previous** and the **Next** button.

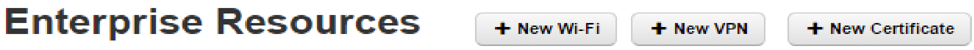
You can perform the following activities from the VPN page:

- Creating a VPN Connection
- Updating a VPN
- Assigning Per App VPN for iOS
- Searching for VPN
- Deleting a VPN Connection

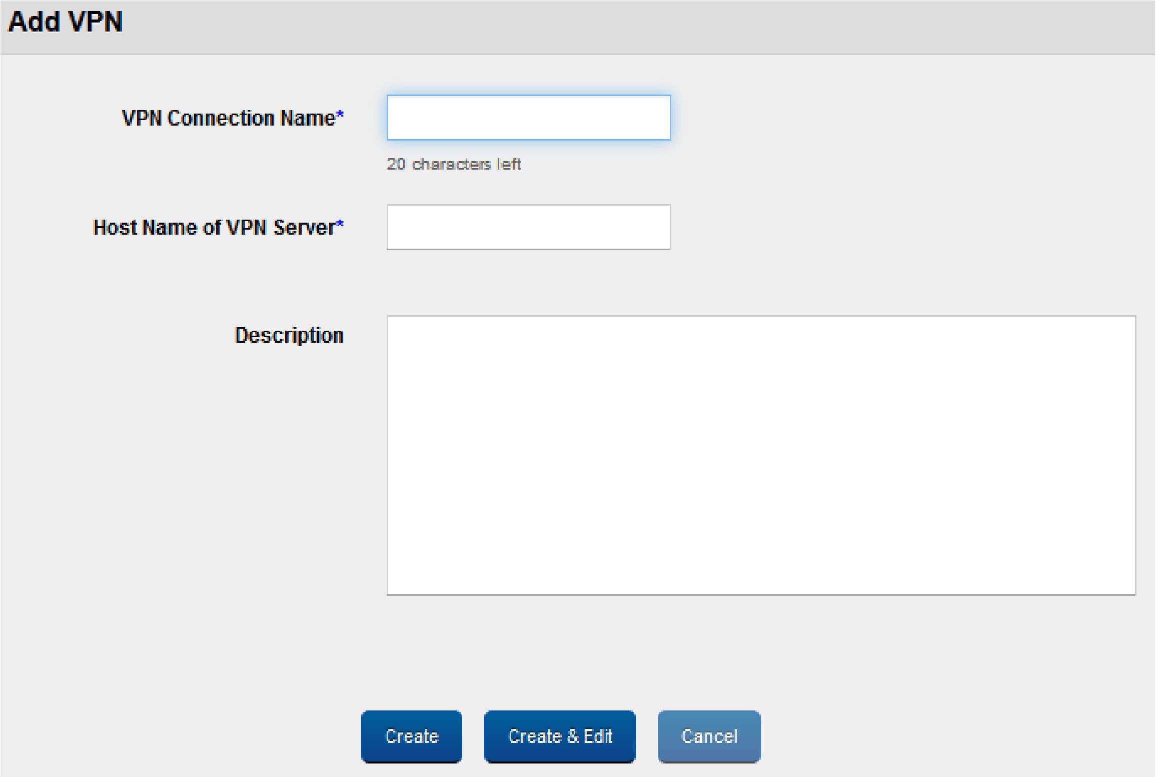
6.6.2.1 Creating a VPN Connection

To create a new VPN, follow these steps:

1. To open the **Add VPN** window, click the **+ New VPN** button next to the + New Wi-Fi button at the top of the page.

   The **Add VPN** window appears.



2. Enter the following details:
    a. **VPN Connecton Name**: Enter a valid name for this VPN Network entry.
    b. **Host Name of VPN Server:** Enter the full server host name that provides access to the VPN.
    c. **Description**: Enter a brief and appropriate description.
3. Click the **Create** button.

    The newly created VPN network appears in the list view.
4. Click the **Create and Edit** button to open the newly created VPN and edit the details.

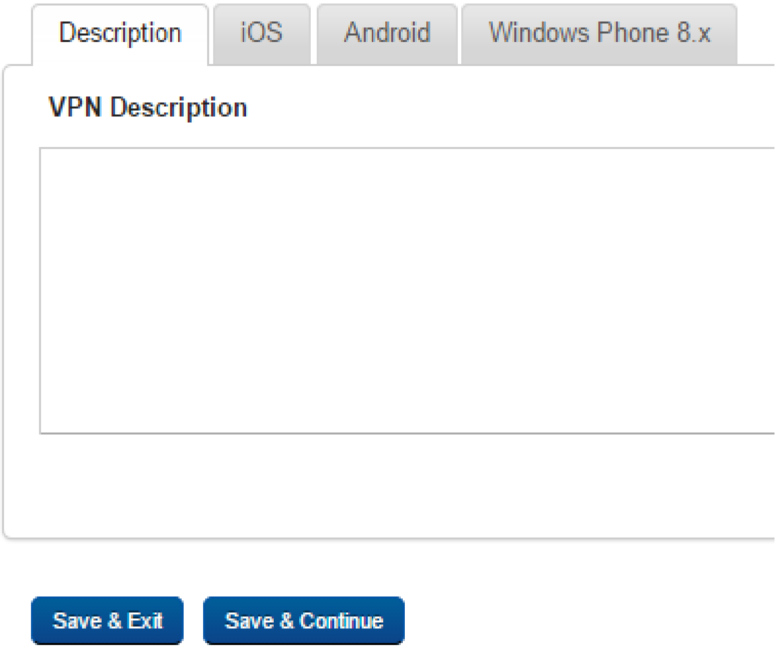
    Click the **Cancel** button to close the window.

6.6.2.2 Updating a VPN

You can update details under four tabs: Description, iOS, Android, and Windows Phone 8.x. By default the Description tab is set to active.

- Description
- iOS
- Android
- Window Phone 8.x

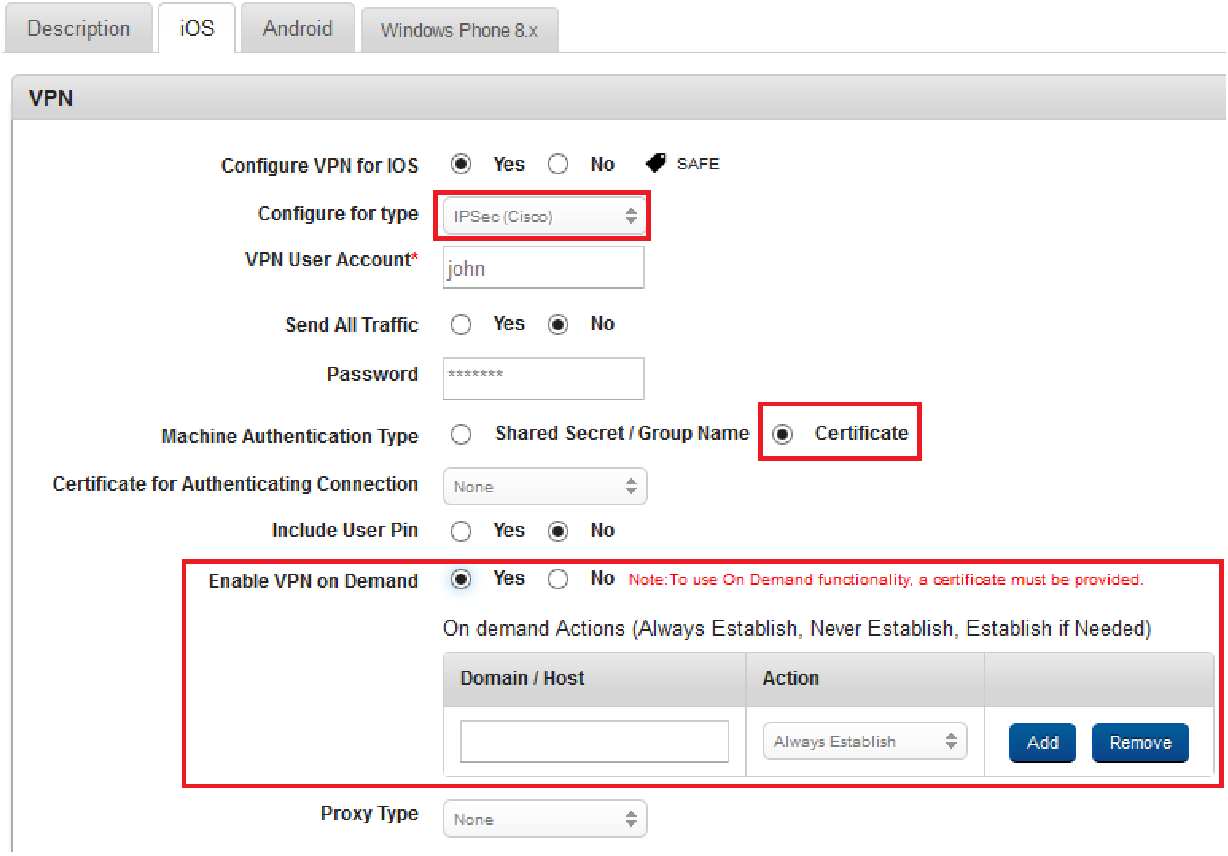
Description Tab



Enter the appropriate description for the VPN, or if required, update the existing content.

iOS Tab

The administrator can allow for On-Demand VPN to configure rules for VPN connections based on domains. Based on the domain accessed on a device, a VPN connection is established automatically.



Configure VPN for IOS	● Yes ○ No SAFE
Configure for type	IPSec (Cisco)
VPN User Account*	john
Send All Traffic	○ Yes ● No
Password	*******
Machine Authentication Type	○ Shared Secret / Group Name ● Certificate
Certificate for Authenticating Connection	None
Include User Pin	○ Yes ● No
Enable VPN on Demand	● Yes ○ No Note:To use On Demand functionality, a certificate must be provided.

On demand Actions (Always Establish, Never Establish, Establish if Needed)

Domain / Host	Action	
	Always Establish	Add Remove

Proxy Type	None

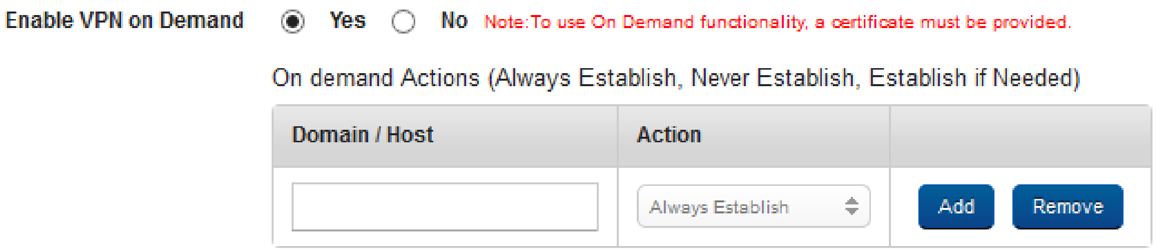
The Following are rules for VPN connections:

Administrators must enable On-Demand VPN. The administrator must specify which action should be performed by default among four actions:

- **Connect**: Unconditionally initiate a VPN connection on the next network attempt.
- **Disconnect**: Tear down the VPN connection, and do not reconnect on demand as long as the specified conditions match.
- **Ignore**: Leave any existing VPN connection up, but do not reconnect on demand as long as the specified conditions match.
- **Evaluate**: Provide the list of Domains to Connect to if needed and ones to never connect. The list of DNS Server IPs and Failure URL (if the system tries to connect to this and fails, the VPN connection is invoked).

To configure OnDemand VPN, follow these steps:

1. In Configure for Type, select from the list. Available options are L2TP, PPTP, IPSec(Cisco), Cisco AnyConnect, and IKEv2. For example, if you select CiscoAnyConnect, the following fields appear: VPN User Account, Group, and User Authentication.
2. Enter **VPN User Account** details.
3. Enter **Group** details.
4. In **User Authentication**, select the **Certificate** option.
5. In the **Certificate for Authenticating Connection** drop-down list, select one of the options.
6. For Enable **VPN on Demand**, select **Yes**.



Enable VPN on Demand ● Yes ○ No Note:To use On Demand functionality, a certificate must be provided.

On demand Actions (Always Establish, Never Establish, Establish if Needed)

Domain / Host	Action	
	Always Establish	Add Remove

   a. In the **Domain/Host**, enter domain details.

   b. In **Action**, select on of the actions from the list.

   Click the **Add** button to add more domains. Click the **Remove** button to remove added domain details.

When you select the IKEv2 (Internet Key Exchange protocol) type from the VPN list, in addition to the fields that are available for every other VPN type, a new section IKEv2 appears. The fields in the IKEv2 section follow:

Field	Description
Always-on VPN	Configure this to **Yes** if you want the VPN always on.
Disable Automatic Connection	Configure this to **Yes** if you want to disable a device from automatically connecting to the VPN.
Same Tunnel for Cellular & Wi-FI	Configure this to **Yes** to allow both the cellular and the Wi-Fi networks to use one tunnel.
Remote Address	Enter the remote IP address of the hostname of the VPN server.
Local Identifier	Enter details of the local identifier.
Remote Identifier	Enter details of the remote identifier.
Authentication Method	Select an authentication method for the VPN. Options are Shared Secret, and Certificate.
Shared Secret	Enter Shared Secret details. This option is available when you select **Shared Secret** from the Authentication Method type.
Certificate	Select the certificate from the available VPN certificates list. If you did not create any certificates, none will appear. This option is available when you select **Certificate** from the Authentication Method type.
Server Certificate Issuer Name	Enter the server certificate issuer name. This option is available when you select **Certificate** from the Authentication Method type.

Field	Description
Server Certificate Common Name	Enter the server certificate common name. This option is available when you select Certificate from the Authentication Method type.
Enable EAP (Extensible Authentication Protocol)	Select **Yes** to enable EAP.
EAP Authentication	Select the EAP authentication type from the list. The options are: UserName/Password and Certificate.
Auth Name	Enter the authentication user name. This option is available when you select UserName/Password from the EAP Authentication list.
Auth Password	Enter the authentication password. This option is available when you select UserName/Password from the EAP Authentication list.
Certificate	Select the certificate from the available EAP certificates list. If you did not create any certificates, none will appear. This option is available when you select Certificate from the EAP Authentication list.
Dead Peer Detection[1] Interval	Select the interval time for Dead Peer Detection interval. Options are: None, Low (1 hour), Medium (30 minutes), and High (10 minutes).

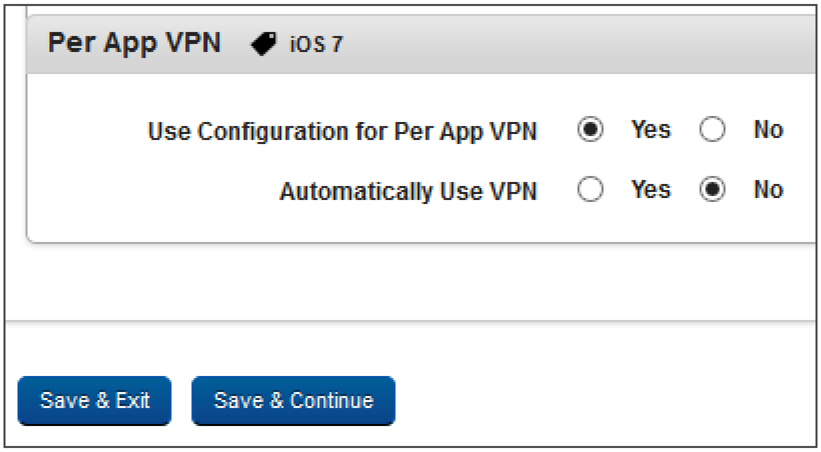
[1] Dead Peer Detection (DPD) detects a dead Internet Key Exchange (IKE) peer. The method uses IPsec traffic patterns to minimize the number of messages required to confirm the availability of a peer. DPD reclaims the lost resources if a peer is found dead, and it is also performs IKE peer failover.

Field	Description
Encryption Algorithm (IKE Security Association Parameters)	Select the encryption algorithm from the list. Options are: DES, 3DES, AES-128, and AES-256.
Integrity Algorithm (IKE Security Association Parameters)	Select the integrity algorithm from the list. Options are: SAH 1-96, SHA 1-160, SHA 2-256, SHA 2-384, and SHA 2-512.
Diffie Hellman Group[1] (IKE Security Association Parameters)	Select the Diffie-Hellman group from the list.
Lifetime in minutes (IKE Security Association Parameters)	Enter the lifetime of the IKE security in minutes.

[1] The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Field	Description
Encryption Algorithm (Child Security Association Parameters)	Select the encryption algorithm from the list. Options are: DES, 3DES, AES-128, and AES-256.
Integrity Algorithm (Child Security Association Parameters)	Select the integrity algorithm from the list. Options are: SAH 1-96, SHA 1-160, SHA 2-256, SHA 2-384, and SHA 2-512.
Diffie Hellman Group (Child Security Association Parameters)	Select the Diffie-Hellman group from the list.
Lifetime in minutes (Child Security Association Parameters)	Enter the lifetime of the IKE security in minutes.

Assigning Per App VPN for iOS



Per App VPN iOS 7

Use Configuration for Per App VPN ● Yes ○ No

Automatically Use VPN ○ Yes ● No

If a VPN is assigned by default, all communications to the Internet go through the VPN. VPNs are applied at the device level.

Per App VPN is an iOS 7 feature that allows administrators to assign VPNs at app level for enterprise apps, and public apps. If Per App VPN is assigned, all communications to the Internet go through the assigned Per App VPN.

> *Important:* Per App VPN is available only for the VPN type **Cisco AnyConnect**.

To assign a Per App VPN to an app, the "**Use Configuration for Per App VPN**' must be **Yes**. Only then can Per App VPN can be assigned to an app.

To define Per App VPN to an app, follow these steps:

Per App VPN must be defined while creating a new VPN or updating a VPN. Ensure that a VPN is configured before defining Per App VPN. For more details, refer to Creating VPN.

1. Click one of the VPNs in the VPN list page.
2. In the VPN details page, click **iOS** tab.

   > *Important:* Ensure that the Configure for Type field is **Cisco AnyConnect**.

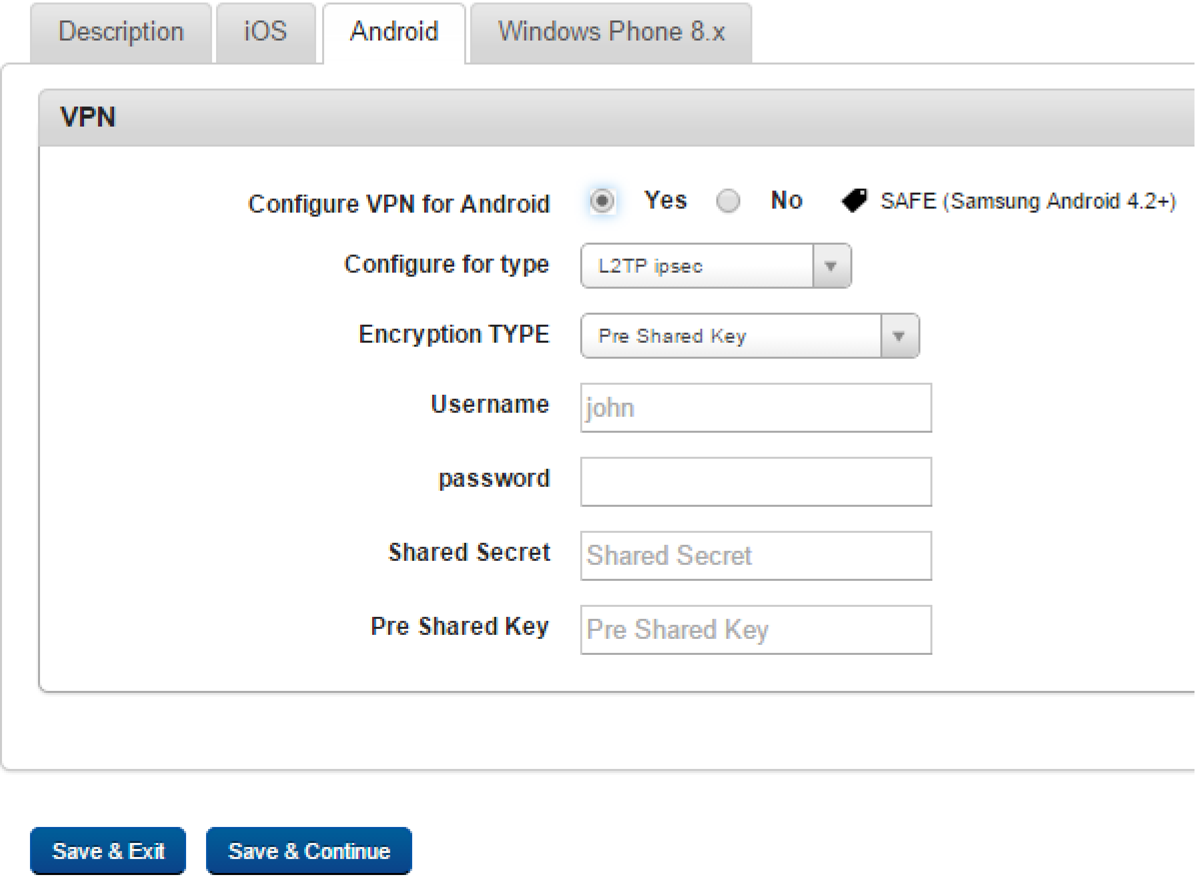
3. Navigate to the **Per App VPN** section, and choose **Yes** for the **Use Configuration for Per App VPN** option.

   Only if the **Use Configuration for Per App VPN** is set to **Yes** will system display the Automatically Use VPN options. By default the **Use Configuration for Per App VPN** is set to No. Admin can also choose whether the assigned VPN to be started automatically.

4. If you want Per App VPN to start automatically, choose **Yes** for the **Automatically Use VPN**.

   If the **Automatically Use VPN** option is set to **No**, the device user is asked to manually choose for the assigned Per App VPN while accessing Internet from the device.

Android Tab



Configure VPN for Android ● Yes ○ No SAFE (Samsung Android 4.2+)

Configure for type: L2TP ipsec

Encryption TYPE: Pre Shared Key

Username: john

password:

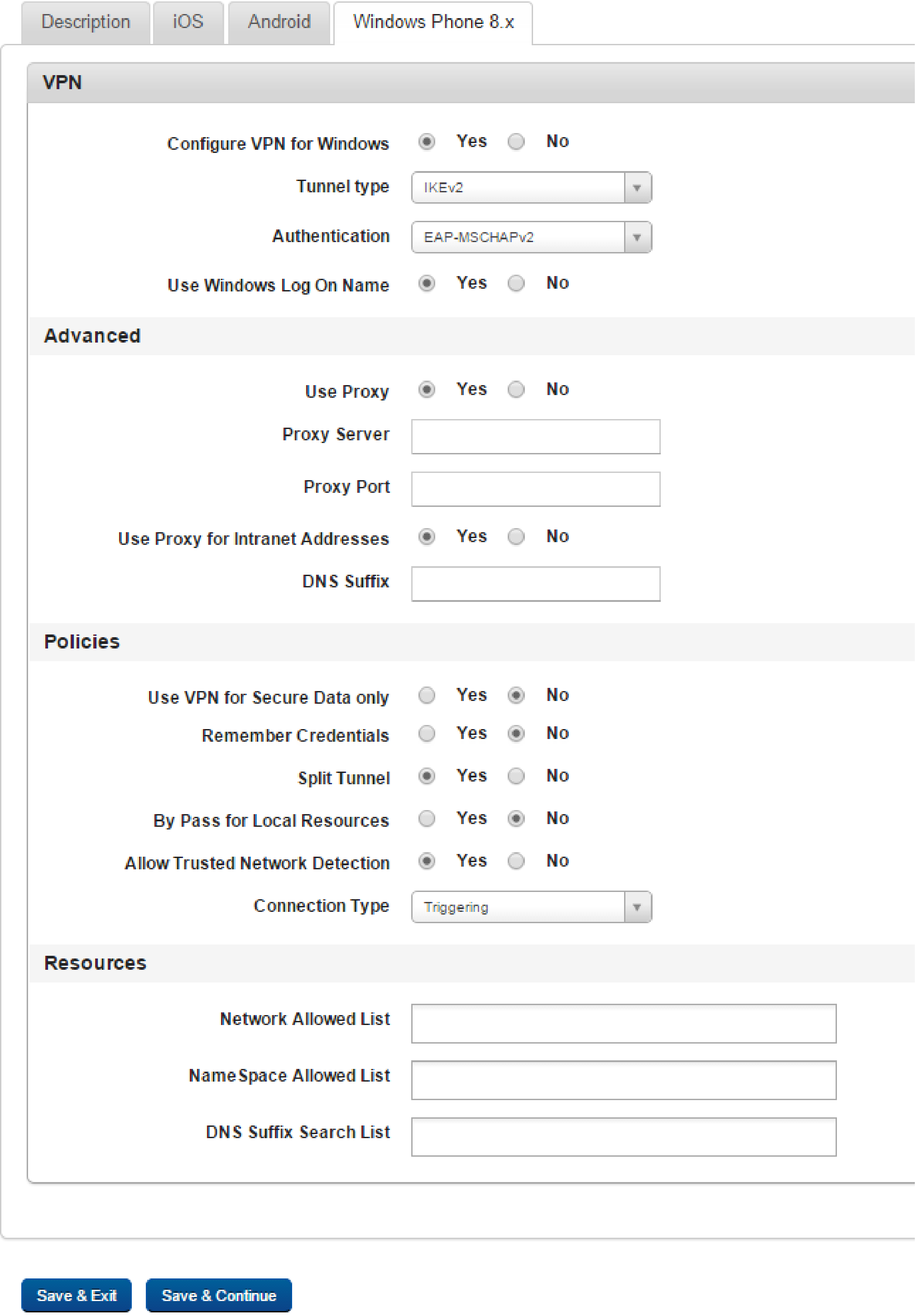
Shared Secret: Shared Secret

Pre Shared Key: Pre Shared Key

- **Configure VPN for Android**: By default, this is set to **No**. To configure VPN for SAFE (Samsung Android 4.2+) enabled devices, select **Yes**. Setting this yes will enable options below.
  - **Configure for type**: Two configurations types are supported. Select an option from the drop-down list.
  - **Encryption TYPE**: Select an encryption type from the drop-down list.
  - **Username**: Enter your VPN user name.
  - **password**: Enter your VPN password.

- **Shared Key:** Enter your Shared Key details.
- **Pre Shared Key**: Enter your pre-shared key details.

Windows Phone 8.x Tab



VPN

Configure VPN for Windows ● Yes ○ No

Tunnel type: IKEv2

Authentication: EAP-MSCHAPv2

Use Windows Log On Name ● Yes ○ No

Advanced

Use Proxy ● Yes ○ No

Proxy Server

Proxy Port

Use Proxy for Intranet Addresses ● Yes ○ No

DNS Suffix

Policies

Use VPN for Secure Data only ○ Yes ● No

Remember Credentials ○ Yes ● No

Split Tunnel ● Yes ○ No

By Pass for Local Resources ○ Yes ● No

Allow Trusted Network Detection ● Yes ○ No

Connection Type: Triggering

Resources

Network Allowed List

NameSpace Allowed List

DNS Suffix Search List

- VPN
  - **Configure VPN for Windows**: By default this is set to **No**. If you want to configure VPN for Windows, select **Yes**. Setting this value to yes will enable all the options below. If you set this value to No, you will not see the options below.
  - **Tunnel type**: Select a tunnel type. For now, only IKEv2 is supported.
  - **Authentication**: Select an authentication type from the drop-down list.
  - **Use Windows Log On Name**: Select whether to use windows log on name or not. By default, this is set to **Yes**.
- Advanced
  - **Use Proxy**: By default, this is set to **Yes**. If you do not want to use a proxy server, set this to **No**.
  - **Proxy Server**: Enter your proxy server host name or IP address.
  - **Proxy Port**: Enter your proxy port number.
  - **Use Proxy for Intranet Addresses**: Choose whether to use proxy for intranet addresses or not. By default, this is set to **Yes**.
  - **DNS Suffix**: Enroll DNS suffix details.
- Policies
  - **Use VPN for Secure Data only**: By default this is set to **No**. If you want to use VPN for secure data, select **Yes**. Options below are enabled when you set this option to yes.
  - **Remember Credentials**: By default this is set to **No**. You can select **Yes**.
  - **Split Tunnel**: By default this is set to **Yes**. If you do not want to splint tunnel, select **No**.

> *Note:* When you select **No**, a warning appears. All network traffic will be forced through this VPN. It is recommended to whitelist the EMM Server else if an invalid VPN configuration is pushed, all communication to and from the device will fail, leaving the device permanently offline.

  - **By Pass for Local Resources**: By default this is set to **No**. Select **Yes** if you want to bypass VPN for local resources.
  - **Allow Trusted Network Detection**: By default, this is set to **Yes**. You can select **No**.
  - **Connection Type**: Choose a connection type from drop-down list. Available options are Triggering and Manual.
- Resources
  - **Network Allowed List/Excluded Network list**: Enter network allowed or excluded list. If you chose **Split Tuner** to **Yes**, **Allowed** appears, if you chose **No**, **Excluded** appears.
  - **NameSpace Allowed List/Excluded NameSpace List**: Enter name space allowed or excluded list here. If you chose **Split Tuner** to **Yes**, **Allowed** appears, if you chose **No**, **Excluded** appears.
  - **DNS Suffix Search List**: Enter DNS suffix search list details.

6.6.2.3 Searching for VPN

You can search a desired VPN connection through search filters available. You can apply a single search filter or a combination of search filters to define the search criteria and refine the outcome.

To search for a VPN connection, follow these steps:

1. **VPN Connection Name**: Enter a partial or complete name of the VPN in the **Search VPN Connection Name** field.
2. **Host Name of the VPN Server**: Enter a partial or complete name of the Service Set Identifier in the **Search Service Set Identifier** field.

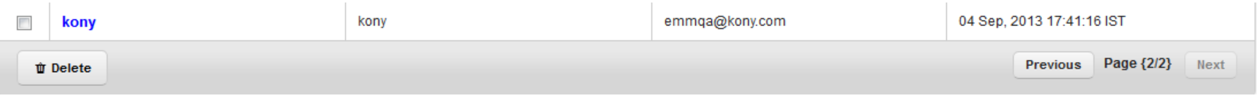
3. **Created By**: Enter a partial or complete name of the administrator in the **Search Created By** field.

4. **Last Modified on**: Select the required time period from the drop-down list when the VPN connection was last modified.

5. According to your search filters criteria, the list view is updated with respective VPN connection details. By default, the list view displays 10 VPN connections according to the Display settings, which you can modify through the Display drop-down list. You can also scroll the list view through Previous and the Next button.

6.6.2.4 Deleting a VPN Connection

To delete a VPN, follow these steps:



□	kony	kony	emmqa@kony.com	04 Sep, 2013 17:41:16 IST

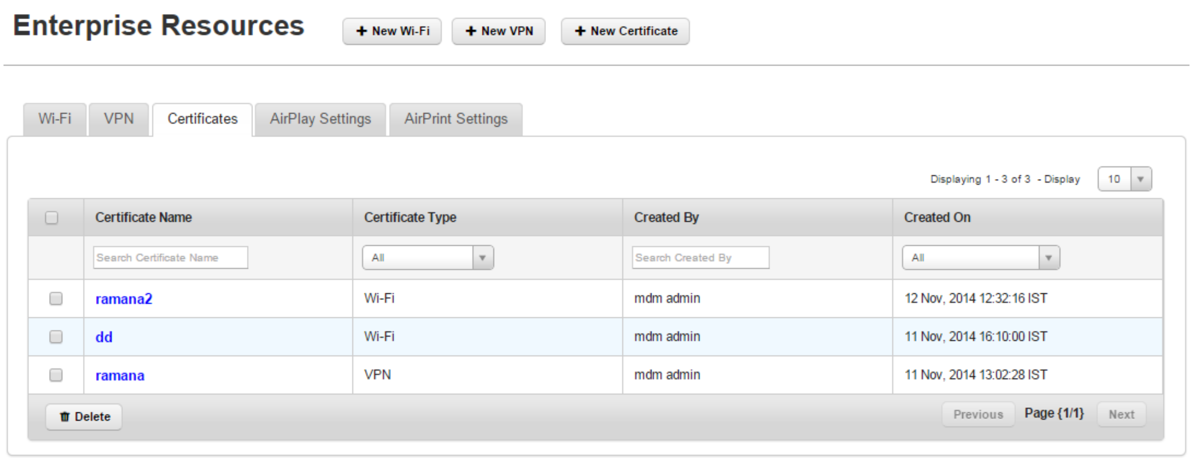
1. Select the required VPN connection from the list view.

2. Click the **Delete** button.

   The deleted VPN is removed from the list view.

6.6.3 Certificates

The list view displays a list of all the Certificates along with other details. You can search Certificates based on each column and also sort on each column.



□	Certificate Name	Certificate Type	Created By	Created On
□	ramana2	Wi-Fi	mdm admin	12 Nov, 2014 12:32:16 IST
□	dd	Wi-Fi	mdm admin	11 Nov, 2014 16:10:00 IST
□	ramana	VPN	mdm admin	11 Nov, 2014 13:02:28 IST

The Certificates page displays the following columns:

Columns	Description
Certificate Type	Displays the Certificate Name.
Certificate Name	Displays the type of Certificate, such as VPN.
Created By	Displays the name of the Administrator who created the Certificates.
Created on	Displays the date on which the Certificate was created.

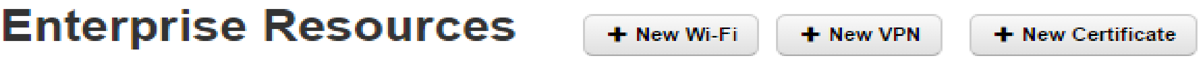
You can scroll the list view through the **Previous** and the **Next** buttons.

You can perform the following activities from the Certificates page:

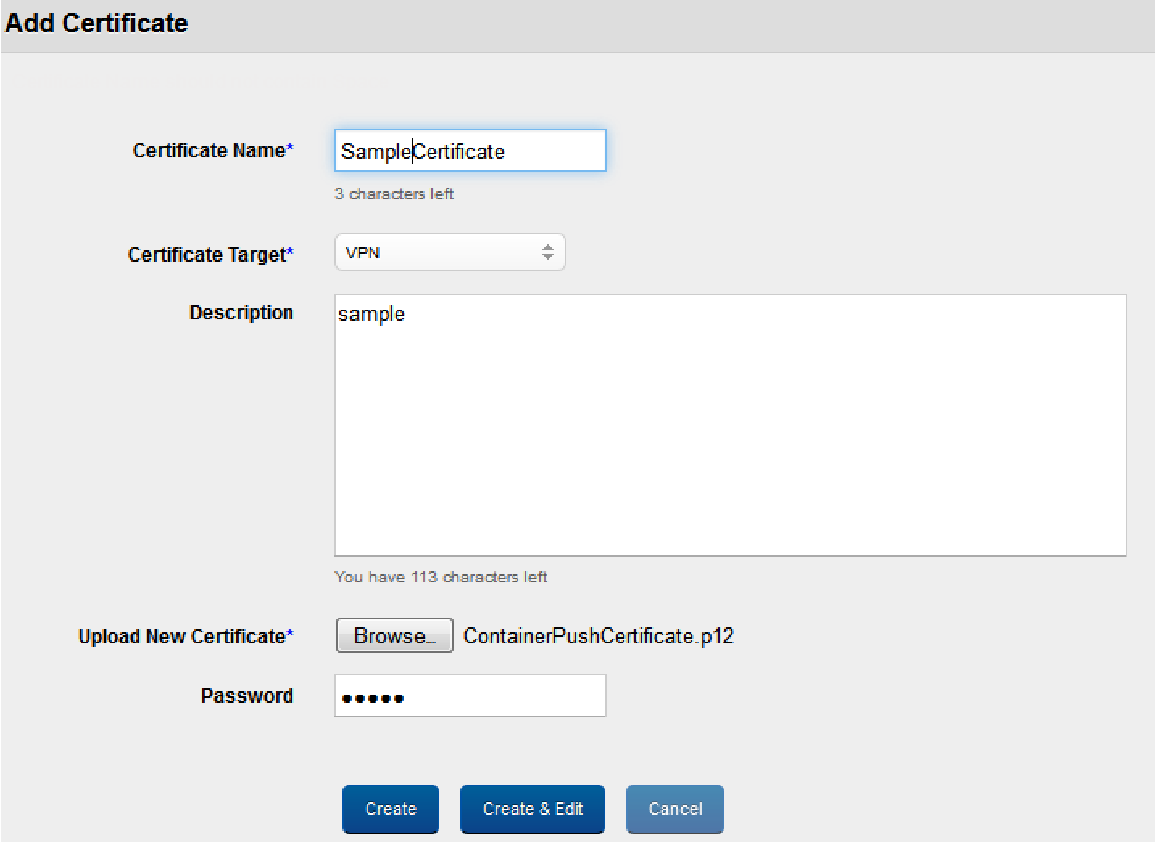
- Creating a Certificate
- Updating a Certificate
- Searching for Certificates
- Deleting a Certificate

6.6.3.1 Creating a Certificate

To create a new Certificate, follow these steps:



1. To open the **Add Certificate** window click the **+ New Certificate** button next to the + New VPN button at the top of the page.


Add Certificate

Certificate Name*: SampleCertificate
3 characters left

Certificate Target*: VPN

Description: sample
You have 113 characters left

Upload New Certificate*: Browse... ContainerPushCertificate.p12

Password: •••••

The **Add Certificate** window appears.

2. Enter the following details:

   a. **Certificate Name**: Enter a valid name for this Certificate entry.

   > *Note:* Ensure that the length of the certificate name is maximum 15 characters.

   b. **Certificate Target**: Select the required target from the drop-down list.

c. **Description**: Enter a brief and appropriate description.

d. **Upload New Certificate**: Click the Browse button to select the certificate from its location. The certificate with its name appears.

e. **Password**: Enter the password to protect the certificate.

3. Click the **Create** button.

   The newly created Certificate appears in the list view.

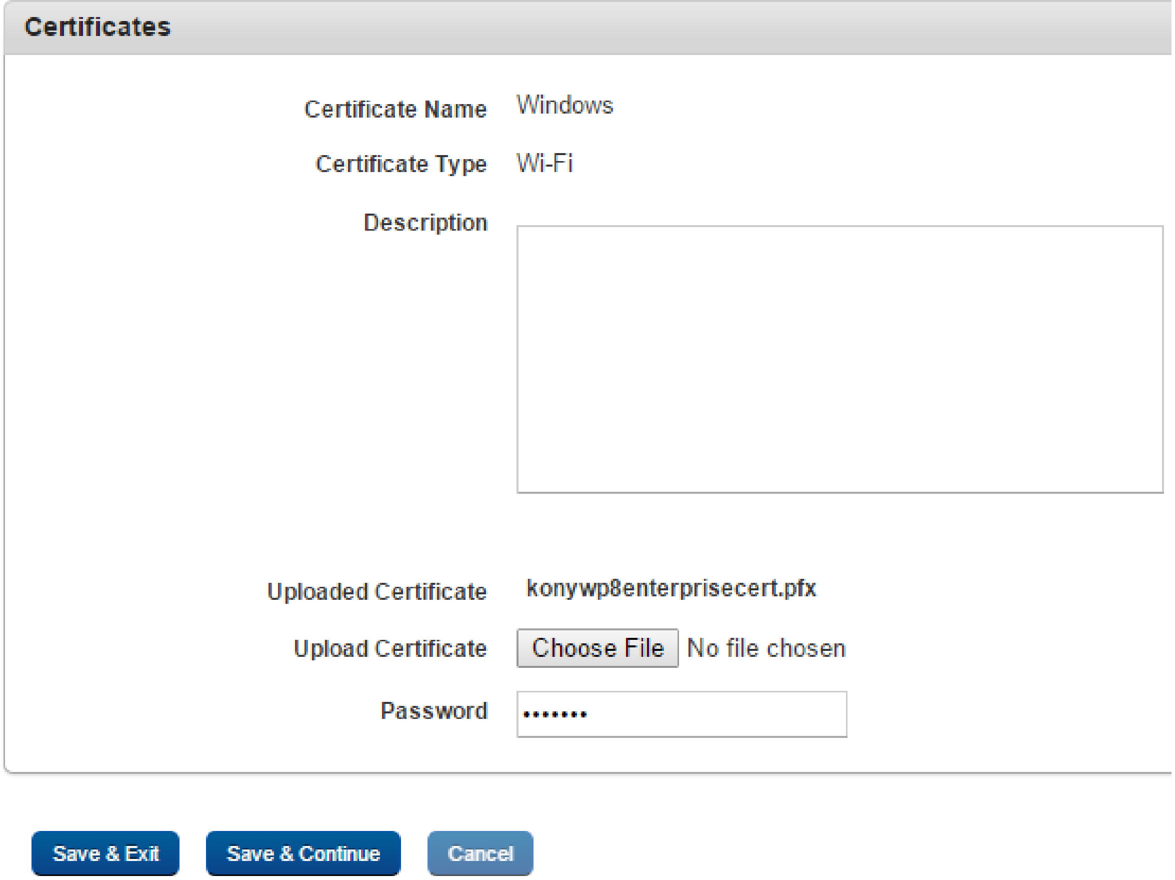
4. Click the **Create and Edit** button to open the newly created Certificate to update any details.

   The Certificate details page appears.

6.6.3.2 How to Update a Certificate

You can update details of certificates.

To update a Certificate, follow these steps:



Certificates

Certificate Name	Windows
Certificate Type	Wi-Fi
Description	
Uploaded Certificate	konywp8enterprisecert.pfx
Upload Certificate	Choose File No file chosen
Password	•••••••

1. **Upload New Certificate**: To select the certificate from its location click **Browse**. The certificate with its name appears.

2. **Password**: Enter the certificate password.

3. Click **Save & Exit** to save the changes and exit the page. or

4. Click **Save & Continue** to save the changes and stay on the same page.

6.6.3.3 Searching for Certificates

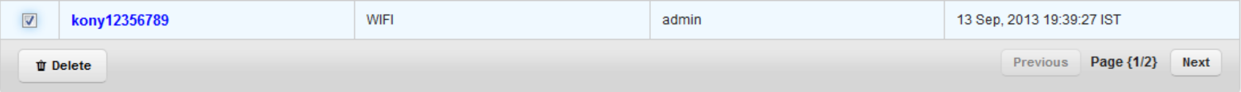
You can search a desired Certificate through search filters available. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome.

To search for a Certificate, follow these steps:

1. **Certificate Name**: Enter partial or complete name of the Certificate in the **Search Certificate Name** field.
2. **Search Certificate Type**: Enter partial or complete name of the certificate type in the **Search Certificate Type** field.
3. **Created By**: Enter partial or complete name of the Administrator in the **Search Created By** field.
4. **Created On**: Select the required time period from the drop-down list when the Certificate was created.
5. According to your search filters criteria, the list view is updated with respective Certificate details. By default, the list view displays ten certificates 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.

6.6.3.4 Deleting a Certificate

To delete a Certificate, follow these steps:



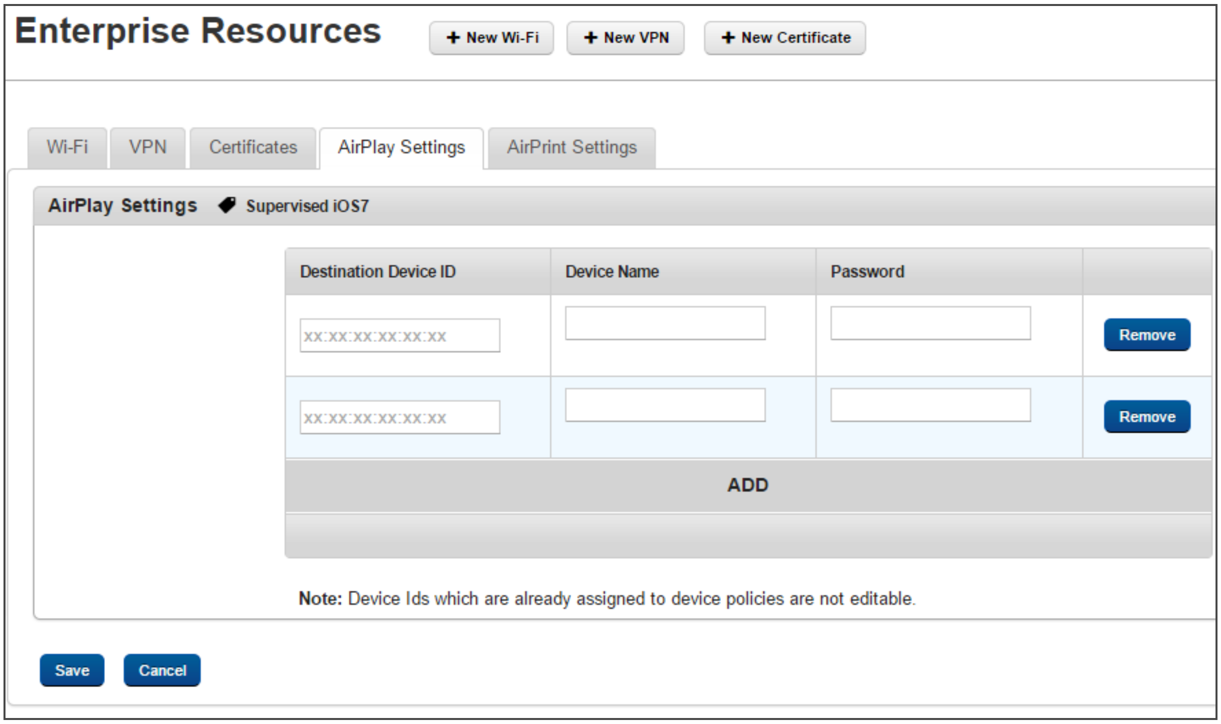
☑	kony12356789	WIFI	admin	13 Sep, 2013 19:39:27 IST

1. Select the required Certificate from the list view.
2. Click the **Delete** button.

   The deleted Certificate is removed from the list view.

6.6.4 AirPlay Settings

Through Airplay, you connect screen sharing between your iOS 7+ device and Apple TV or Mac. Configure the settings for destination device ID and password.

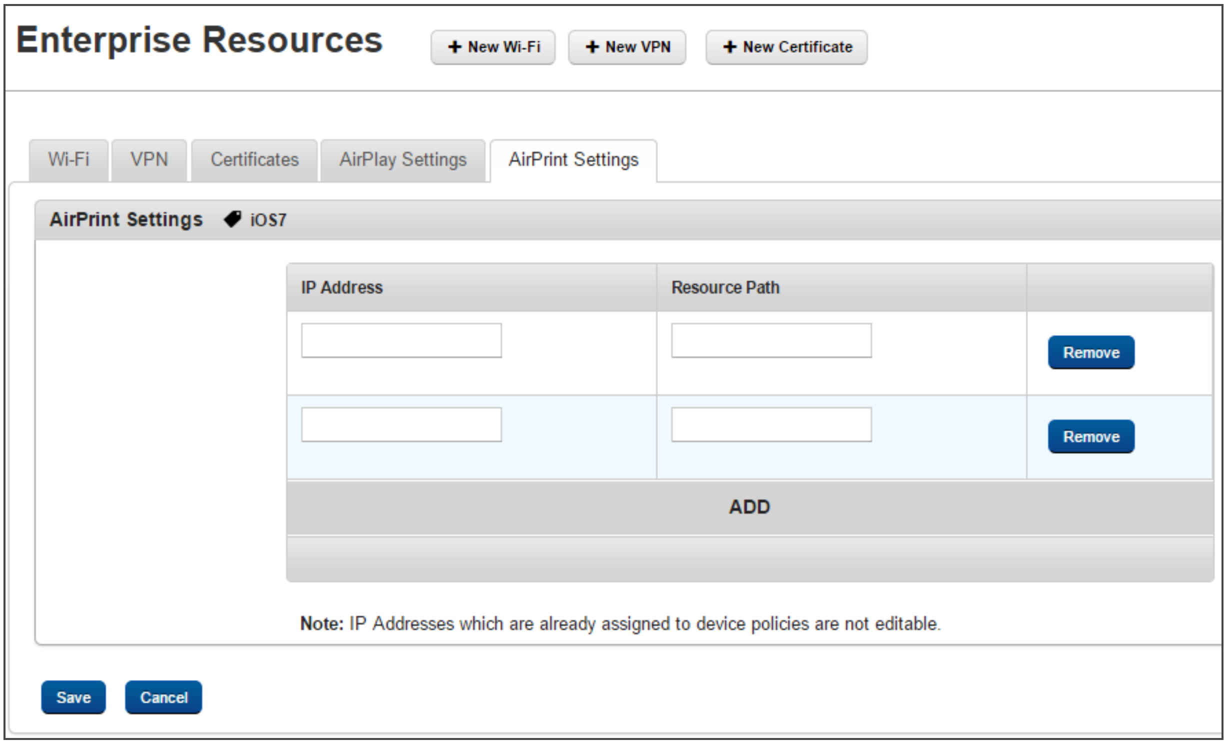


Destination Device ID	Device Name	Password	
xx:xx:xx:xx:xx:xx			Remove
xx:xx:xx:xx:xx:xx			Remove

Note: Device Ids which are already assigned to device policies are not editable.

6.6.5 AirPrint Settings

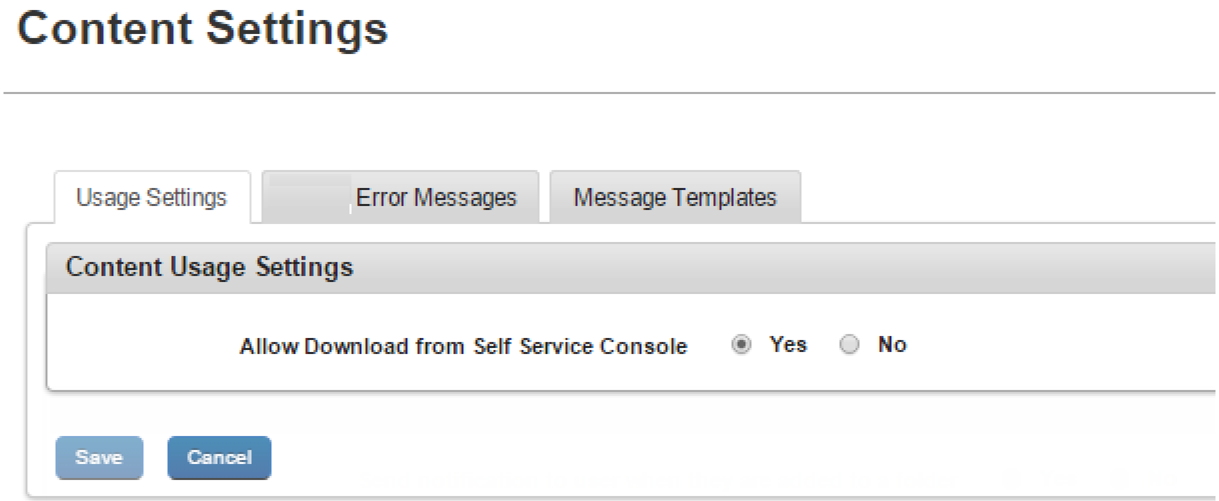
Using AirPrint, you can print from your iOS7+ device. Configure the settings for IP addresses and resource path.



Note: IP Addresses which are already assigned to device policies are not editable.

6.7 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.



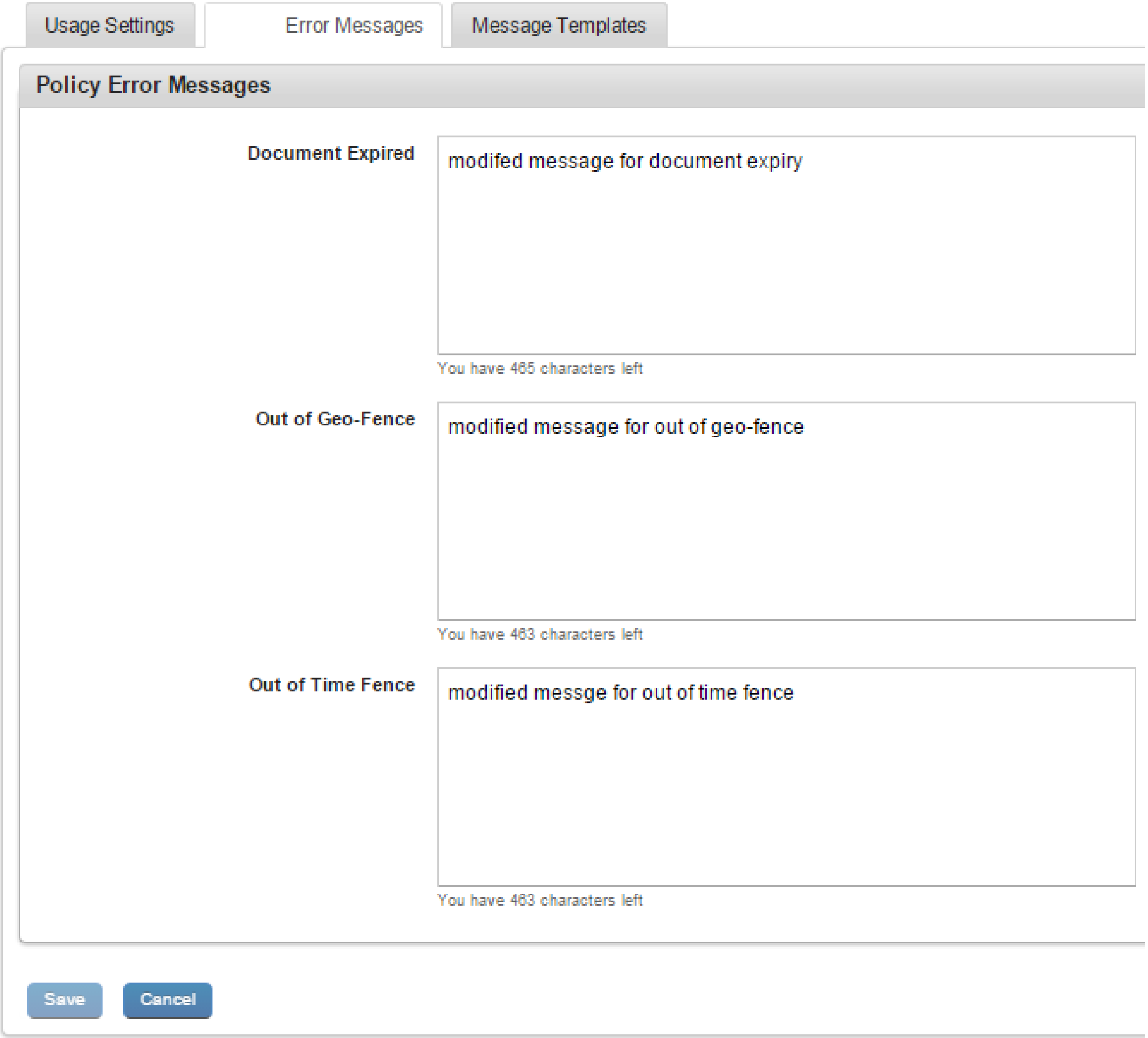
Content Settings

Content Usage Settings

Allow Download from Self Service Console ● Yes ○ No

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**.



Policy Error Messages

Document Expired: modifed message for document expiry

You have 465 characters left

Out of Geo-Fence: modified message for out of geo-fence

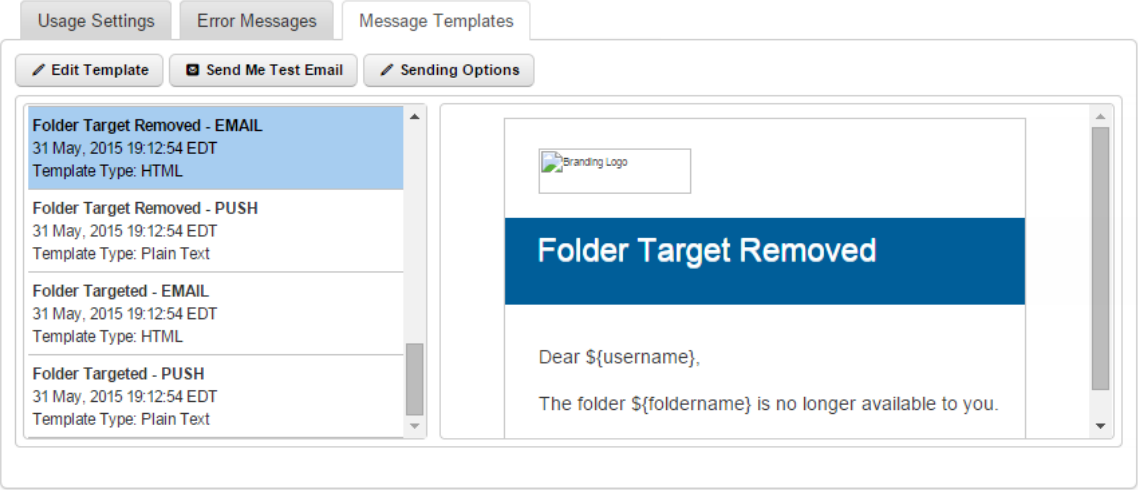
You have 463 characters left

Out of Time Fence: modified messge for out of time fence

You have 463 characters left

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



Folder Target Removed - EMAIL
31 May, 2015 19:12:54 EDT
Template Type: HTML

Folder Target Removed - PUSH
31 May, 2015 19:12:54 EDT
Template Type: Plain Text

Folder Targeted - EMAIL
31 May, 2015 19:12:54 EDT
Template Type: HTML

Folder Targeted - PUSH
31 May, 2015 19:12:54 EDT
Template Type: Plain Text

Folder Target Removed

Dear ${username},

The folder ${foldername} is no longer available to you.

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

6.7.0.1 Editing a Template

The Admin can edit pre-defined templates. The placeholder tags must not 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.

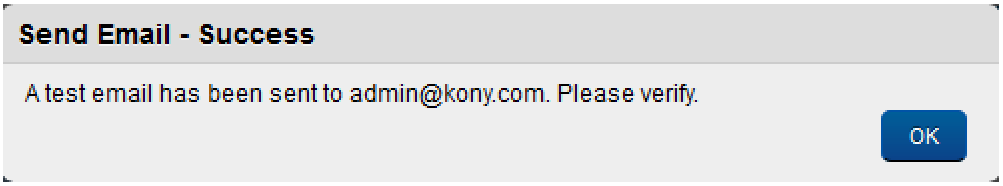
6.7.0.2 Sending a Test Email

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.*"

   
   Send Email - Success
   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.

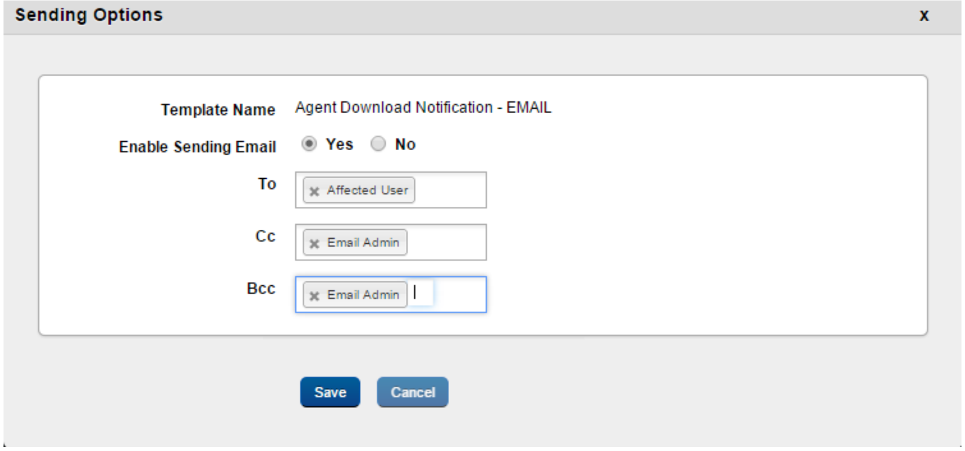
6.7.0.3 Configuring Sending Options

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.



Sending Options

Template Name: Agent Download Notification - EMAIL

Enable Sending Email: ● Yes ○ No

To: Affected User

Cc: Email Admin

Bcc: Email Admin

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**.

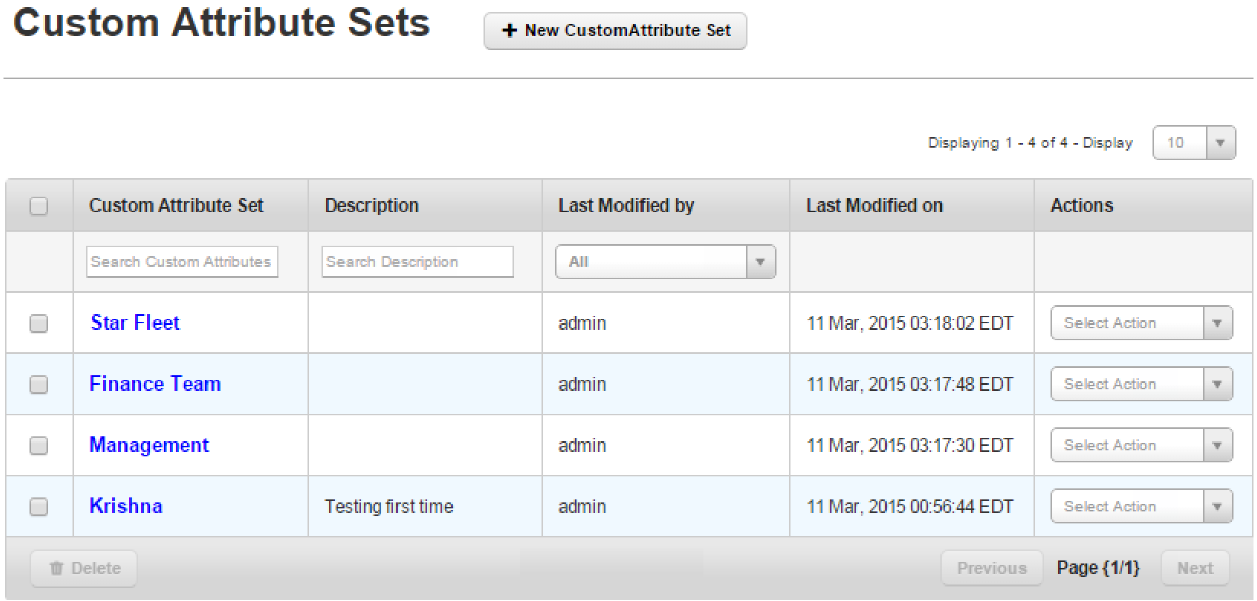
6.8 Custom Attribute Sets

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 Set	Description	Last Modified by	Last Modified on	Actions
	Search Custom Attributes	Search Description	All		
□	Star Fleet		admin	11 Mar, 2015 03:18:02 EDT	Select Action
□	Finance Team		admin	11 Mar, 2015 03:17:48 EDT	Select Action
□	Management		admin	11 Mar, 2015 03:17:30 EDT	Select Action
□	Krishna	Testing first time	admin	11 Mar, 2015 00:56:44 EDT	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.

6.8.1 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.

6.8.2 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.

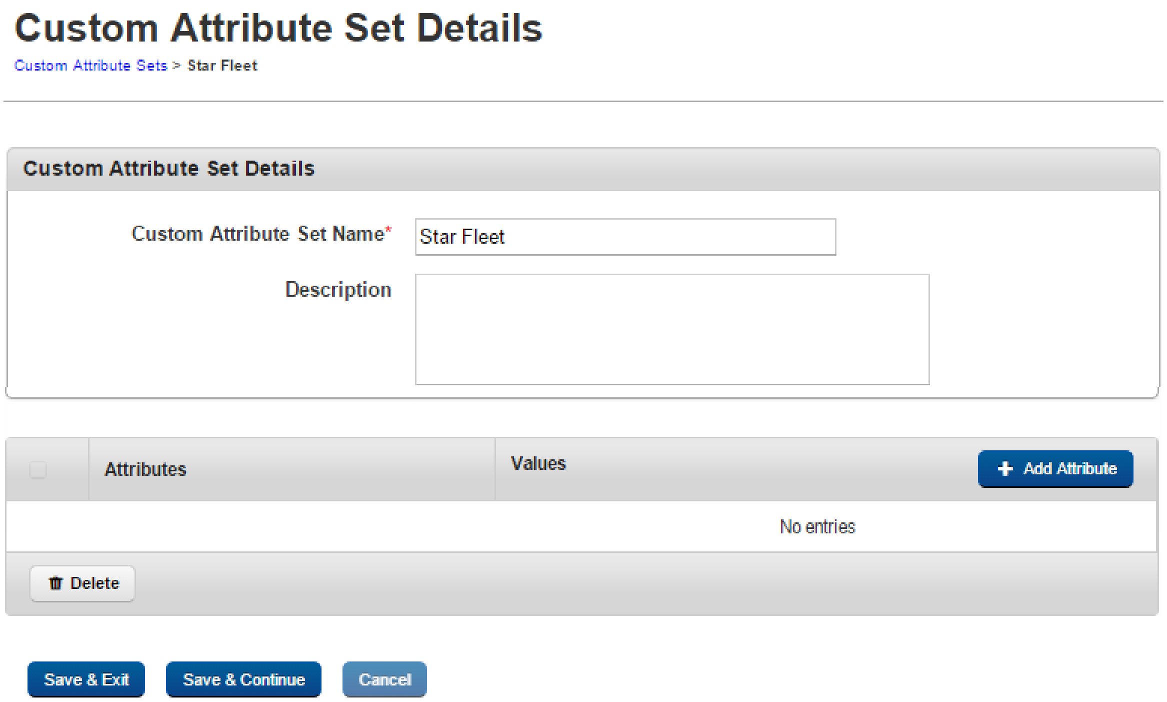
6.8.3 How to Delete a Custom Attribute Set

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.

6.8.4 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*: Star Fleet

Description:

Attributes	Values
No entries	

- **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.

6.8.5 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.

6.8.6 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.

6.8.7 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.

6.8.8 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.

6.8.9 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.

6.8.10 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.

6.9 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.

6.9.1 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:

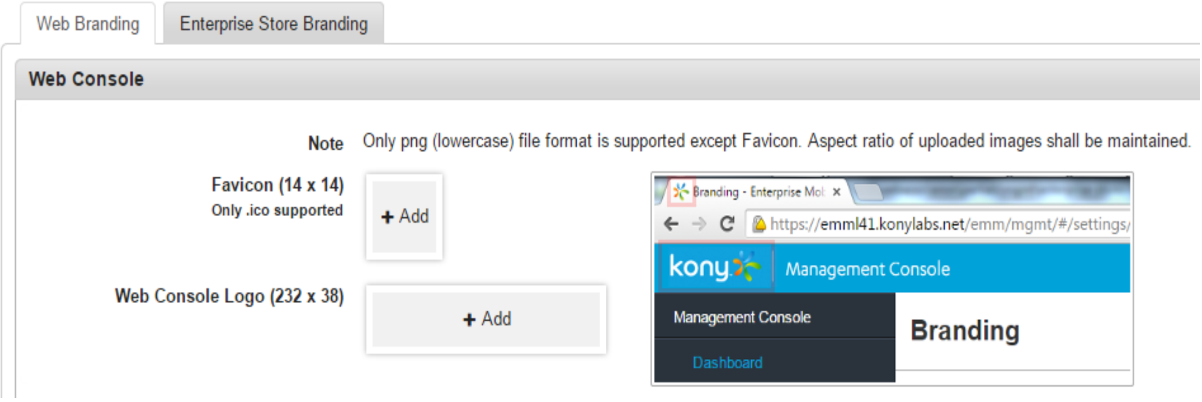
- Web Console
- Enterprise Store Download Page

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

6.9.1.1 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.



Note Only png (lowercase) file format is supported except Favicon. Aspect ratio of uploaded images shall be maintained.

Web Branding
Enterprise Store Branding
Web Console
Favicon (14 x 14)
Only .ico supported
+ Add
Web Console Logo (232 x 38)
+ Add
Branding - Enterprise Mol ×
https://emml41.konylabs.net/emm/mgmt/#/settings/
kony
Management Console
Management Console
Branding
Dashboard

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: • Size: 232 x 39 pixels • Color Mode: RGB, flattened, no transparency • File Type: High-quality PNG image file

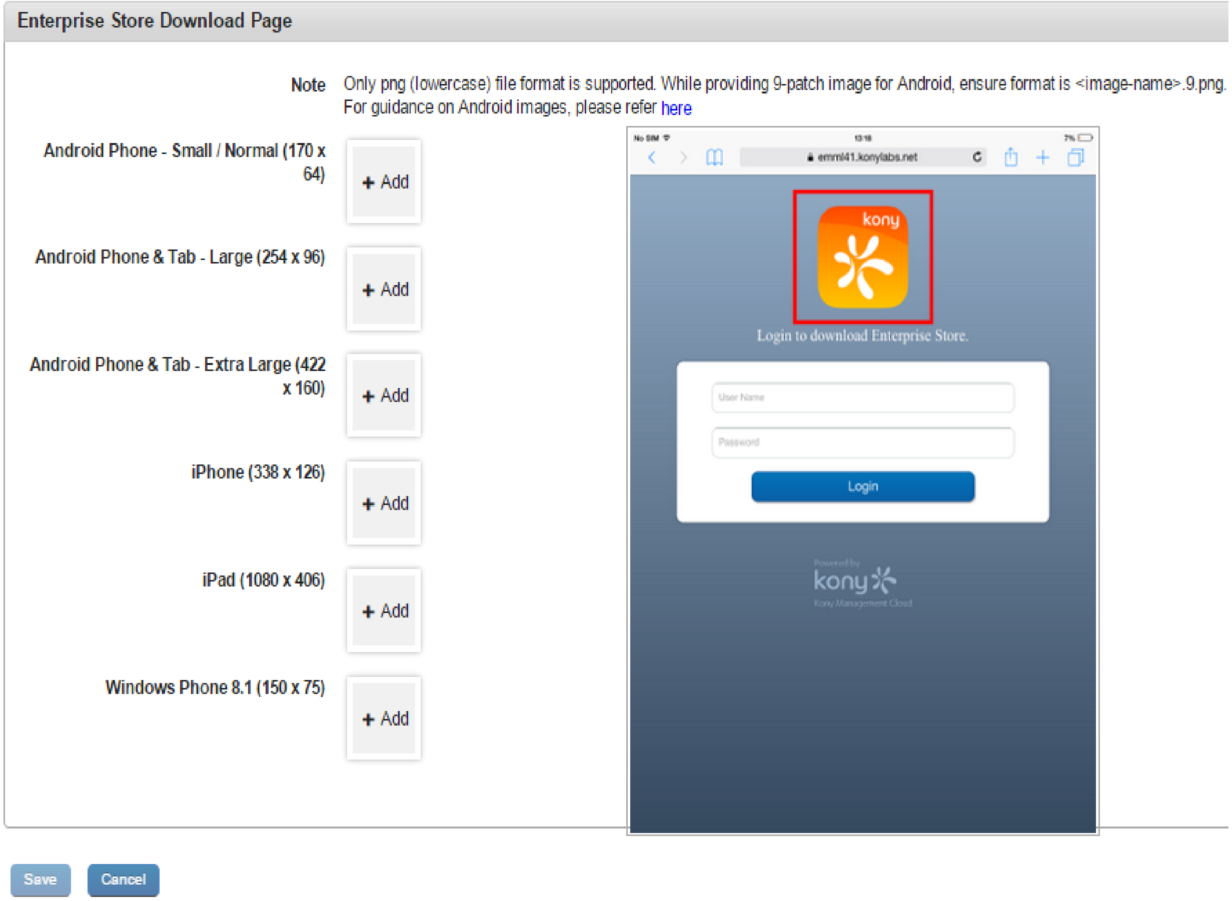
Icons	Description
Favicon (14 x 14) Only .ico supported	A favicon (short for favorites icon), is a shortcut icon, or bookmark icon. On the browser tab when EMM is open. Dimensions of the favicon are: • Size: 14 X14 pixels • Color Mode: RGB, flattened, no transparency • File Type: High-quality

6.9.1.2 Enterprise Store Download Page

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



Enterprise Store Download Page

Note 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

Android Phone - Small / Normal (170 x 64)

Android Phone & Tab - Large (254 x 96)

Android Phone & Tab - Extra Large (422 x 160)

iPhone (338 x 126)

iPad (1080 x 406)

Windows Phone 8.1 (150 x 75)

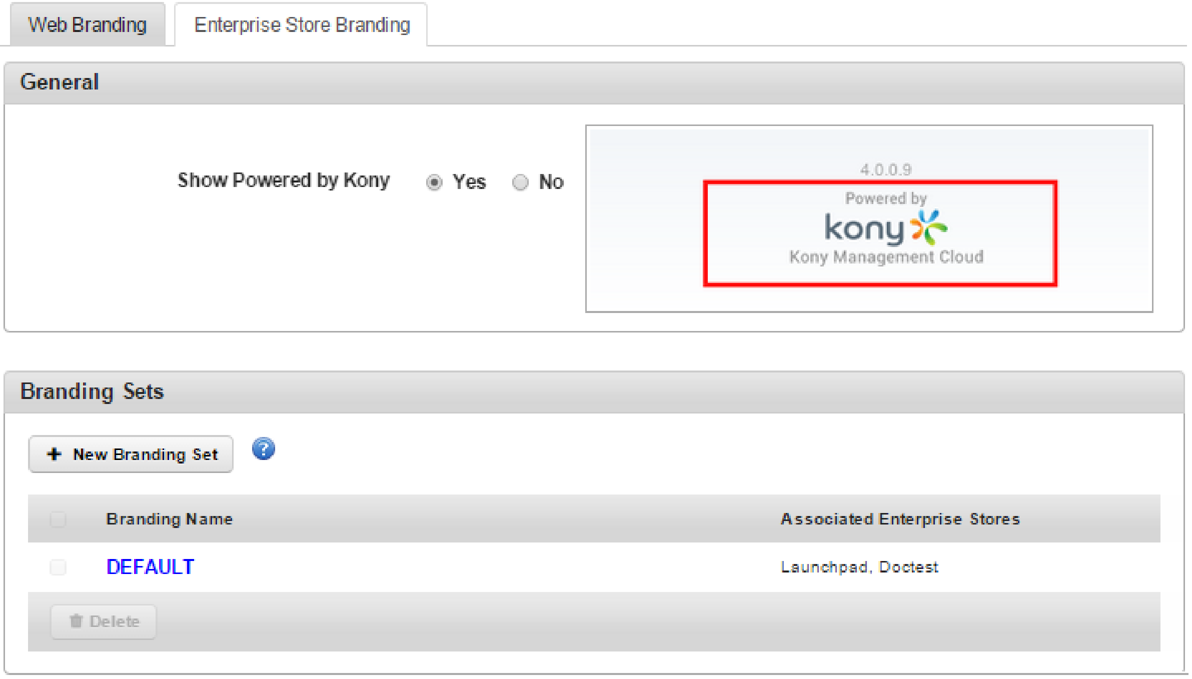
The Enterprise Store Download Page displays the following icon sizes for supported devices.

Icons	Description
Android Phone - Small and Normal	Dimensions of the log are: • Size: 170 x 64 pixels • File Type: High-quality PNG image file
Android Phone - Large	Dimensions of the logo are: • Size: 254 x 96 pixels • File Type: High-quality

Icons	Description
Android Phone and Tab - Extra Large	Dimensions of the logo are: • Size: : 422 x 160 pixels • File Type: High-quality
iPhone	Dimensions of the logo are: • Size: 338 x 126 pixels • File Type: High-quality PNG image file
iPad	Dimensions of the logo are: • Size: 1080 x 406 pixels • File Type: High-quality PNG image file
Windows Phone 8.1	Dimensions of the logo are: • Size: 150 x 75 pixels • File Type: High-quality PNG image file

6.9.2 Enterprise Store Branding

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



General

Show Powered by Kony ● Yes ○ No

Branding Sets

□	Branding Name	Associated Enterprise Stores
□	DEFAULT	Launchpad, Doctest

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

6.9.2.1 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.

6.9.2.2 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.

6.9.3 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.

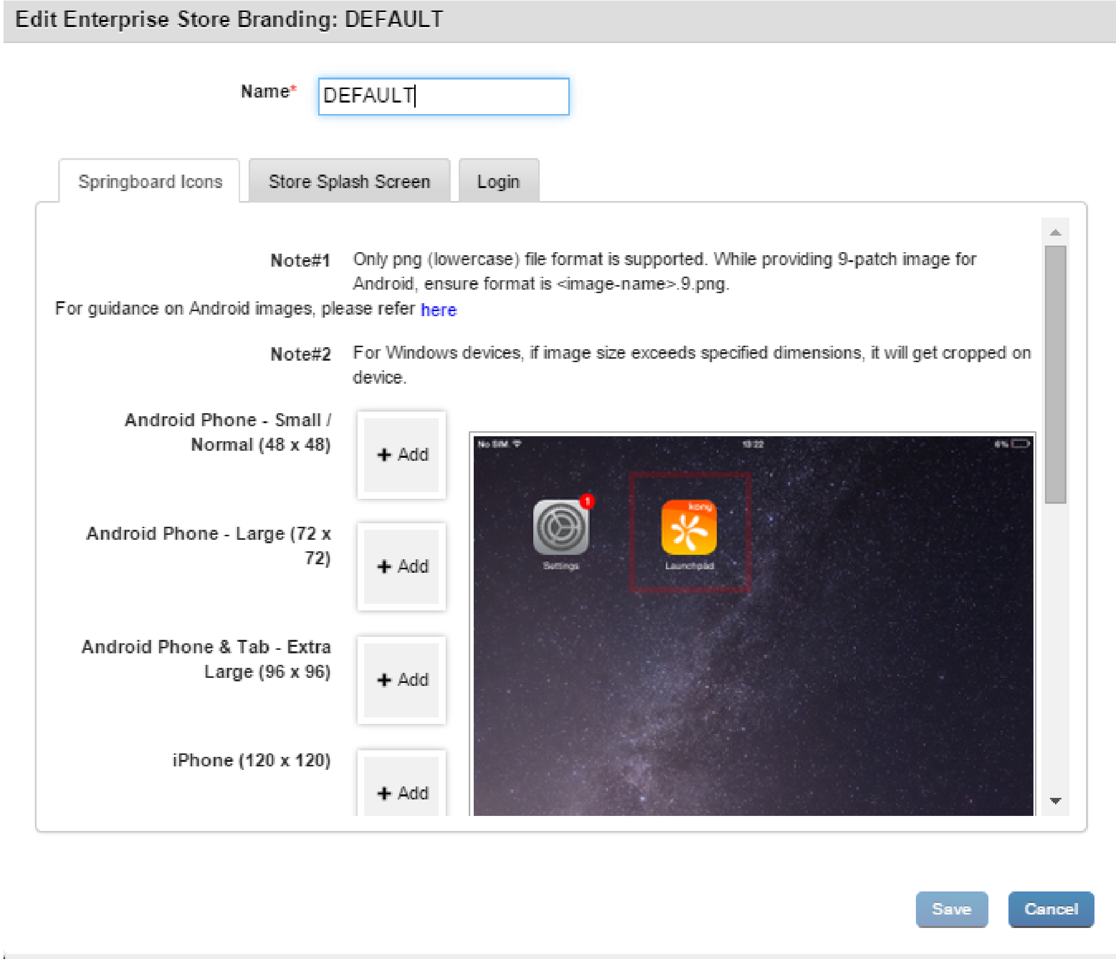
A branding Set page contains the following tabs:

- Springboard Icons
- Store Splash Screen
- Login

6.9.3.1 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.



Edit Enterprise Store Branding: DEFAULT

Name* DEFAULT

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, if image size exceeds specified dimensions, it will get cropped on device.

Android Phone - Small / Normal (48 x 48) + Add

Android Phone - Large (72 x 72) + Add

Android Phone & Tab - Extra Large (96 x 96) + Add

iPhone (120 x 120) + Add

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

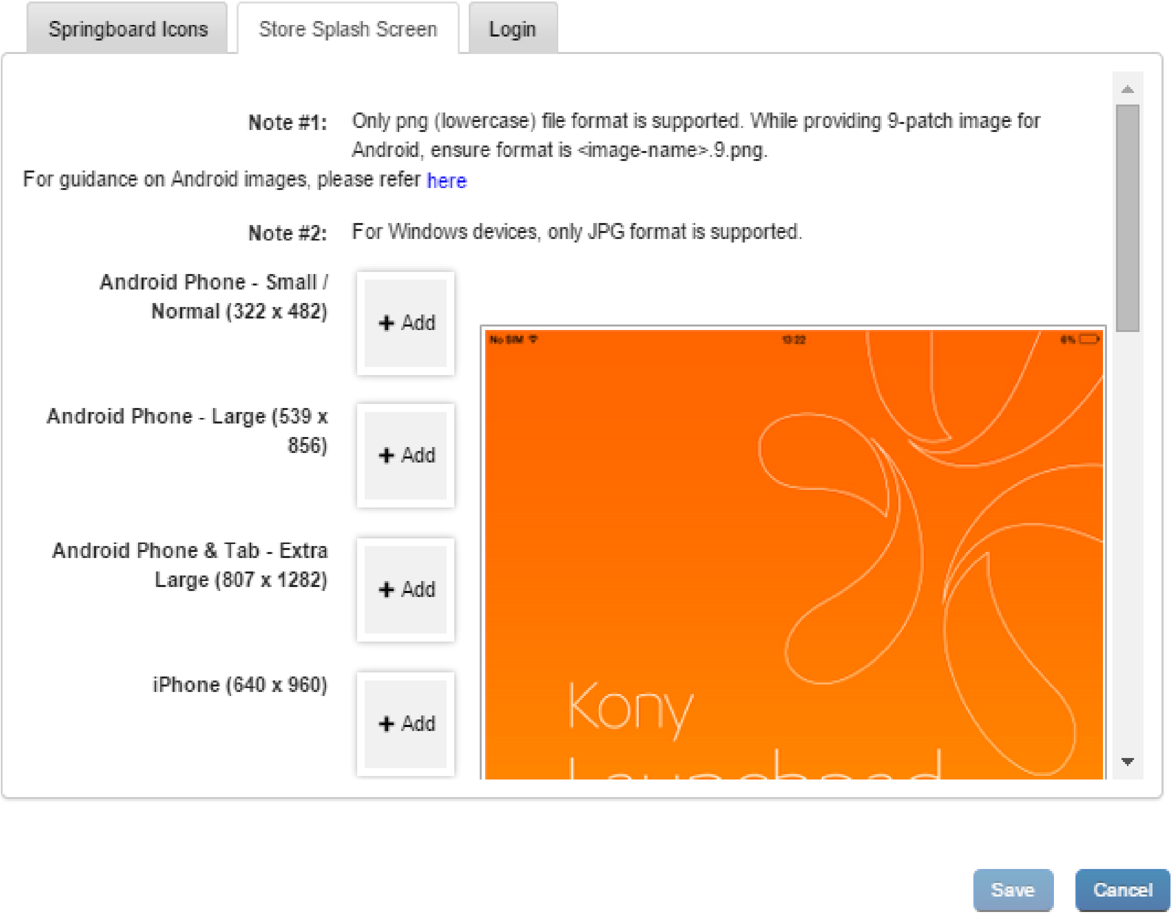
Icons	Description
Android Phone - Small and Normal	Dimensions of the logo are: • Size: 48 x 48 pixels • File Type: High-quality PNG image file
Android Phone - Large	Dimensions of the logo are: • Size: 72 x 72 pixels • File Type: High-quality PNG image file

Icons	Description
Android Phone and Tab - Extra Large	Dimensions of the logo are: • Size: 96 x 96 pixels • File Type: High-quality PNG image file
iPhone	Dimensions of the logo are: • Size: 120 x 120 pixels • File Type: High-quality PNG image file
iPad	Dimensions of the logo are: • Size: 152 x 152 pixels • File Type: High-quality PNG image file
Windows Phone 8.1	Dimensions of the logo are: • Size: 62 x 62 pixels • File Type: High-quality PNG image file
Windows Phone 8.1 Small Tile	Dimensions of the logo are: • Size: 159 x 159 pixels • File Type: High-quality PNG image file
Windows Phone 8.1 Medium Tile	Dimensions of the logo are: • Size: 336 x 336 pixels • File Type: High-quality PNG image file
Windows Phone 8.1 Wide Tile	Dimensions of the logo are: • Size: 691 x 336 pixels • File Type: High-quality PNG image file

6.9.3.2 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.



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)

Android Phone - Large (539 x 856)

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

iPhone (640 x 960)

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

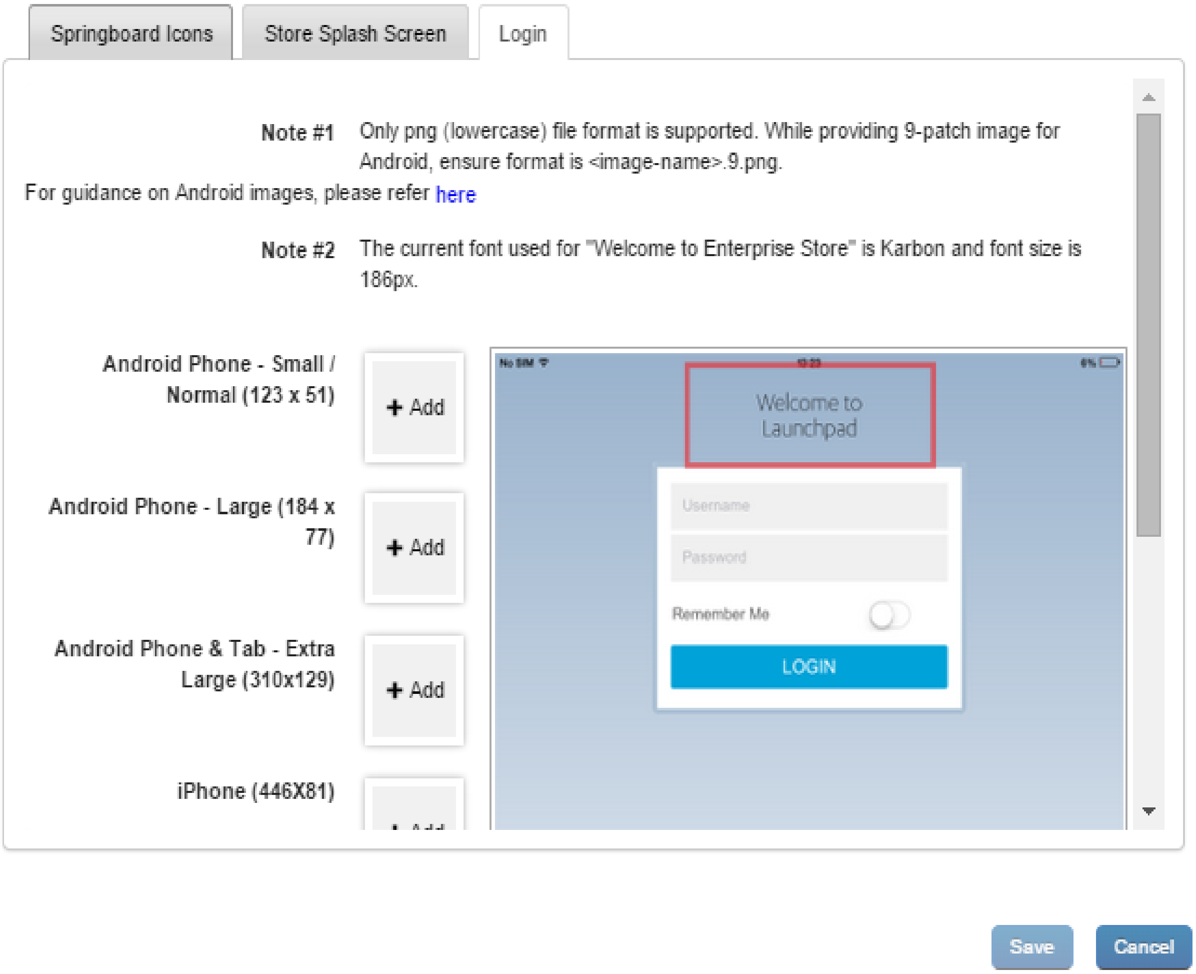
Icons	Description
Android Phone - Small and Normal	Dimensions of the logo are: • Size: 322 x 482 pixels • File Type: High-quality PNG image file
Android Phone - Large	Dimensions of the logo are: • Size: 539 x 856 pixels • File Type: High-quality PNG image file
Android Phone and Tab - Extra Large	Dimensions of the logo are: • Size: 807 x 1282 pixels • File Type: High-quality PNG image file
iPhone	Dimensions of the logo are: • Size: 640 x 960 pixels • File Type: High-quality PNG image file
iPhone 5	Dimensions of the logo are: • Size: 640 x 1136 pixels • File Type: High-quality PNG image file
iPhone 6 (Portrait)	Dimensions of the logo are: • Size: 750 x 1334 pixels • File Type: High-quality PNG image file
iPhone 6 (Landscape)	Dimensions of the logo are: • Size: 1334 x 750 pixels • File Type: High-quality PNG image file

Icons	Description
iPhone 6 Plus (Portrait)	Dimensions of the logo are: • Size: 1242 x 2208 pixels • File Type: High-quality PNG image file
iPhone 6 Plus (Landscape)	Dimensions of the logo are: • Size: 2208 x 1242 pixels • File Type: High-quality PNG image file
iPad	Dimensions of the iPad touch icon are: • Size: 1536 x 2048 pixels • File Type: High-quality PNG image file
Windows Phone 8.1 WVGA	Dimensions of the iPad touch icon are: • Size: 480 x 800 pixels • File Type: JPG image file
Windows Phone 8.1 WVGA	Dimensions of the iPad touch icon are: • Size: 768 x 1280 pixels • File Type: JPG image file
Windows Phone 8.1 720p	Dimensions of the iPad touch icon are: • Size: 720 x 1280 pixels • File Type: JPG image file

6.9.3.3 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.



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 The current font used for "Welcome to Enterprise Store" is Karbon and font size is 186px.

Android Phone - Small / Normal (123 x 51) + Add

Android Phone - Large (184 x 77) + Add

Android Phone & Tab - Extra Large (310x129) + Add

iPhone (446X81) + Add

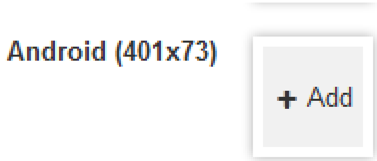
The enterprise store app Login Screen displays the following icon sizes for supported devices.

Icons	Description
Android Phone - Small and Normal	Dimensions of the logo are: • Size: 123 x 51 pixels • File Type: High-quality PNG image file

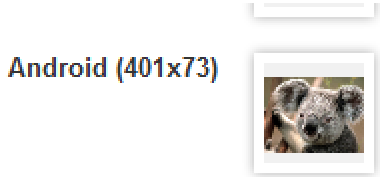
Icons	Description
Android Phone - Large	Dimensions of the logo are: • Size: 184 x 77 pixels • File Type: High-quality PNG image file
Android Phone and Tab - Extra Large	Dimensions of the logo are: • Size: 310 x 129 pixels • File Type: High-quality PNG image file
iPhone	Dimensions of the logo are: • Size: 446 x 81 pixels • File Type: High-quality PNG image file
iPad	Dimensions of the logo are: • Size: 800 x 140 pixels • File Type: High-quality PNG image file
Windows Phone 8.1	Dimensions of the logo are: • Size: 456 x 166 pixels • File Type: High-quality PNG image file

6.9.4 Uploading logos

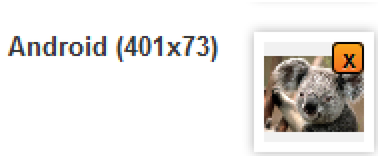
To upload your logos for Branding, follow these steps:



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



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



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.

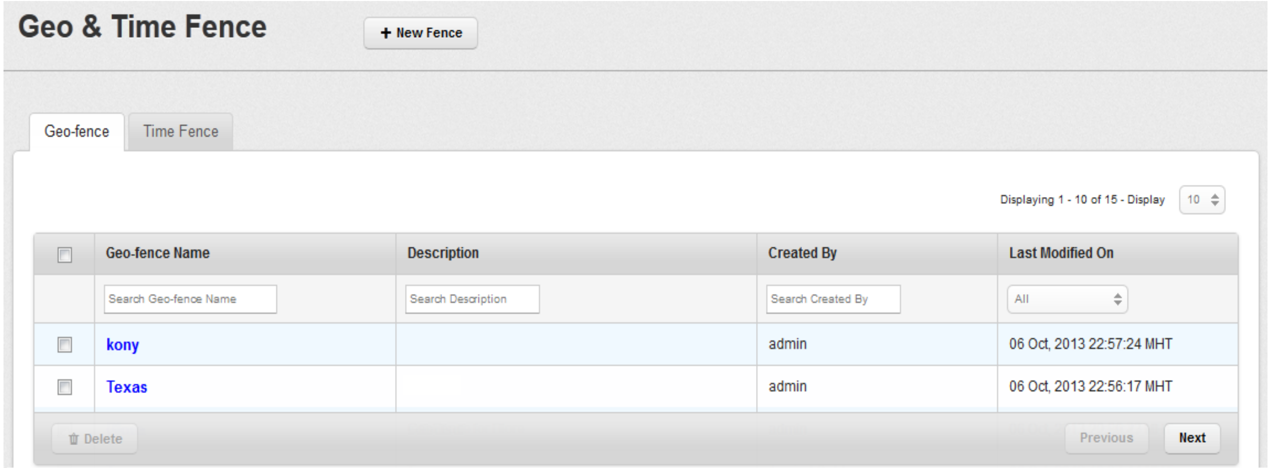
6.10 Geo and Time Fence List

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.



Displaying 1 - 10 of 15 - Display 10

□	Geo-fence Name	Description	Created By	Last Modified On
	Search Geo-fence Name	Search Description	Search Created By	All
□	kony		admin	06 Oct, 2013 22:57:24 MHT
□	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

6.10.1 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:

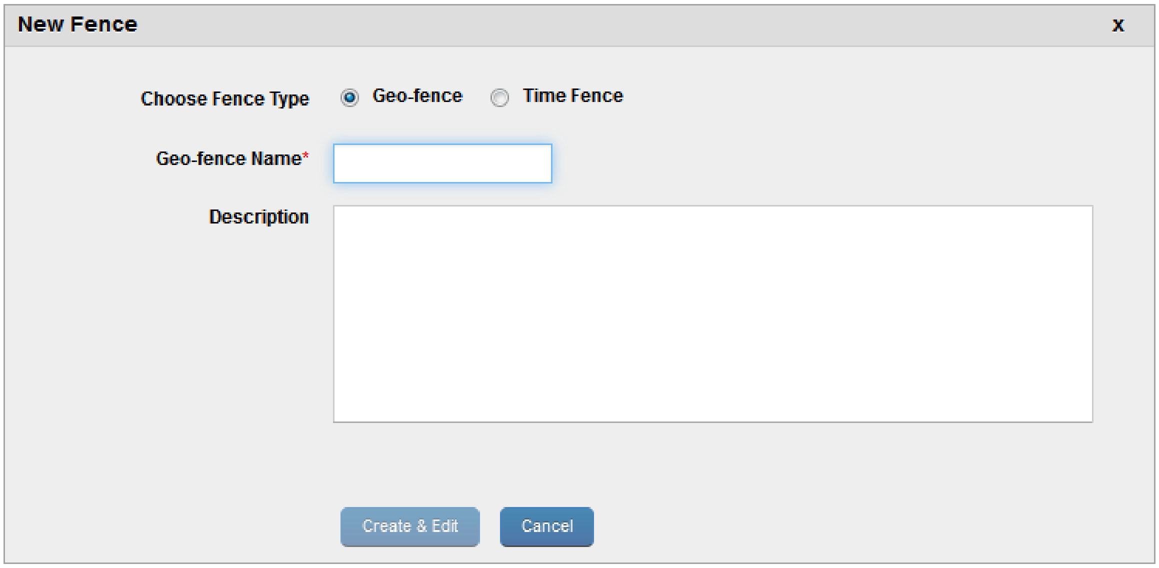
1. **Geo Fence Name**: Enter partial or complete name in the **Search Geo Fence Name** field.
2. **Description**: Enter the specific details in the **Search Description** field.
3. **Created By**: Enter partial or complete name of the Administrator in the **Search Created By** field.
4. **Last Modified 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.

6.10.2 Creating a Geo-fence

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

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



Choose Fence Type ● Geo-fence ○ Time Fence

Geo-fence Name*

Description

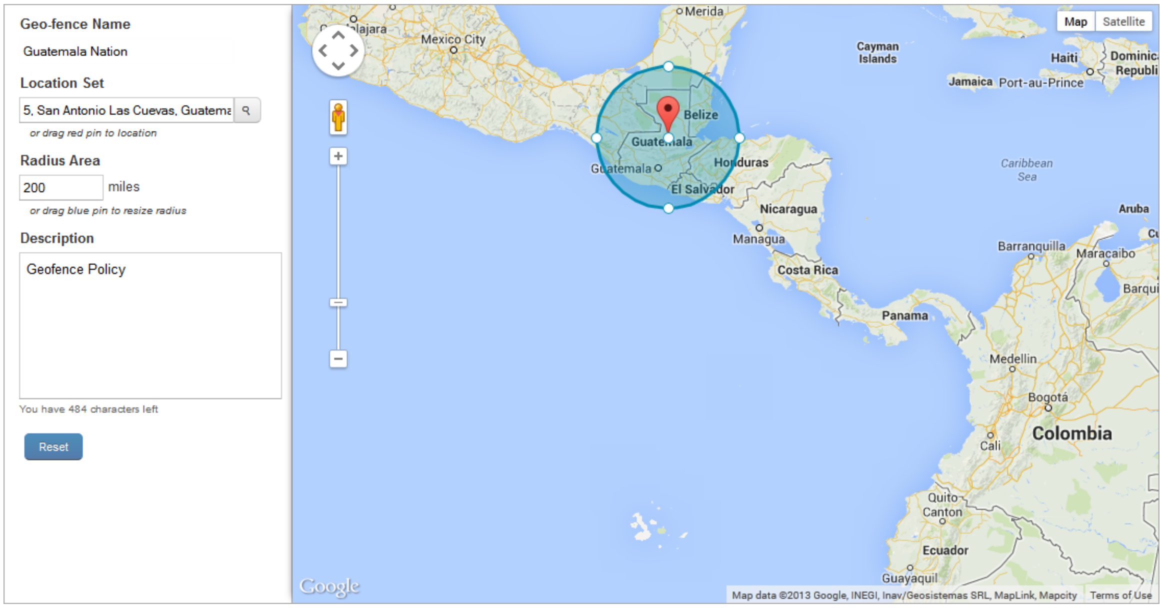
2. The **New Fence** window appears. Enter the following details:
   a. **Choose Fence Type**: By default, this option is set to **Geo-fence** that you can modify to Time Fence.
   b. **Geo Fence Name**: Enter a valid name for the Geo-fence.
      This action enables the **Create and Edit** button.

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:



Geo-fence Name
Guatemala Nation

Location Set
5, San Antonio Las Cuevas, Guatema
or drag red pin to location

Radius Area
200 miles
or drag blue pin to resize radius

Description
Geofence Policy

You have 484 characters left

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.

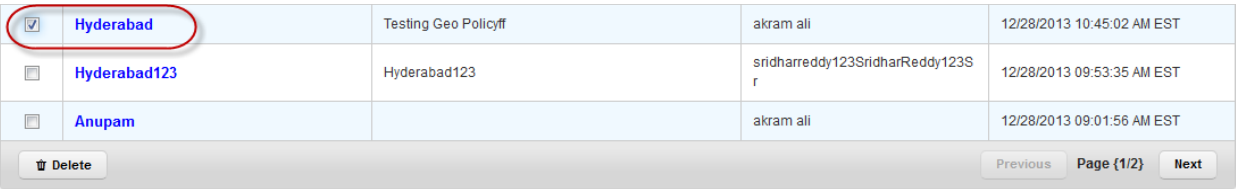
c. **Description**: This field is pre-populated with the existing details.If required, you can update this field.

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.

6.10.3 Deleting a Geo-fence

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



☑	Hyderabad	Testing Geo Policyff	akram ali	12/28/2013 10:45:02 AM EST
□	Hyderabad123	Hyderabad123	sridharreddy123SridharReddy123Sr	12/28/2013 09:53:35 AM EST
□	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.

6.10.3.1 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 enrollment of a device, then after enrolling the device, Geo-fence becomes effective immediately.

Scenario 2

If a Geo-fence is created or modified after a device is enrolled, 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.

6.10.4 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.

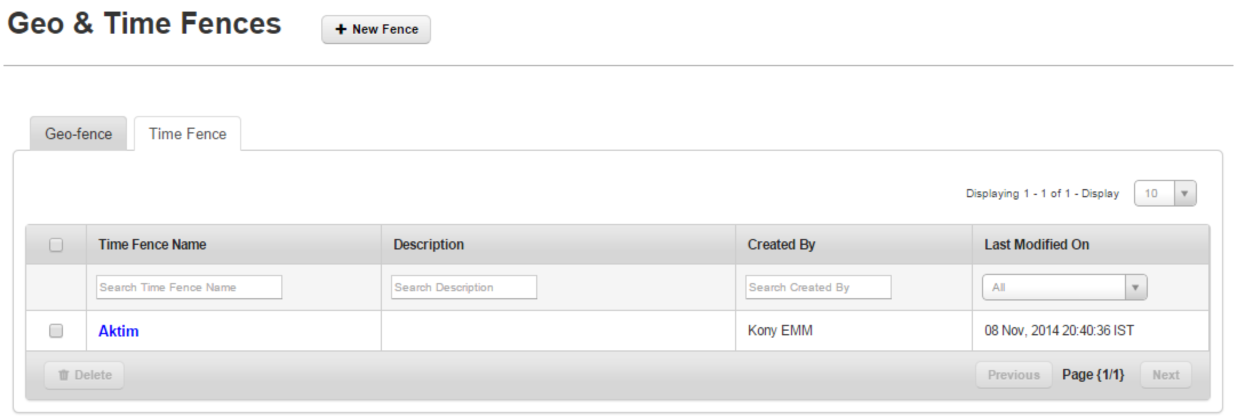
To search a Time Fence, follow these steps:

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.

6.10.5 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.



Displaying 1 - 1 of 1 - Display 10

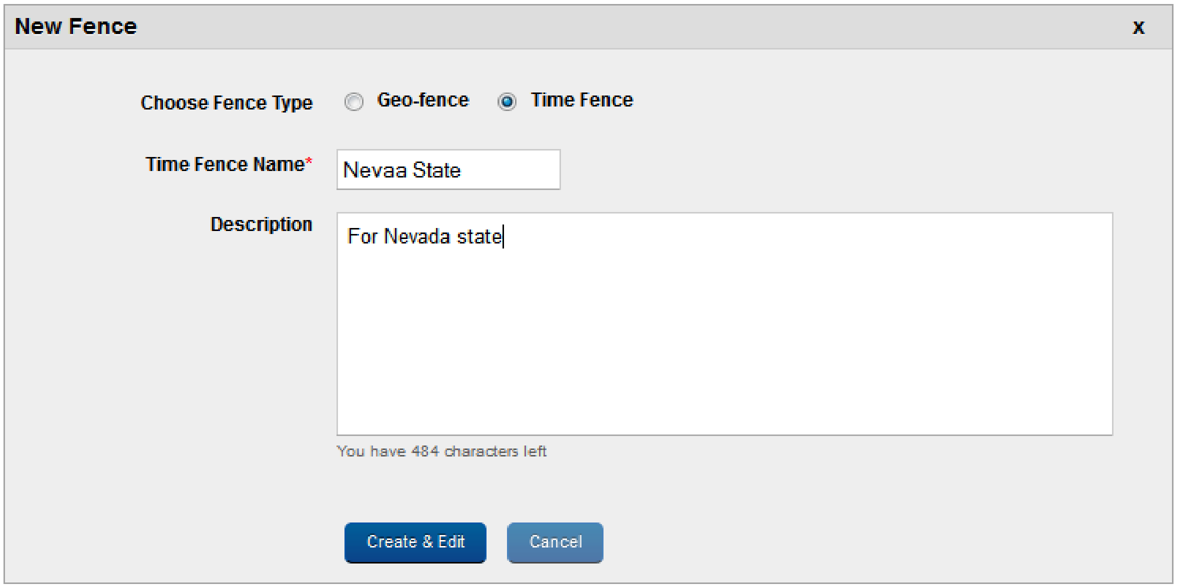
☐	Time Fence Name	Description	Created By	Last Modified On
	Search Time Fence Name	Search Description	Search Created By	All
☐	Aktim		Kony EMM	08 Nov, 2014 20:40:36 IST

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:

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.



Choose Fence Type ○ Geo-fence ● Time Fence

Time Fence Name* Nevaa State

Description For Nevada state

You have 484 characters left

New Fence window appears.

2. Enter the following details:

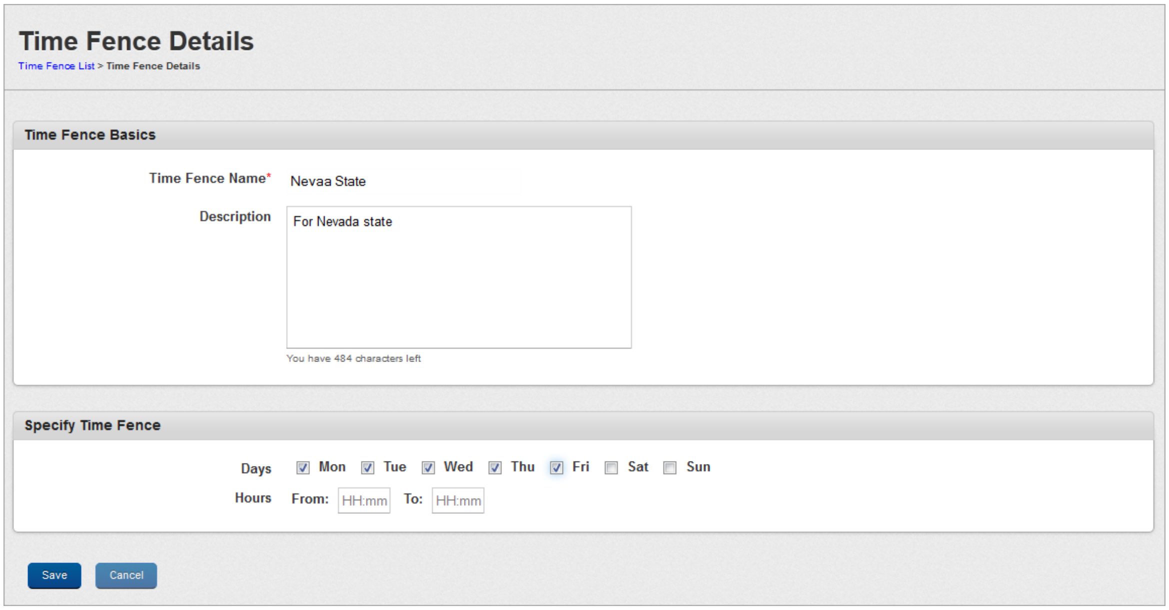
   a. **Choose Fence Type**: By default, this option is set to Timefence, which you can modify to Geofence.

   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

The Time Fence details page appears.

4. Enter details for the following fields:

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

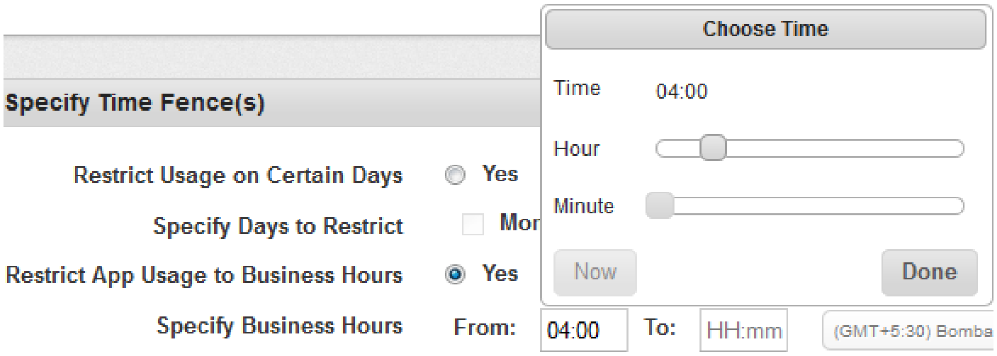
      i. **Timefence(s) Name**: Displays timefence name.

      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 □ Mor

Restrict App Usage to Business Hours ● Yes

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

Time 04:00

      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 in 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:

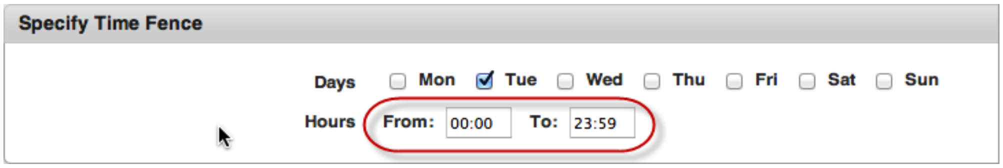
Monday - 12. 00 a.m to 08.00 a.m

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 untill 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.

6.10.6 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.

6.11 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:

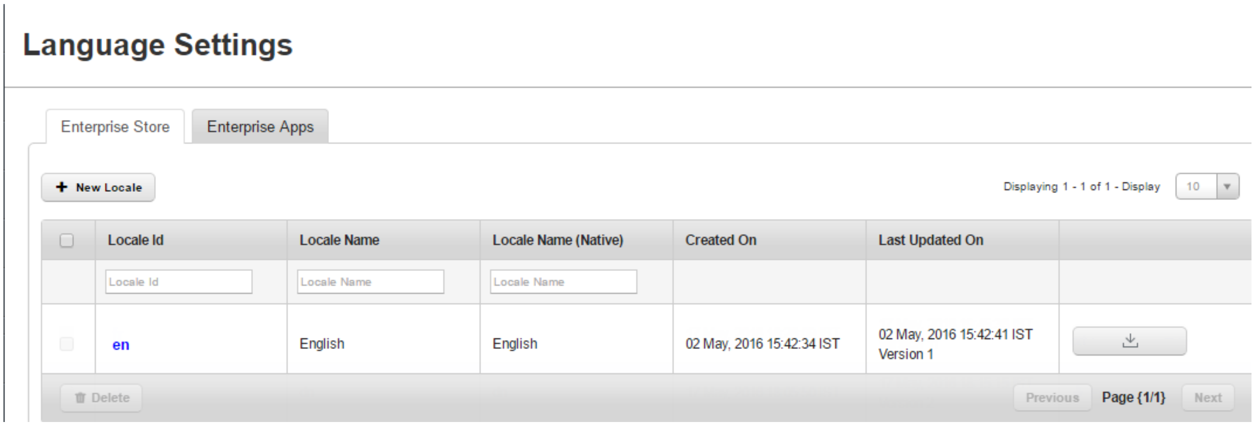
- Application store (except Kony Enterprise App Store names)
- App details
- Push messages
- Policy alert and error messages
- Terms and conditions

> *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.

6.11.1 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.



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

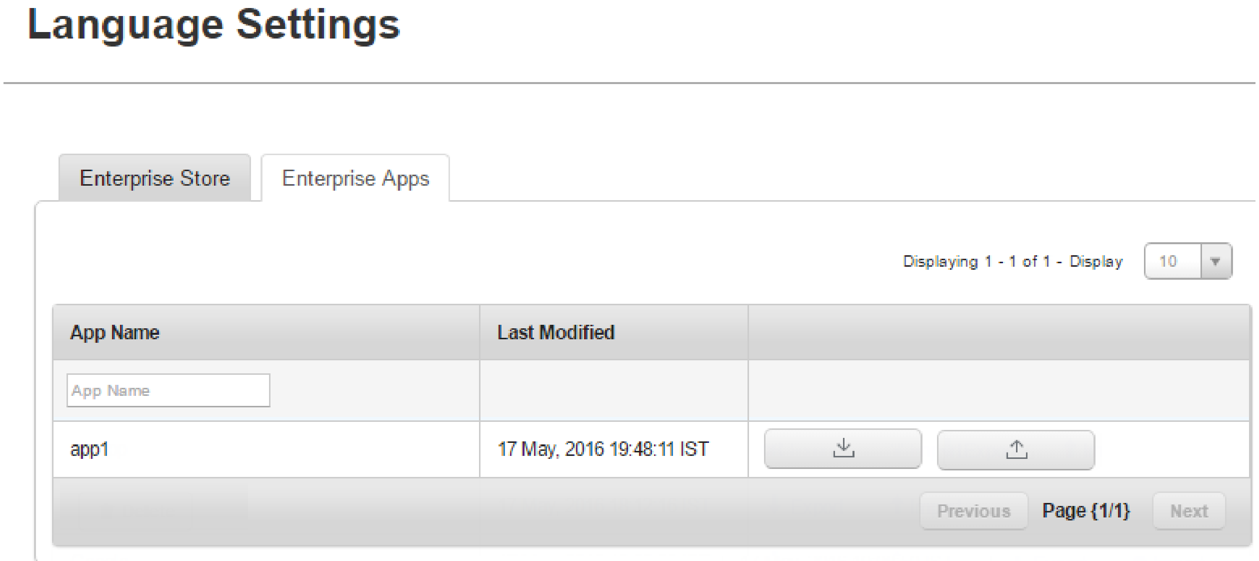
The Enterprise Store tab displays the following user interface features:

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).

6.11.2 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.



App Name	Last Modified
app1	17 May, 2016 19:48:11 IST

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).

6.12 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.

6.13 Working with Internationalization

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

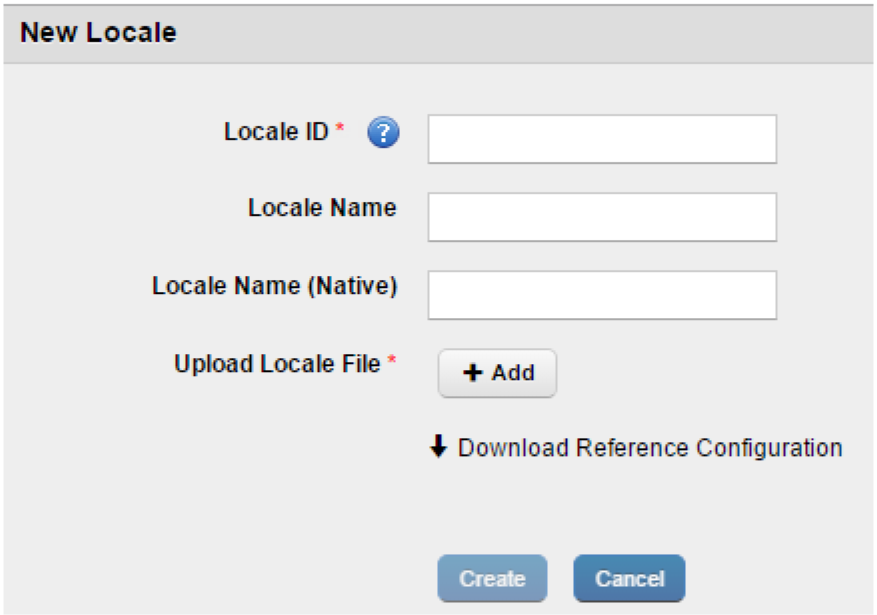
- Create a new locale
- Modify an existing locale
- Delete an existing locale

- Work with the locale excel file
- Modify an existing Enterprise App locale

6.13.1 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.



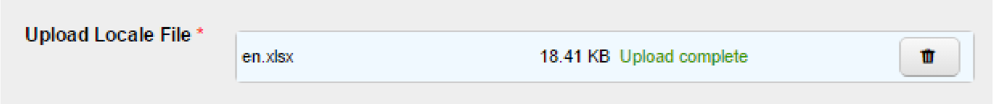
3. Enter the following details:
   a. **Locale ID**: Enter the locale ID. For example, for Spanish for Mexico, the locale ID is es_MX or, es for Spanish.

> *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.



Upload Locale File *

en.xlsx 18.41 KB Upload complete

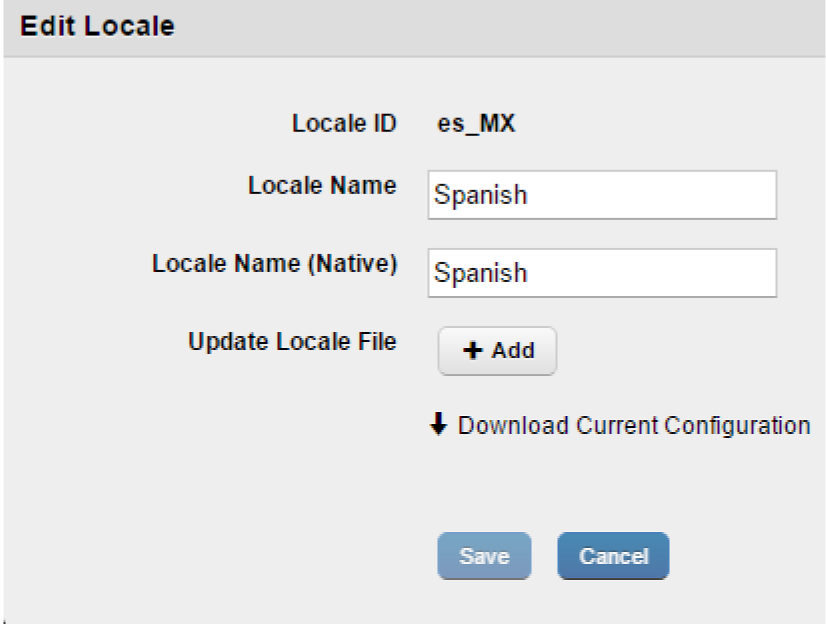
7. Click **Create**. A success message appears.
8. Click **OK**.

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

6.13.2 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

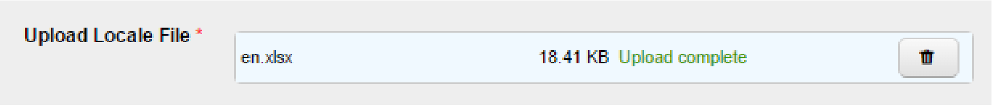
Locale ID	es_MX
Locale Name	Spanish
Locale Name (Native)	Spanish
Update Locale File	+ Add

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.



Upload Locale File *

en.xlsx 18.41 KB Upload complete

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.

6.13.3 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.

6.13.4 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.

6.13.5 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:

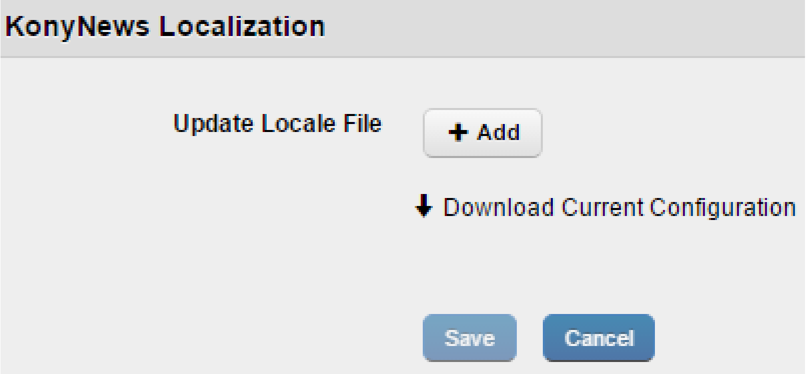
1. In the EMM management console, from **Settings**, click **Language Settings**. The Language Settings page appears. The Enterprise Store tab is open by default.

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.



KonyNews Localization

Update Locale File

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.

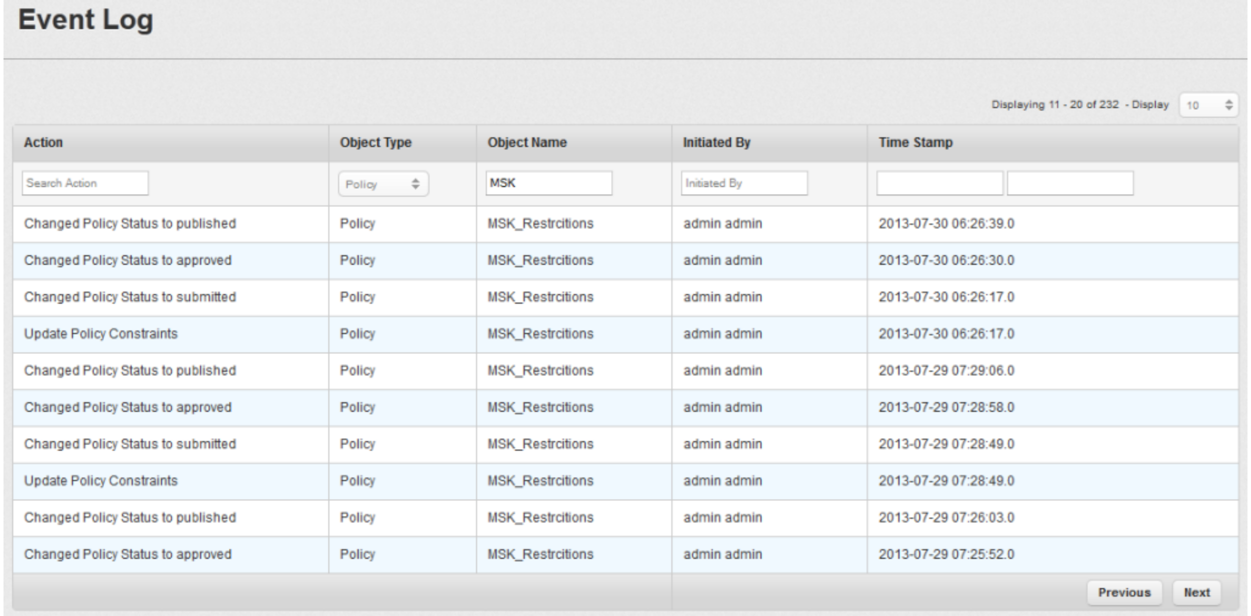
10. Click **OK**. Your enterprise app locale file is now updated. Every time you upload a new locale file, the previous version of the locale file is replaced by the new version.

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

6.14 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 11 - 20 of 232 - Display 10

Action	Object Type	Object Name	Initiated By	Time Stamp
Search Action	Policy	MSK	Initiated By	
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:39.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:30.0
Changed Policy Status to submitted	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:17.0
Update Policy Constraints	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:17.0
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:29:06.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:58.0
Changed Policy Status to submitted	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:49.0
Update Policy Constraints	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:49.0
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:26:03.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:25:52.0

The Event Log List view displays the following columns:

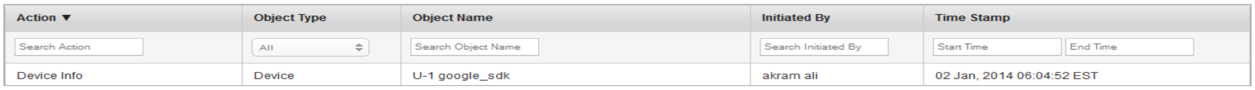
Search Elements Properties	Description
Actions	Displays a list of all the actions that are performed on devices, policies or device sets.
Object Type	Displays a list of the object types, for example Device, Policy or Device Set. The actions are performed on the specific object types.
Object Name	Displays 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

6.14.1 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
Search Action	All	Search Object Name	Search Initiated By	Start Time End Time
Device Info	Device	U-1 google_sdk	akram ali	02 Jan, 2014 06:04:52 EST

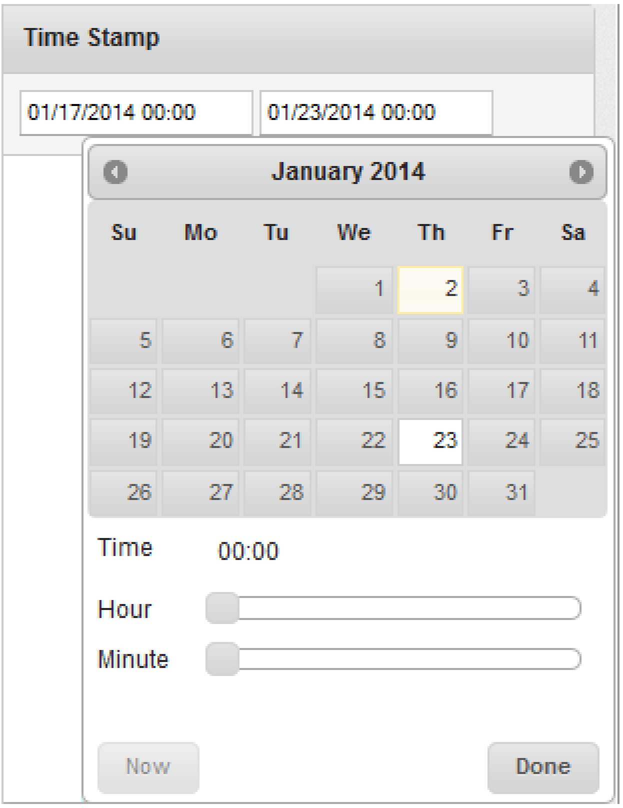
1. Enter or select details for following search filters:

    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.



Time Stamp

01/17/2014 00:00

01/23/2014 00:00

January 2014

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Time 00:00

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.

6.15 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.

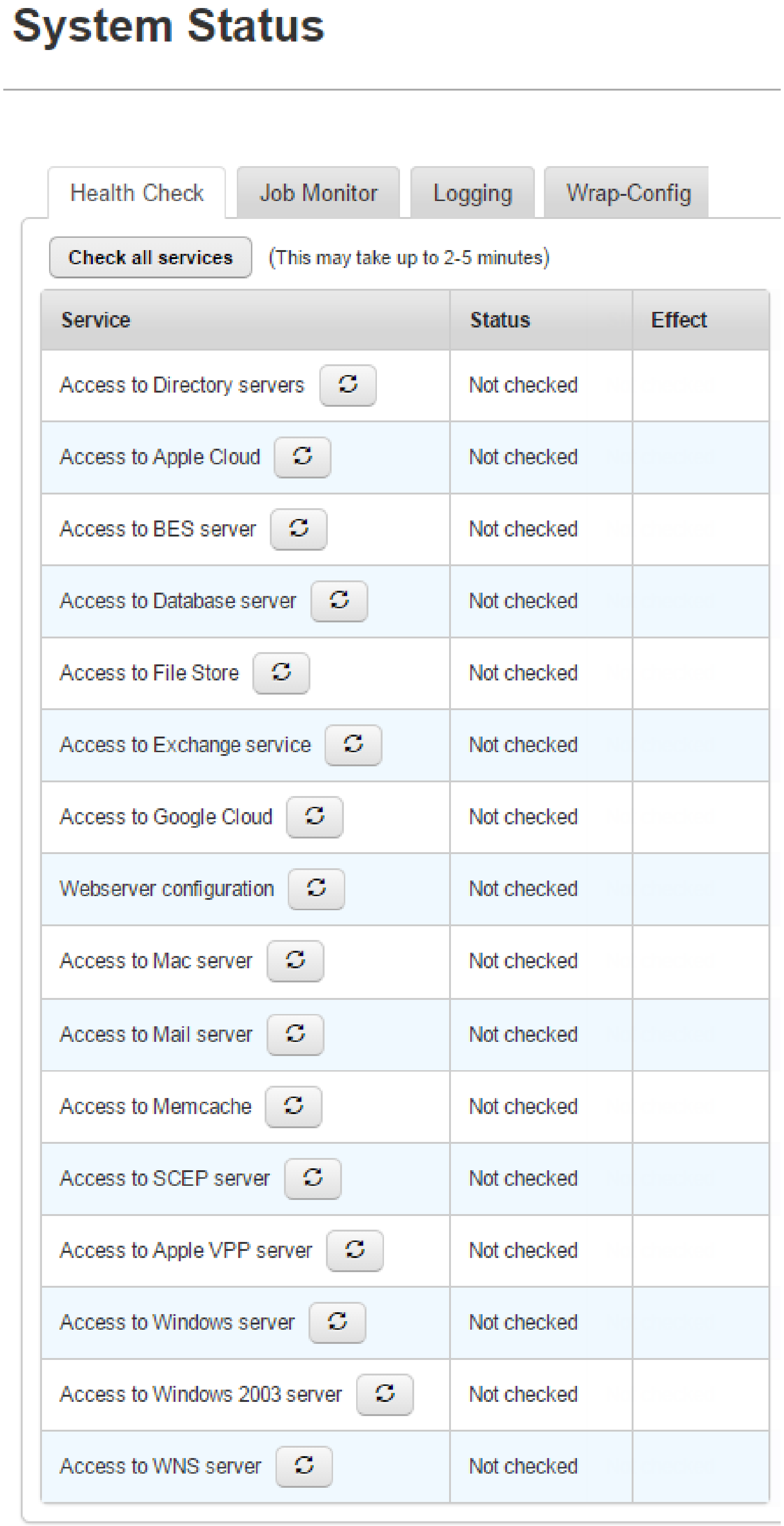
- Health Check
- Job Monitor
- Logging
- Wrap-Config

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.

6.15.1 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

(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	

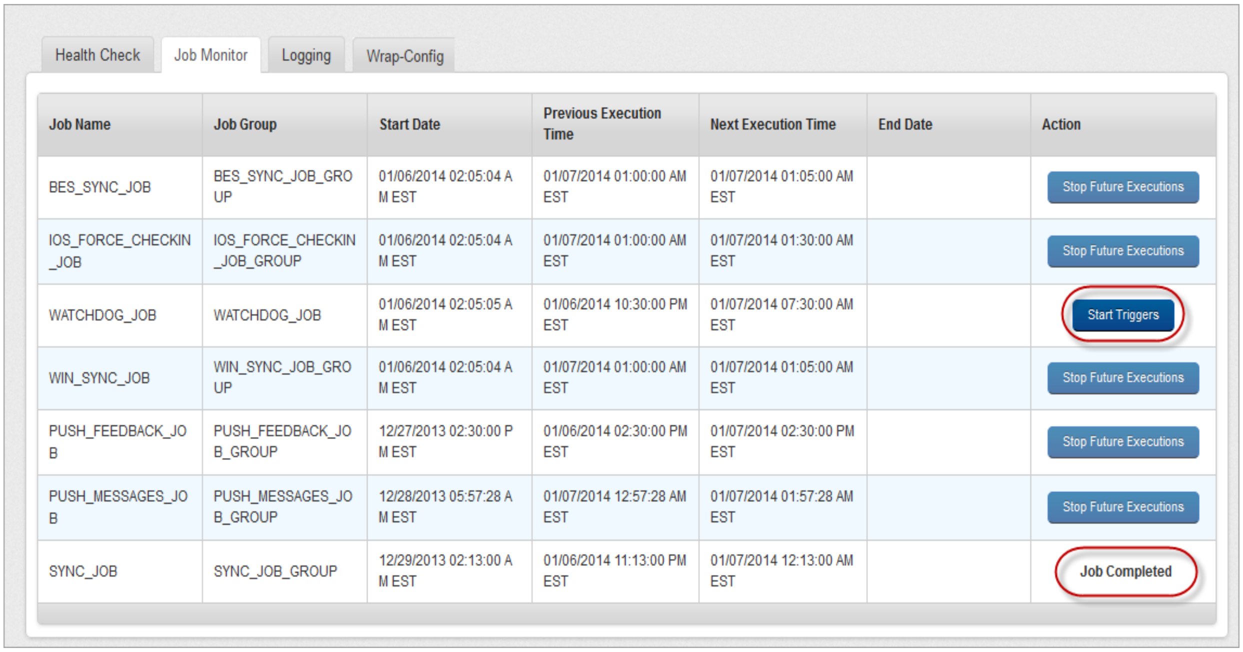
The health checking system runs internally on a periodic basis.

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.

6.15.2 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

6.15.2.1 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.

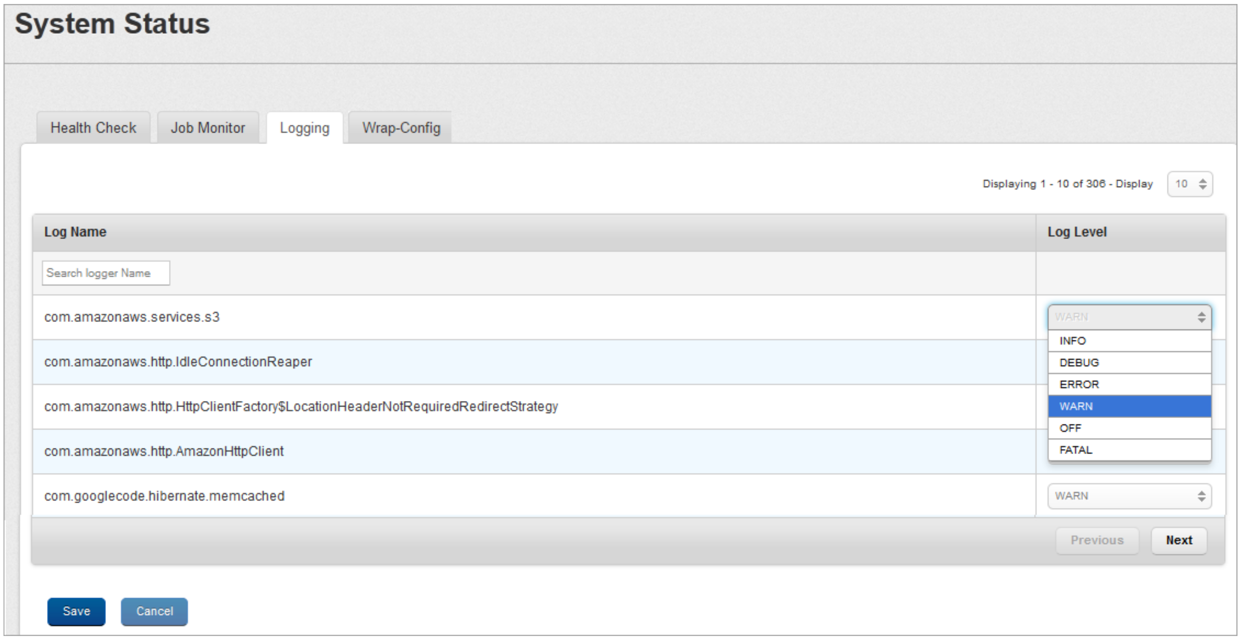
   Jobs that are already triggered and in progress cannot be stopped, and the server waits for the completion of the job.Once already initiated job is completed ,the status is displayed as Jobs Completed in the list view.

> *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.

6.15.3 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.



System Status

Displaying 1 - 10 of 306 - Display 10

Log Name	Log Level
Search logger Name	
com.amazonaws.services.s3	WARN
com.amazonaws.http.IdleConnectionReaper	
com.amazonaws.http.HttpClientFactory$LocationHeaderNotRequiredRedirectStrategy	
com.amazonaws.http.AmazonHttpClient	
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.

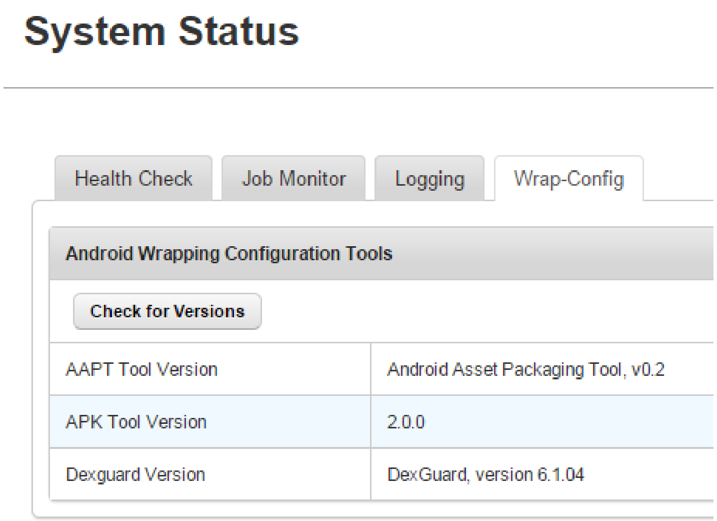
Log Level	Description
Debug	Information that is helpful to resolve any type of issues.
Error	Information that can be useful for debugging problems.
Off	Disables the log level.
Fatal	An error that causes a service to abort.

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

6.15.4 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.



AAPT Tool Version	Android Asset Packaging Tool, v0.2
APK Tool Version	2.0.0
Dexguard Version	DexGuard, version 6.1.04

7. EMM Licenses

EMM is now available in two types of licenses.

- Enterprise License
- Simple Authentication (MAM) License
- Store Only License

7.1 Enterprise License

The Enterprise licenses are available with full functionality of EMM.

7.1.1 Availability of Features in EMM and MAM/MCM Enrollment Mode for EMM License

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Dashboard	Total Non-Compliant Devices - Count	Available	Not available.
	Locations	Available	Not available.
	Compliance Chart	Available	Not available.
Reports	Compliance Action Report	Available	Not available. When a user is moved from EMM to MAM/MCM mode, old data(when user is in EMM mode) generated for compliance action will be shown in the report.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Enterprise Apps	iOS - Managed Apps Configuration	Available	Not available. When a user is moved from EMM to MAM/MCM, these will be revoked.
	iOS - VPN	Available	Not available. When a user is moved from EMM to MAM/MCM, VPN will be revoked.
	Windows - VPN	Available	Not available. When a user is moved from EMM to MAM/MCM, VPN will be revoked.
App Policies	App Usage - Device Policy	Available	Not available. Device policies will be revoked when device is moved from EMM to MAM/MCM.
VPP apps	VPP apps	Available	Not available. When device is moved from EMM to MAM/MCM, consumed app licenses will be released.
Device Sets	Device Sets	Available	Not available. When a user is moved from EMM to MAM/MCM the device will be removed from the device sets as well.
Device Enrollment	New Device	Available	Available
	Bulk Enroll Devices	Available	Available

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Device Policies	Device Policies	Available	Not available. When a user is moved from EMM to MAM/MCM, these will be revoked.
Application Settings	Usage Settings- Online Login - Web and Enterprise Store - Require captcha- Enterprise wipe	Available	Not available. When wrong captcha is given and wipe condition is met, nothing happens.
	VPP Apps	Available	Not available.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Device Settings	Usage Configuration-Heartbeat Settings	Available	Not available.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
	Usage Configuration- Enrollment Settings	Available	Not available.
	Usage Configuration- Watchdog Settings	Available	Not available.
	Usage Configuration- Tracking Settings - Enable viewing device location	Available	Not available.
	Usage Configuration- Tracking Settings - Allow Mock Location	Available	Not available.
	Usage Configuration- Tracking Settings- Allow User installed applications that have mock location permission	Available	Not available.
	Usage Configuration- Communication logs (SAFE, Android)	Available	Not available.
	Usage Configuration- SAFE Settings (Android)	Available	Not available.
	Usage Configuration- Mail+ for Enterprise	Available	Not available.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Exchange Services	Exchange Services	Available	Not available.
Enterprise Resources	Enterprise Resources	Available	Not available.
Even Log	Even Log	Available	Not available.

7.2 Simple Authentication (MAM) License

The Simple Authentication (MAM) license is a limited version of EMM. The companies that use this license will have access to only some functionality in EMM. For more information, see the Kony Management Simple Authentication User Guide.

The following features are available for MAM licenses:

- App polices
- Custom branding
- Device Details
- Content Management
- Access Management
- Settings

7.3 Store Only License

The Store Only license is a limited version of Kony Management that is available for users by default with Kony Fabric. Users of the Store Only license will have limited functionality in Kony Management (EMM). For more information, see the Kony Management Store Only User Guide.

The following features are available for Store Only licenses:

- Enterprise Apps
- Custom branding
- Device Details
- Access Management
- Settings
- Reports

8. 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.

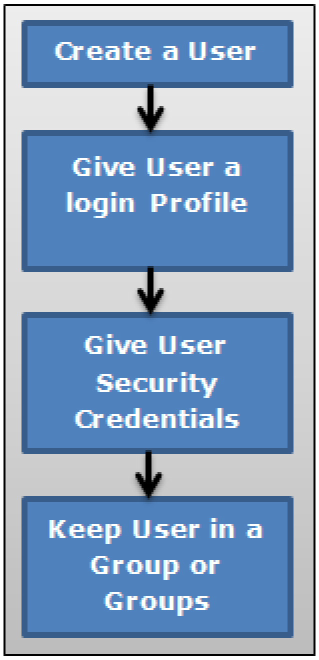
8.1 Managing Access

Access management includes:

- User Management
- Group Management
- Enrollment Mode
- Permission Set

8.2 Users

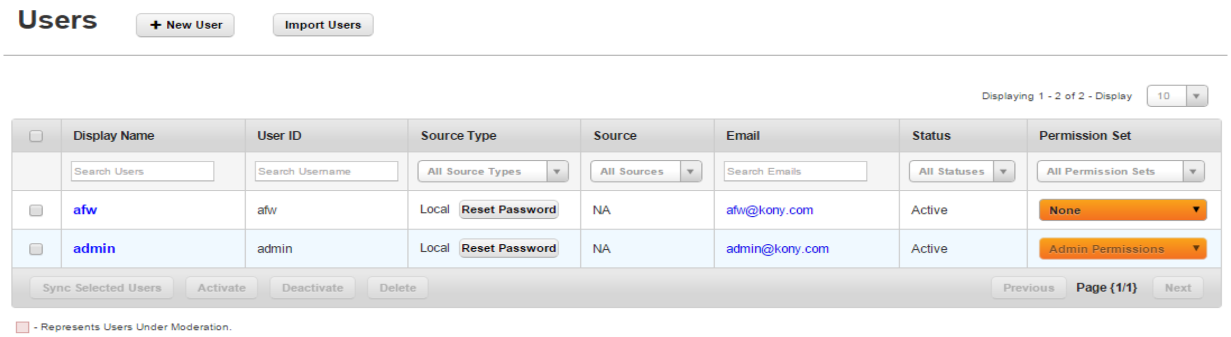
A user is an individual person. Each user needs an account to access the EMM Console. Administrator creates a user account for each person who uses the EMM Console.


Create a User
Give User a login Profile
Give User Security Credentials
Keep User in a Group or Groups

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 10

□	Display Name	User ID	Source Type	Source	Email	Status	Permission Set
	Search Users	Search Username	All Source Types	All Sources	Search Emails	All Statuses	All Permission Sets
□	afw	afw	Local Reset Password	NA	afw@kony.com	Active	None
□	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	If selected at row level, the particular user is selected for any further actions. Multiple rows can also be selected. Selection can only be done on a single page of records. You can choose to display upto 100 records (users).
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

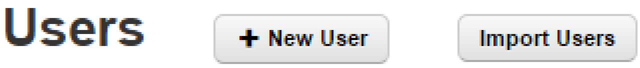
8.2.1 Creating a New User

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.

8.2.2 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.

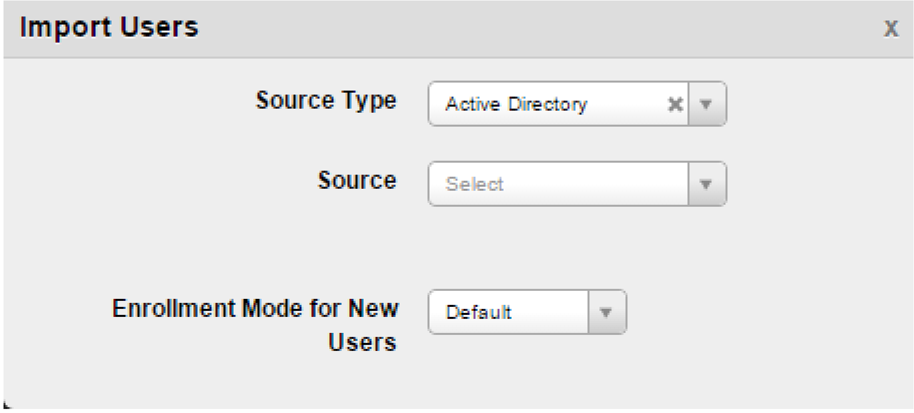
Before initiating a new request to import Users, as an Admin you must meet the following conditions:

- 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.



Import Users

Source Type: Active Directory

Source: Select

Enrollment Mode for New Users: Default

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.

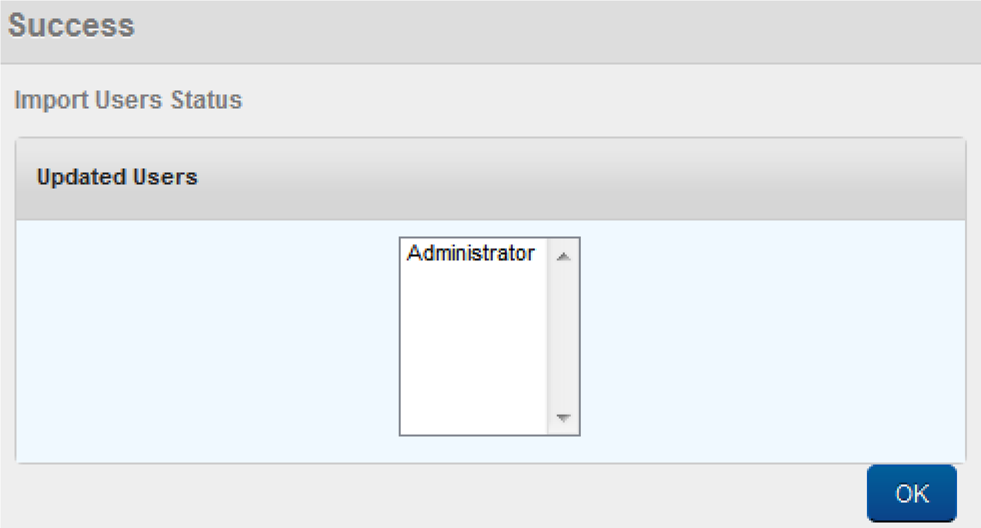
d. **Phone Number**: Enter phone number of the user in the Search Phone field.

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.



Success

Import Users Status

Updated Users

Administrator

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

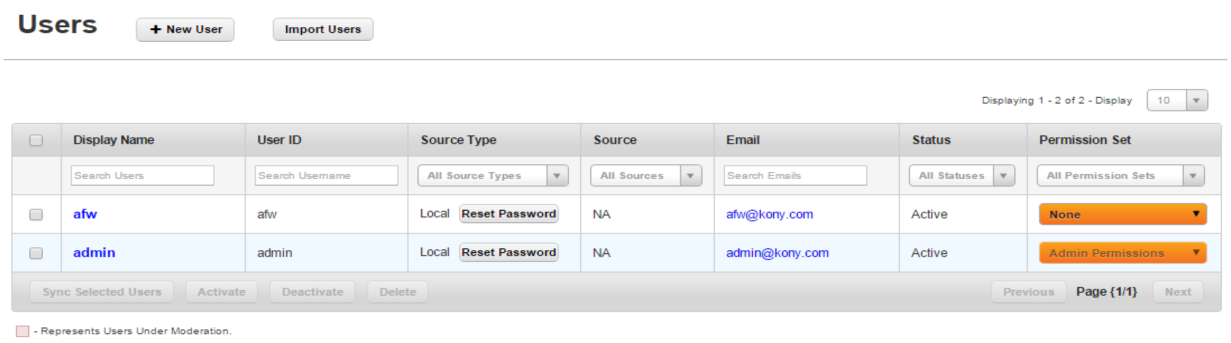
8.2.3 Automatic Creation of a New User Using Kony Fabric Data

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.

8.2.4 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

Displaying 1 - 2 of 2 - Display 10

☐	Display Name	User ID	Source Type	Source	Email	Status	Permission Set
	Search Users	Search Username	All Source Types	All Sources	Search Emails	All Statuses	All Permission Sets
☐	afw	afw	Local Reset Password	NA	afw@kony.com	Active	None
☐	admin	admin	Local Reset Password	NA	admin@kony.com	Active	Admin Permissions

▨ - 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.

8.2.5 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

8.2.5.1 Local User

To update a local user details, follow these steps:

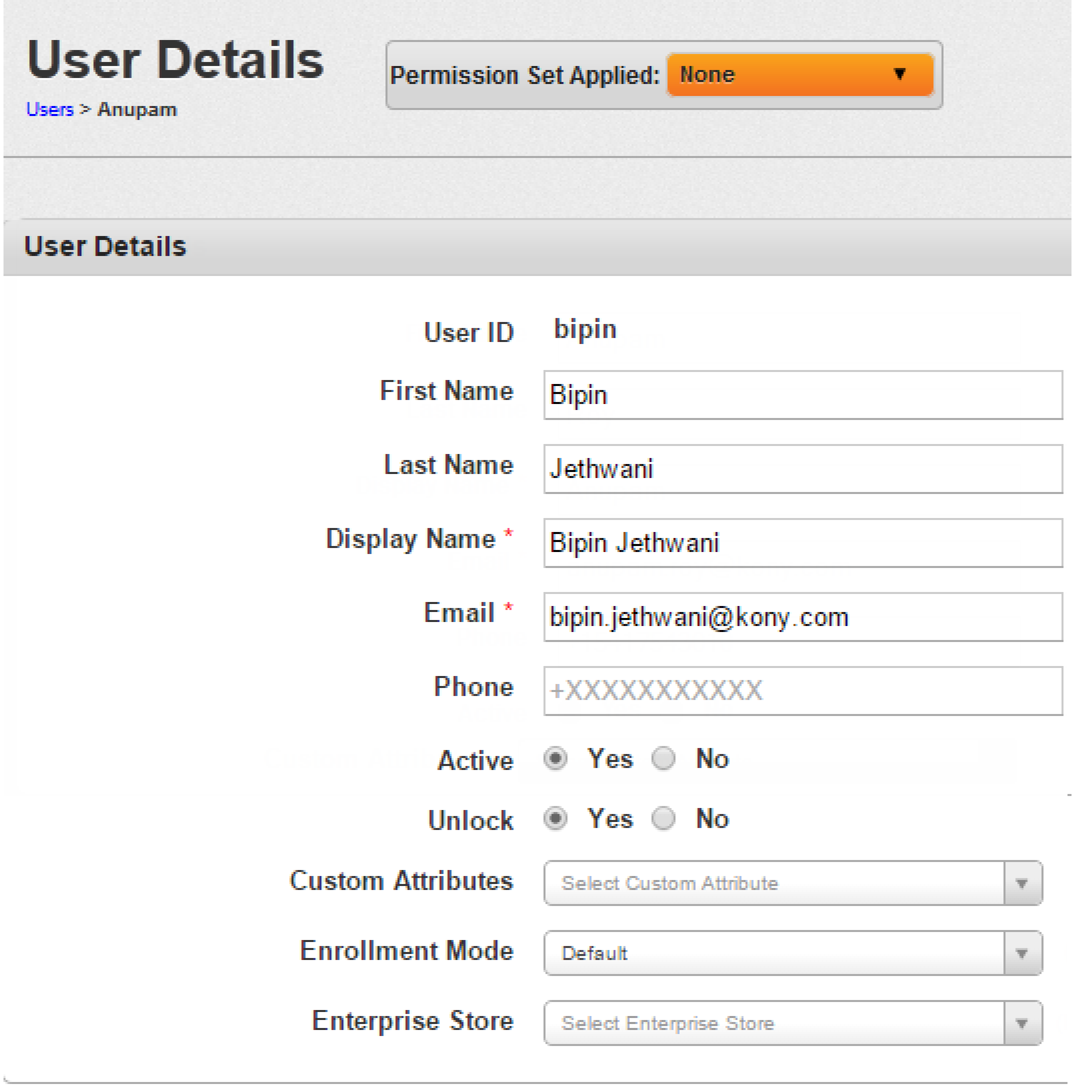
1. Select the user source as Local from the list view.

   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	Bipin
Last Name	Jethwani
Display Name *	Bipin Jethwani
Email *	bipin.jethwani@kony.com
Phone	+XXXXXXXXXXX
Active	● Yes ○ No
Unlock	● Yes ○ No
Custom Attributes	Select Custom Attribute ▼
Enrollment Mode	Default ▼
Enterprise Store	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.

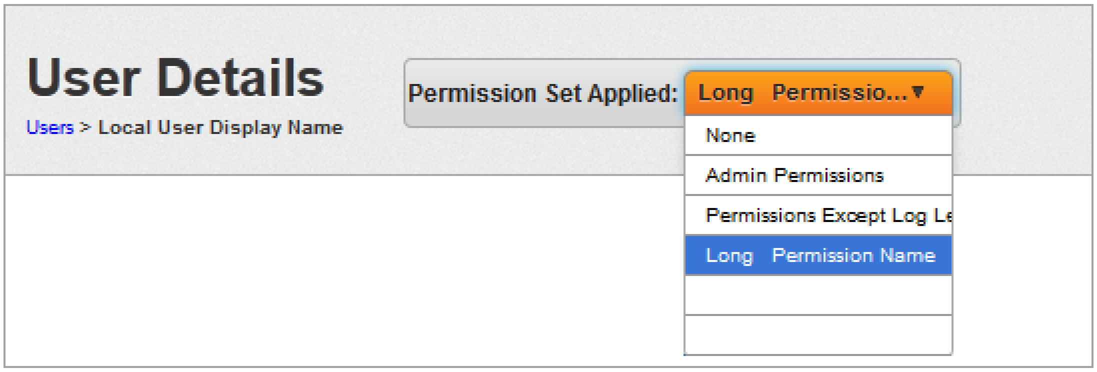
   By default, the user status is set to active. If required, you can change the user status to inactive.

   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.

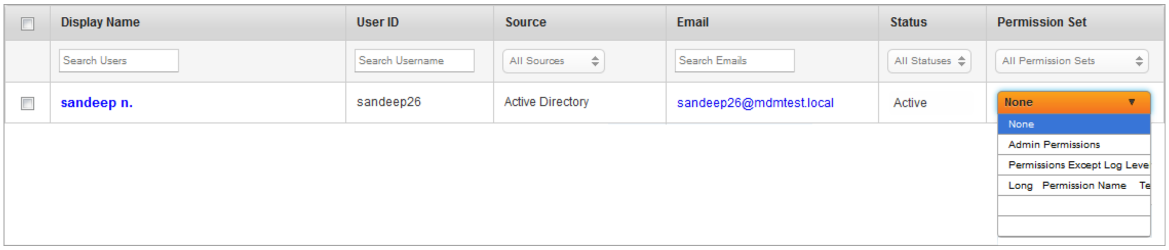


6. **Permission Set**: Select the required permission set from the **Permission Set Applied** drop-down list.

   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:



□	Display Name	User ID	Source	Email	Status	Permission Set
	Search Users	Search Username	All Sources	Search Emails	All Statuses	All Permission Sets
□	sandeep n.	sandeep26	Active Directory	sandeep26@mdmtest.local	Active	None

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.

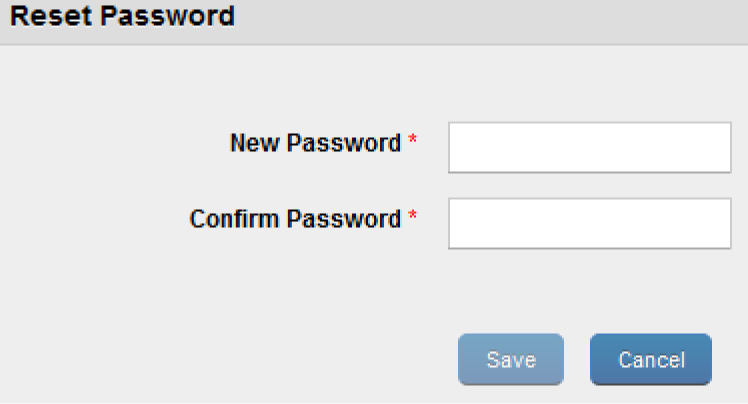
Reset Password

> *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 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.

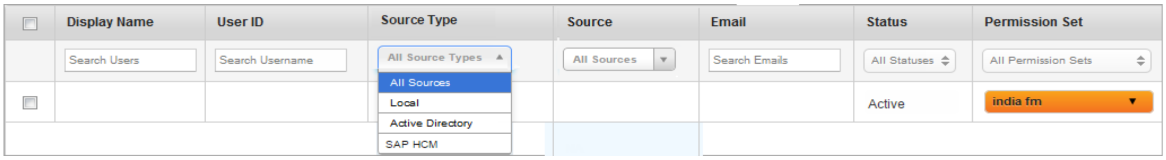
   A confirmation message about password acceptance appears.

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

   A confirmation message about password update appears.

8.2.5.2 Users imported from Active Directory

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



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.

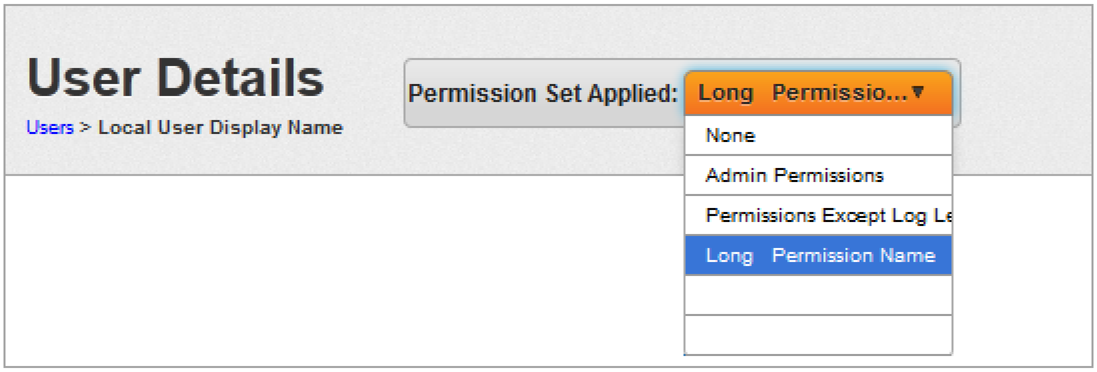
   User Details page appears.

   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	• 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.

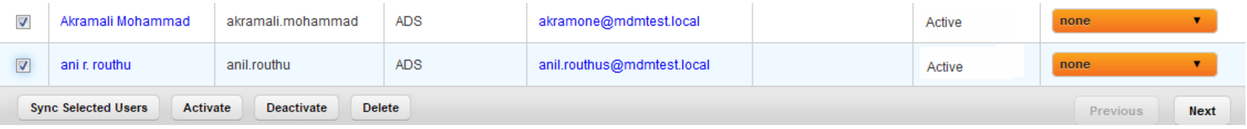
8.2.5.3 Cloud

Admin can create users with admin privileges for cloud environment. The created user can login into EMM Management Console through cloud login credentials.

8.2.6 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.

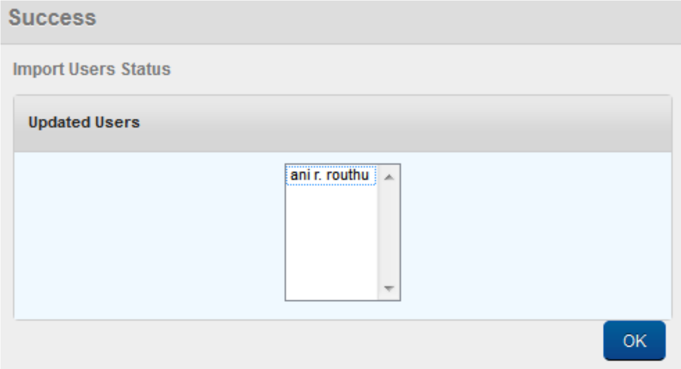
> ***Note:*** Synchronizing Users applies only to Users from multiple ADs. It does not apply to local Users.



☑	Akramali Mohammad	akramali.mohammad	ADS	akramone@mdmtest.local		Active	none ▼
☑	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.



Success

Import Users Status

Updated Users

ani r. routhu

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

8.2.7 Activating/Deactivating a User

If a User is deleted in the Active Directory, then the user should be deactivated in the EMM Access Management. When a user is deactivated, an enterprise wipe is done on all the user's devices and devices are also deactivated. This ensures that all policies and resources such as emails, Wi-Fi, VPN, and certificates are removed from the device. The User cannot be active and should be removed from all the Groups.

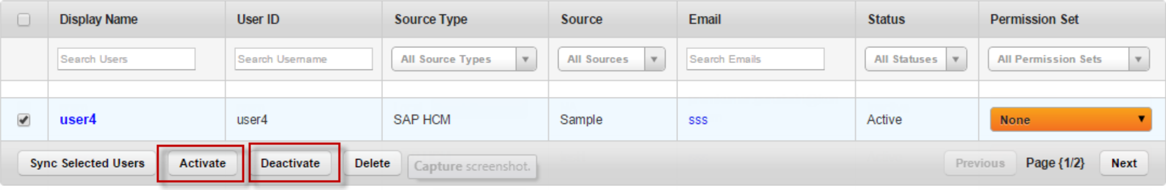
> *Important:* When any of the users (Local or AD) is deactivated, the user's association with the All group is removed. Once the user is activated again, the user is automatically added to the All group again.

If the User as an Admin created any entities, the user is still credited with the same entities - Applications, categories, device sets, 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.



☐	Display Name	User ID	Source Type	Source	Email	Status	Permission Set
	Search Users	Search Username	All Source Types ▾	All Sources ▾	Search Emails	All Statuses ▾	All Permission Sets ▾
☑	user4	user4	SAP HCM	Sample	sss	Active	None ▾

2. Click **OK** to continue. A confirmation message about activated/deactivated user status appears.

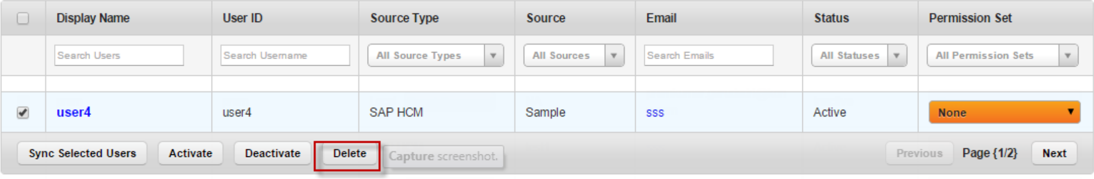
   The system changes the state of the User to Active/Inactive.

8.2.8 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.



☐	Display Name	User ID	Source Type	Source	Email	Status	Permission Set
	Search Users	Search Username	All Source Types ▾	All Sources ▾	Search Emails	All Statuses ▾	All Permission Sets ▾
☑	user4	user4	SAP HCM	Sample	sss	Active	None ▾

2. Click **OK** to continue. A confirmation message about deletion appears.

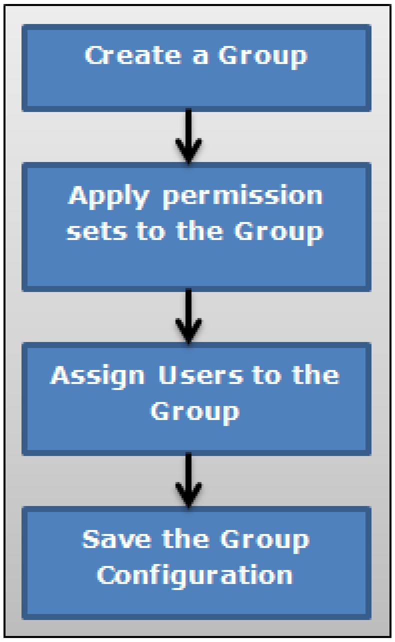
   The system deletes the user from the grid.

   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.

8.3 Groups

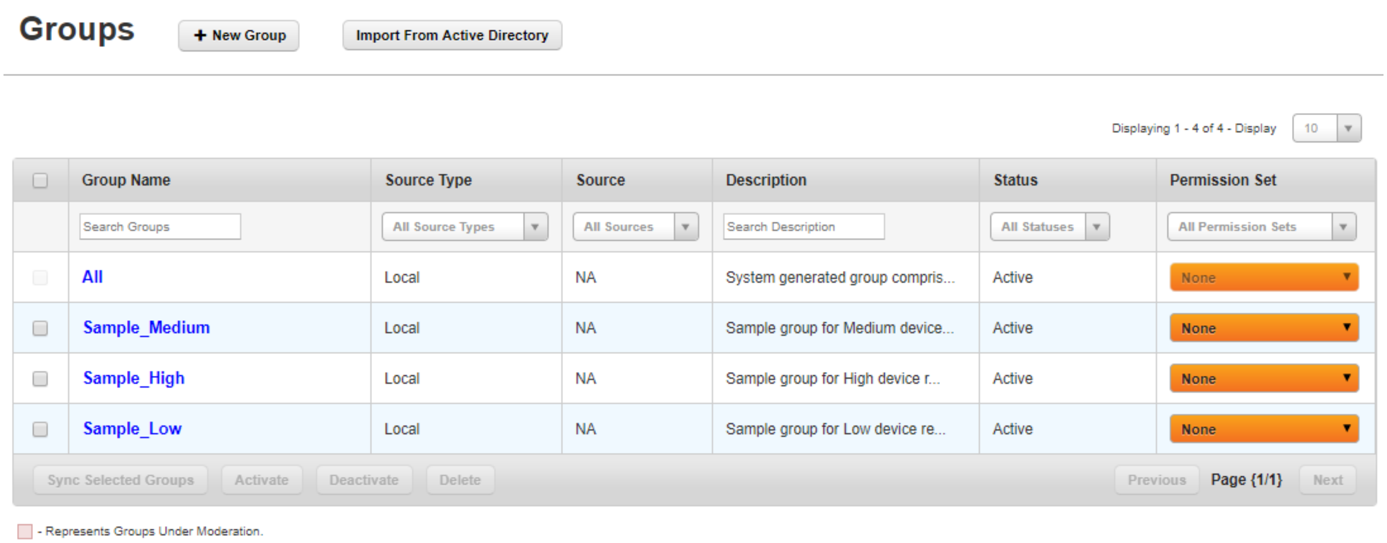
Groups represent a collection of users created to provide security options for domains and other business services. Using the permission sets, you can grant or deny a group access to one or more domains, or set privileges for individual services. In all, a group represents multiple users with the same requirement and authority to access particular business services.


Create a Group
Apply permission sets to the Group
Assign Users to the Group
Save the Group Configuration

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

Displaying 1 - 4 of 4 - Display 10

□	Group Name	Source Type	Source	Description	Status	Permission Set
	Search Groups	All Source Types	All Sources	Search Description	All Statuses	All Permission Sets
□	All	Local	NA	System generated group compris...	Active	None
□	Sample_Medium	Local	NA	Sample group for Medium device...	Active	None
□	Sample_High	Local	NA	Sample group for High device r...	Active	None
□	Sample_Low	Local	NA	Sample group for Low device re...	Active	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.

Several other default groups include Sample_Medium, Sample_High, and Sample_Low.

The default groups are associated with their respective default device sets. These devices sets are associated with some default device policies. When a user is assigned to a group, devices enrolled by the user are associated with the corresponding device set and device policies.

The grouping of Sample_High, Sample_Medium, and Sample_low is based on the following four policies.

- Public Apps Policy
- Compliance Policy
- Device Restrictions Policy
- Passcode Policy

In the Sample_High group, the restrictions for all the policies are high. In the Sample_ Medium group, the restrictions for all the policies are medium. In the Sample_ Low group, the restrictions for all the policies are low.

For more information, you can open each one the policy and check the configuration.

When a user is added to a particular group (for example Sample_High), the user gets associated with the Device set Sample_High, and all the policies that are available in that device set will apply on the devices enrolled by the user.

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	If selected at row level, the particular group is selected for any further actions. Multiple rows can also be selected. Selection can only be done on a single page of records. You can choose to display upto 100 records (groups).
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.

Columns	Description
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	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 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.
Delete	Selected groups cab 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:

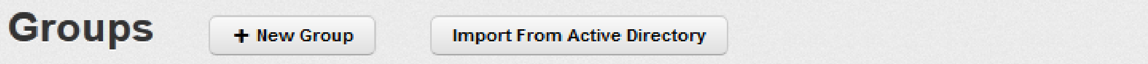
- Creating a New Group
- Importing Groups from the Active Directory
- Searching for Groups
- Updating a Group
- Sync Selected Group

- Deactivating a Group
- Deleting a Group

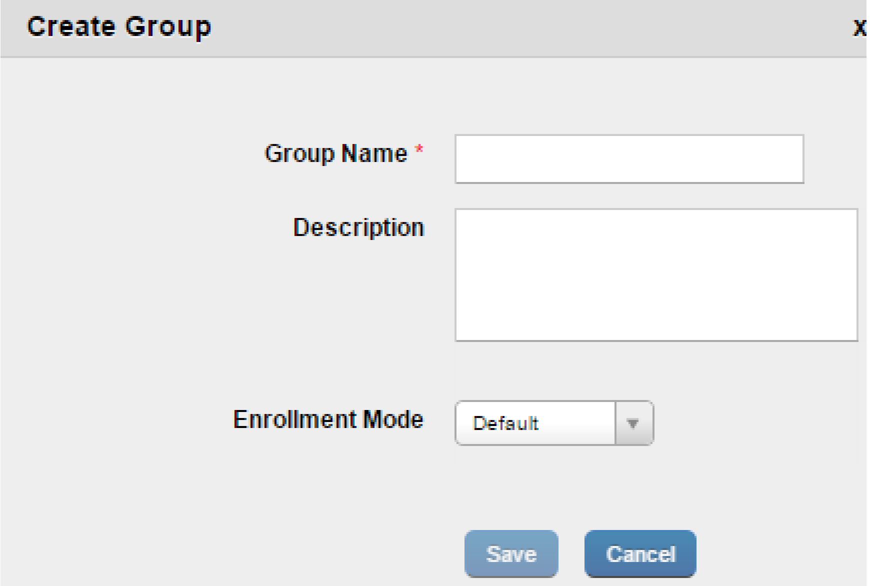
8.3.1 Creating a New Group

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 **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.

8.3.2 Importing Groups from the Active Directory

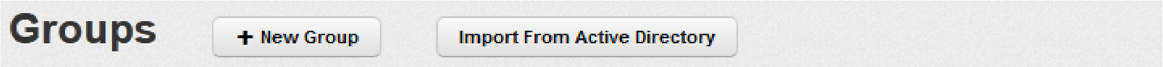
You can also add groups to the EMM database by importing them from the Active Directory, using the **Import Groups from Active Directory** window.

> *Note:* Users imported into Kony Management Suite with this method (Importing Groups from Active Directory) will also be part of the default **All** group.

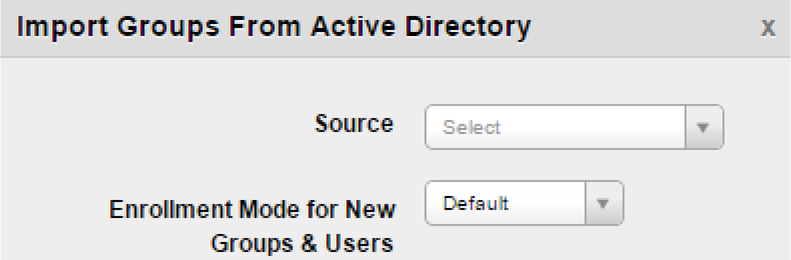
> *Important:* If you move users from one Active Directory group to another, this may result in app un-targetting and re-targetting users who are moved.

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.



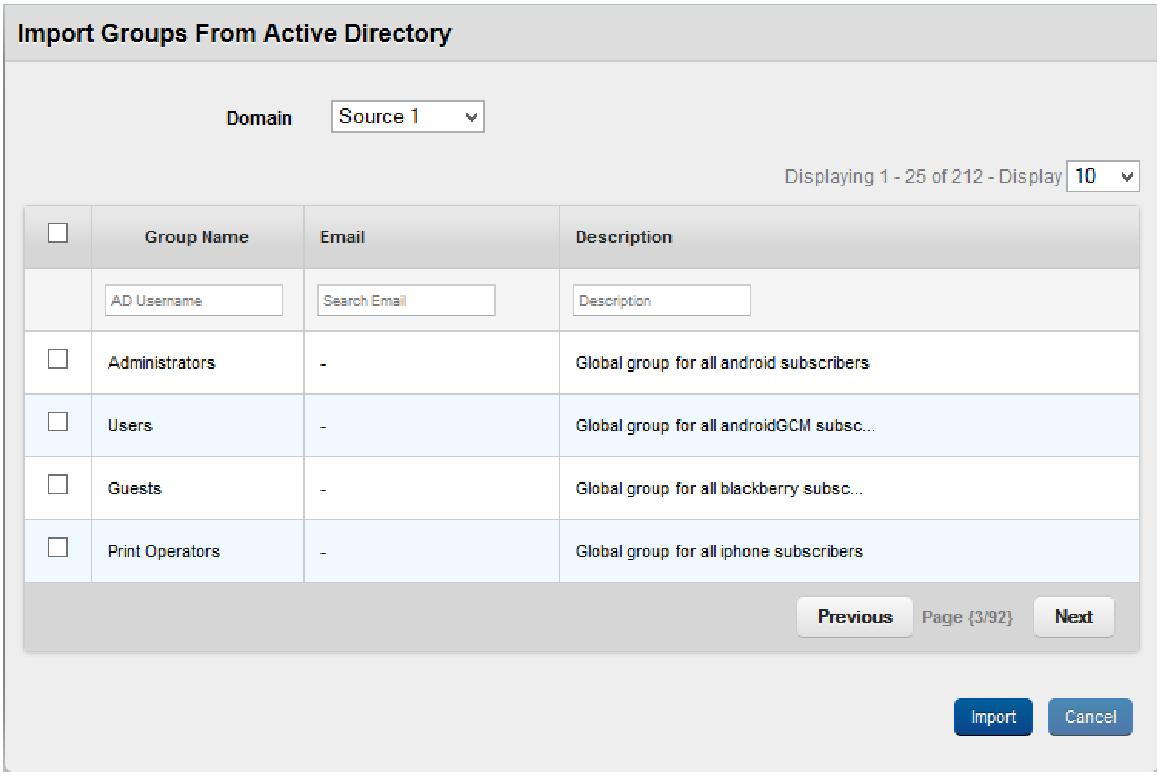
Import Groups From Active Directory

Source: Select

Enrollment Mode for New Groups & Users: Default

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: Source 1

Displaying 1 - 25 of 212 - Display 10

□	Group Name	Email	Description
	AD Username	Search Email	Description
□	Administrators	-	Global group for all android subscribers
□	Users	-	Global group for all androidGCM subsc...
□	Guests	-	Global group for all blackberry subsc...
□	Print Operators	-	Global group for all iphone subscribers

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.

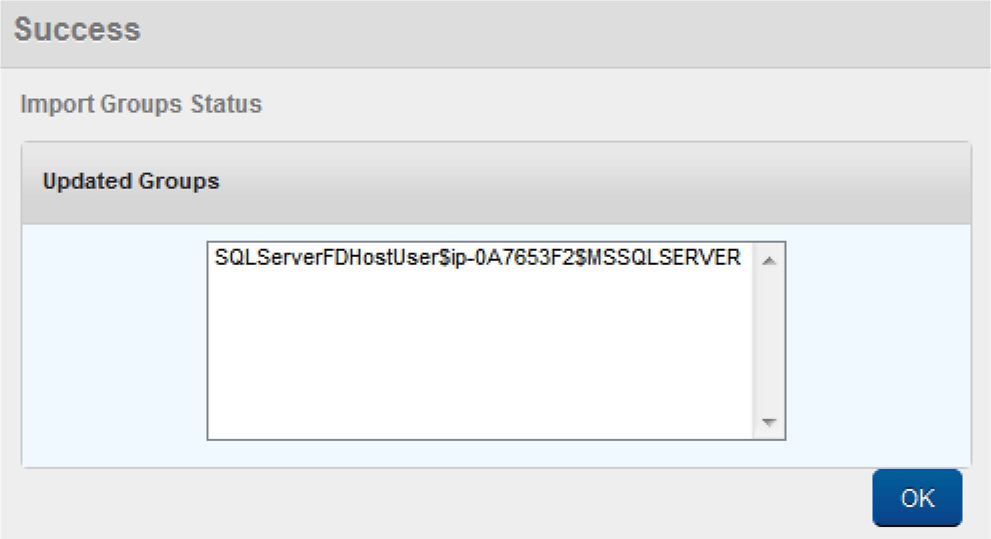
   a. **Group Name**: Enter partial or complete name of the group in the **Search Groups** field.

   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.



SQLServerFDHostUser$ip-0A7653F2$MSSQLSERVER

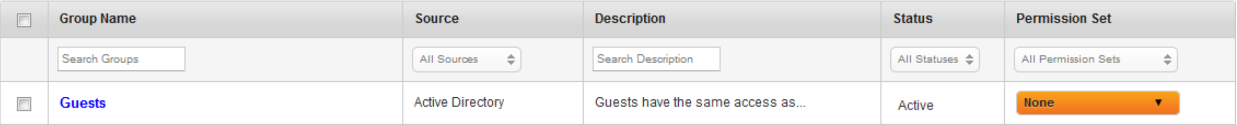
7. Click the **OK** button to return to the main page. The Groups thus selected are copied to the EMM database and displayed in the Groups List page.

The following table provides additional information about Groups:

Properties	Description
Group Name	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. • 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.

8.3.3 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.



☐	Group Name	Source	Description	Status	Permission Set
	Search Groups	All Sources	Search Description	All Statuses	All Permission Sets
☐	Guests	Active Directory	Guests have the same access as...	Active	None

1. Enter or select details for following search filters:

   a. **Group Name**: Enter partial or complete name of the group in the **Search Groups** field.

   b. **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.

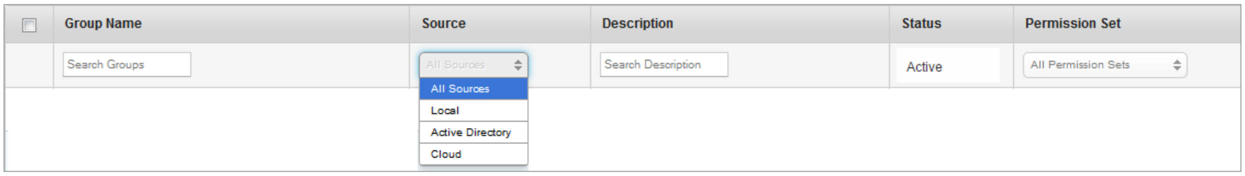
8.3.4 Updating a Group

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

8.3.4.1 Local Group

To update a local group details, follow these steps:



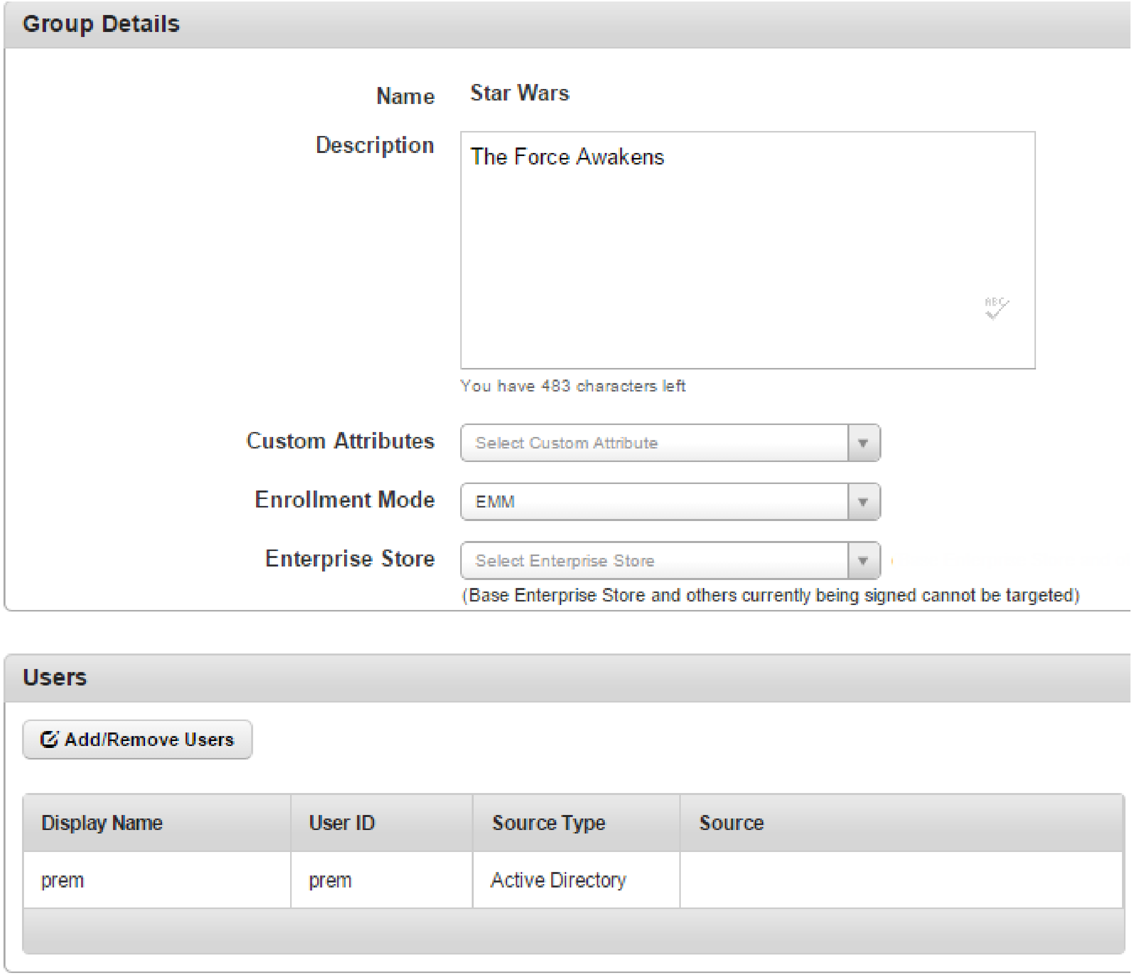
□	Group Name	Source	Description	Status	Permission Set
	Search Groups	All Sources	Search Description	Active	All Permission Sets

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	The Force Awakens You have 483 characters left
Custom Attributes	Select Custom Attribute
Enrollment Mode	EMM
Enterprise Store	Select Enterprise Store (Base Enterprise Store and others currently being signed cannot be targeted)

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.

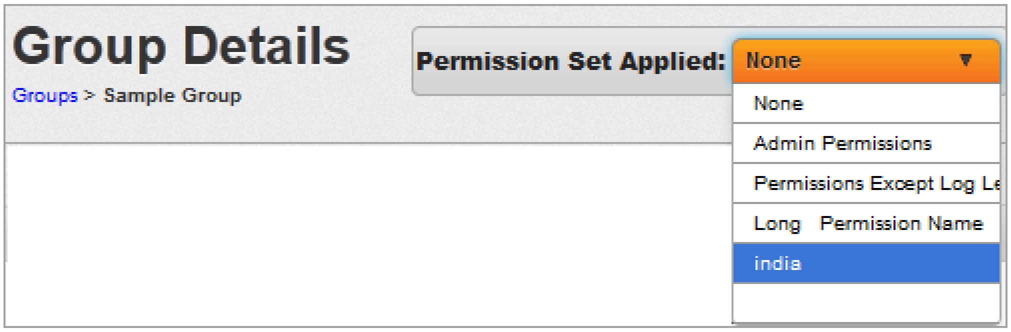
   a. To assign a user, use the left single-arrow icons to select the user.

   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

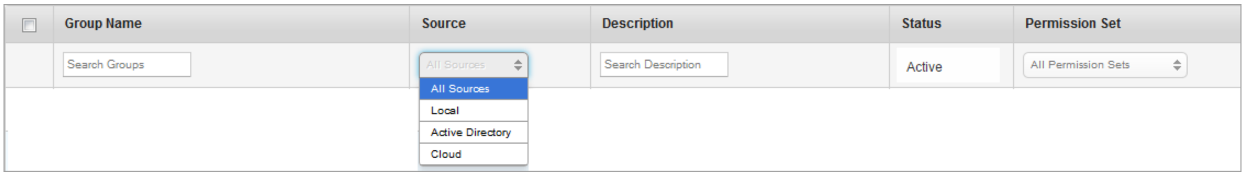
c. A confirmation message about changed permission set appears. Click **OK** to return to the main page.

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.

8.3.4.2 Group imported from Active Directory

To update an Active Directory group, follow these steps:



☐	Group Name	Source	Description	Status	Permission Set
	Search Groups	All Sources	Search Description	Active	All Permission Sets

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

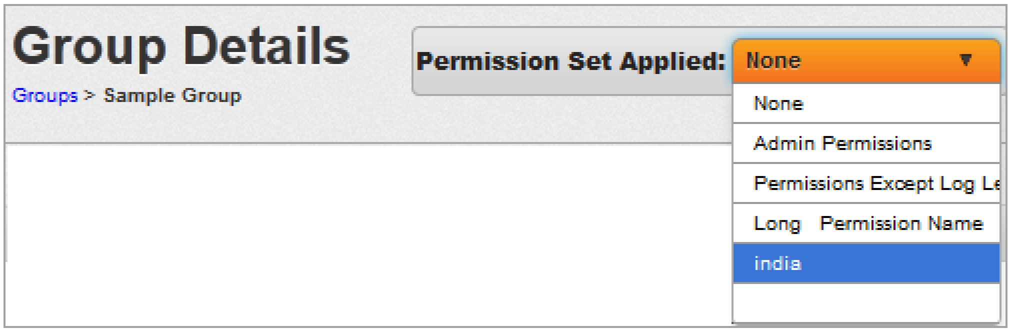
   A list of Active Directory groups appears in the list view.

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.

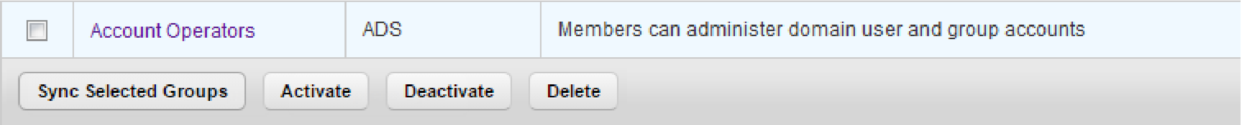


6. **Permission Set**: Select the required permission set from the **Permission Set Applied** drop-down list. All the permissions granted in the Permission Set automatically gets applied to all the Users that are part of the Group.
7. Click the **Save** button to save the details.In the message that appears, click **OK** to return to the main page. The updated Group details with applied permission set appear in the list view

8.3.5 Sync Selected Group

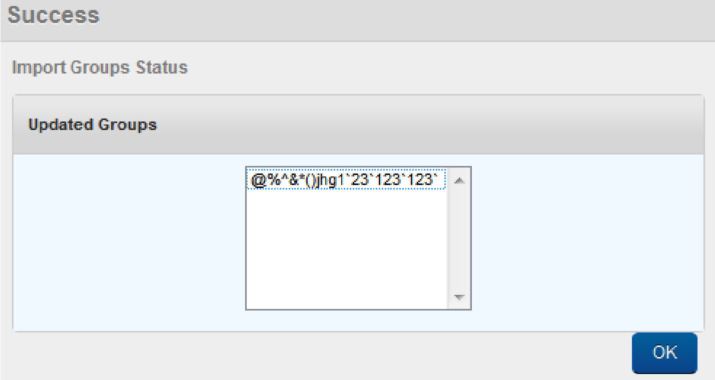
The Admin can choose to synchronize an individual AD group or multiple groups. This action synchronizes all details with regards to that Group. This includes importing any new User as part of the group who are currently not part of EMM. It also includes removing any User or Users from the Group or Groups. This action is limited to AD Groups.

To Sync selected groups, follow these steps:



☐	Account Operators	ADS	Members can administer domain user and group accounts

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.



Success

Import Groups Status

Updated Groups

@%^&*()jhg1`23`123`123`

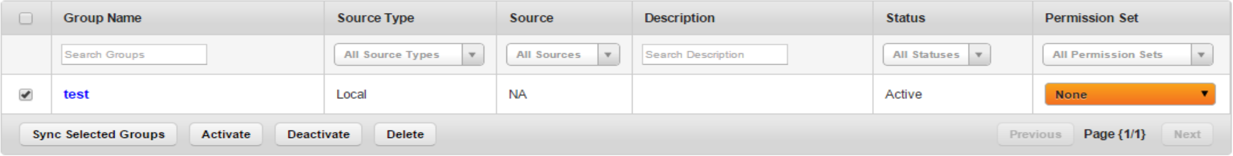
3. Click the **OK** button to return to the main page.

8.3.6 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:



□	Group Name	Source Type	Source	Description	Status	Permission Set
	Search Groups	All Source Types	All Sources	Search Description	All Statuses	All Permission Sets
☑	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.

8.3.7 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**.

8.4 Enrollment Mode

The Enrollment Mode page in the Kony Management Suite Access Management section enables a user to manage the enrollment modes for various users and groups. You can view details of all groups and users who are enrolled into Kony Management Suite.

Using the Enrollment Mode page, you can change the enrollment modes of various users and groups from a Kony Management Enterprise Mobile Management (EMM) mode to Kony Management Mobile Content Management/Mobile Application Management mode in a single instance.

With the EMM enrollment mode, you can manage devices, applications, and content.

Using the MAM/MCM enrollment mode, you can only manage applications and content.

If you are using an external product for your mobile device management, you can still use Kony Management in the MAM/MCM enrollment mode.

If at a later point, if you want to add the device management capability, you can do that by changing the enrollment mode to EMM.

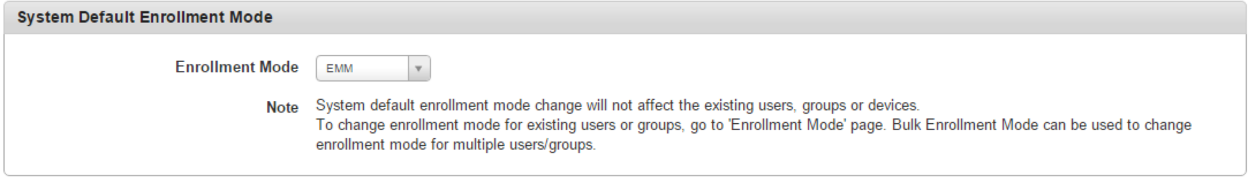
For more information on changing from EMM to MAM/MCM enrollment mode, click here.

For more information on changing from MAM/MCM to EMM enrollment mode, click here.

The enrollment page displays data about users and groups.

8.4.1 System Default Enrollment Mode

This section displays the system default enrollment mode setting.



System Default Enrollment Mode

Enrollment Mode: EMM

Note: System default enrollment mode change will not affect the existing users, groups or devices.
To change enrollment mode for existing users or groups, go to 'Enrollment Mode' page. Bulk Enrollment Mode can be used to change enrollment mode for multiple users/groups.

Enrollment Mode Settings

- **Enrollment mode**: By default, this is configured to **EMM**. You can change this to **MAM/MCM**.

An administrator cannot change a user's enrollment mode under the following conditions:

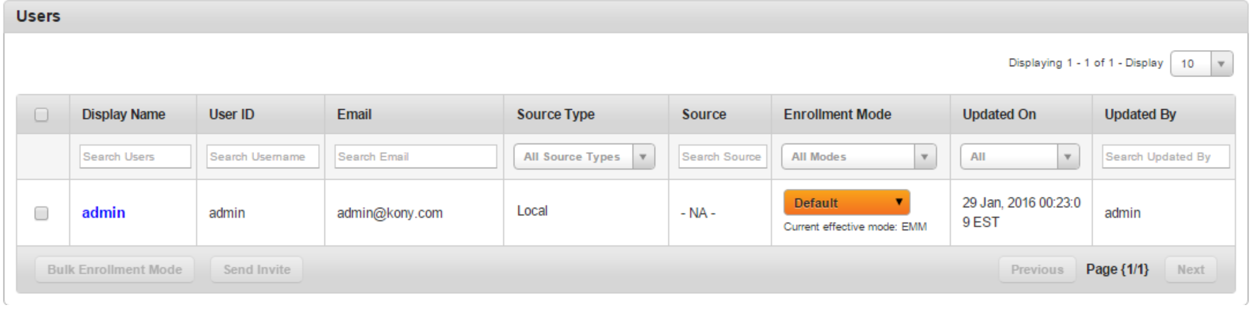
- If a device is in a suspended state due to any compliance action.
- If a device is in a suspended state because of any administrator action.
- If a device is in a suspended state because of exceeding the wrong no of failed attempts limit.
- If the **Allow log in to rooted/jailbroken** feature in the Device settings section is device is set to **No** after the device enrollment.

The administrator must manually release devices from suspended state for the enrollment mode change to reflect on these devices.

Whenever the enrollment mode changes, user has to accept terms and conditions again. Currently, there is no provision for separate Terms and Conditions for EMM and MAM/MCM enrollment modes.

8.4.2 Users

The Users section displays a list of all the users along with other details.



Users

Displaying 1 - 1 of 1 - Display 10

□	Display Name	User ID	Email	Source Type	Source	Enrollment Mode	Updated On	Updated By
	Search Users	Search Username	Search Email	All Source Types	Search Source	All Modes	All	Search Updated By
□	admin	admin	admin@kony.com	Local	- NA -	Default Current effective mode: EMM	29 Jan, 2016 00:23:09 EST	admin

The Users list view displays the following columns:

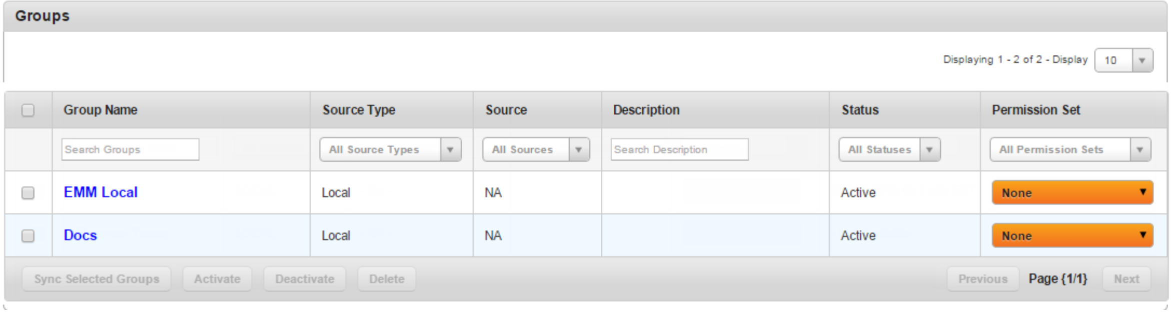
Column	Description
Select check box	If selected at the row level, the particular user is selected for any further actions. Multiple rows can also be selected. Selection can only be done on a single page of records. You can choose to display up to 100 records (users).
Display Name	Displays the First Name and the Last Name of the user.
User ID	Displays the User ID of the user.
Email	Displays the email ID as received from the Active Directory or as specified by the administrator.
Source Types	Displays source types that belongs to the user. If it is a local user, the system displays as NA
Source	Displays source that belongs to the user. If it is a local user, the system displays as NA
Enrollment Mode	Displays the enrollment mode of the user. Options are EMM, MAM/MCM, and Default.

Column	Description
Updated On	Displays the date and time the user was updated on.
Updated By	Displays the user who updated the user details.
Bulk Enrollment Mode	Using this button, you can change the enrollment mode when you select multiple users. This button is only active if the check box next to Display Name is selected or if the multi-select check box is selected.
Send Invite	Using this button, you can send invites to selected users for selected enrollment mode. 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.

8.4.3 Groups

The Groups section displays a list of all the groups along with other details.



Groups

Displaying 1 - 2 of 2 - Display 10

□	Group Name	Source Type	Source	Description	Status	Permission Set
	Search Groups	All Source Types	All Sources	Search Description	All Statuses	All Permission Sets
□	EMM Local	Local	NA		Active	None
□	Docs	Local	NA		Active	None

The Groups list view displays the following columns:

Column	Description
Select check box	If selected at the row level, the particular group is selected for any 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 (groups).
Group Name	Displays the group name.
Source Type	Displays source type that belongs to the group.
Source	Displays source that belongs to the group.
Description	Displays the group description.
Enrollment Mode	Displays the enrollment mode of the group. Options are EMM, MAM/MCM, and Default.
Updated On	Displays the date and time the group was updated on.
Updated By	Displays the user who updated the group details.
Bulk Enrollment Mode	Using this button, you can change the enrollment mode when you select multiple users. This button is only active if the check box next to Display Name is selected or if the multi-select check box is selected.
Send Invite	Using this button, you can send invites to selected users for selected enrollment mode. 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 tasks in the Enrollment Mode page.

- Modifying Enrollment Mode for users or groups in bulk
- Send invitations to groups or users for enrollment

8.4.4 Modifying Enrollment Mode for Users or Groups in Bulk

To modify the enrollment mode for users or groups in bulk, do the following:

1. In the **Enrollment Mode** page, select the users or groups you want to change the enrollment mode in bulk. The **Bulk Enrollment Mode** field appears.
2. Click **Bulk Enrollment Mode**. The **Bulk Enrollment Mode** page appears.
3. From the **Enrollment Mode** list, select the enrollment mode. Options are EMM, MAM/MCM, and Default. The **Change Enrollment Mode** button appears.
4. Click **Change Enrollment Mode**. A success page appears.
5. Click **OK**. The users or groups enrollment mode is modified.

8.4.5 Sending Invitations to Users or Groups to Enroll

To send invitations to users or groups to enroll into Kony Management Suite, do the following:

1. In the **Enrollment Mode** page, select the users or groups you want to send the invite to enroll into Kony Management Suite. The Send Invite field appears.
2. Click **Send Invite**. The **Confirm** page appears.
3. Click **Yes** to send the invite. A success page appears.
4. Click **OK**. The invitation to the user or group to enroll into Kony Management Suite is sent.

8.4.6 Impact of Switching an Enrollment Mode from EMM to MAM/MCM

When a user or group's enrollment mode is switched from EMM to MAM/MCM,

- All user's devices are logged out of their current sessions.
- A platform specific command is sent to log out from the Enterprise store.
- Heartbeat timer is disabled in the enterprise store.
- User devices are skipped from Watchdog and Device check-in actions.
- User devices are excluded from all Device set change and Policy change events.
- All MDM commands are disabled on user's devices.
- Exchange services and enterprise resources will not be available.
- Enterprise store switches to MAM/MCM mode. These changes are specific to each platform.
    - Windows
        - The server records a list of non-mandatory installed enterprise apps and then initiates license switch.
        - Workplace MDM wipe command is initiated.
        - The user has to once again enroll with the in MAM/MCM mode.
        - The server initiates enterprise wipe. This will remove all managed apps, but the MDM profile and are not removed.
        - User must wait for the workplace account to be deleted on the device.
        - VPN configuration will be revoked.
        - All device policies will be revoked.
        - Consumed VPP app licenses will be released.

    - All devices will be removed from device sets.

    > *Important:* When a user moves from EMM to MAM/MCM mode, if the user’s device is in **Denied future enrollment** by an administrator or through a compliance policy, the device would not be blocked for enrollment in MAM/MCM mode.

- iOS
    - The server records a list of non-mandatory installed enterprise apps and then initiates license switch.
    - The server initiates enterprise wipe. This will remove all managed apps, but the MDM profile and Enterprise store are not removed.
    - The device will be in MAM/MCM mode after re-login and shows the new Terms and Conditions page.
    - If there are any pending app installations on the device, a prompt to install this app will appear. If the user cancels the app install, the prompt will not appear again.
    - App usage report does not work for Windows. A trigger to push a requesting child apps for usage statistics can not be sent for the Windows phones. This is a limitation.
    - The Managed App configuration will be revoked.
    - VPN configuration will be revoked.
    - All device policies will be revoked.
    - Consumed VPP app licenses will be released.
    - All devices will be removed from device sets.

- Android
    - The server will send a STOP MDM command to the device which remove all currently applied MDM policies.
    - All enterprise apps will be retained. Administrator rights are also left as it.
    - All device policies will be revoked.
    - Consumed VPP app licenses will be released.
    - All devices will be removed from device sets.

8.4.7 Impact of Switching an Enrollment Mode from MAM/MCM to EMM

When a user or group's enrollment mode is switched from MAM/MCM to EMM,

- All user's devices are logged out of their current sessions.
- The user's device list page reflects the enrollment mode as EMM.

> ***Important:*** It may take a while for the enrollment mode to switch from MAM/MCM mode to EMM mode. During the transition state, MDM specific features (buttons and options in drop-down lists) will not be available. Once the transition is complete, all features will be available.

- All device policies will be resolved as per configured device sets. Applicable policies will be applied.
- Enterprise store switches to EMM. Changes are specific to each platform.
    - Windows
        - The server records a list of non-mandatory installed enterprise apps and then initiates license switch.
        - Existing Enterprise app store is deleted. The Kony aetx certificate is

removed. The user must enroll again through workplace enrollment.

    - Previously installed apps are reinstalled again. If there are any pending app installations on the device, a prompt to install the app will appear. If the user cancels the app install, the prompt will not appear again.

    - User does not have to delete the workplace account unlike in the EMM to MAM/MCM mode. Existing Enterprise store and Enterprise Apps will be replaced. All MDM policies will be automatically applied.

- iOS

    - The server sends a log out push to the device.

    - The user must delete all enterprise apps from the device.

    - If the user does not delete existing enterprise apps, apps will work in the MAM/MCM mode. Device policies will not be honored and MDM policy will be applied to apps.

    - The user must re-enroll the device.

    - Records a list of non-mandatory installed enterprise apps and then initiates license switch.

    - Enterprise Store will be in EMM mode after re-login and shows the new Terms and Conditions page.

    - If there are any pending app installations on the device, they are automatically installed on the device.

    - MDM push starts working.

- Android

    - The user will be prompted to allow administrator permissions for Enterprise store. Enterprise apps will be retained as they are and MDM policies will be applied.

8.4.8 Frequently Asked Questions

When a device is offline, if the device's enrollment mode is changed, how will the device behave when it is online?

The user will be logged out from the store and a notification will appear on the device about the enrollment mode change. The user must enroll the device again and log in.

8.4.9 Availability of Features in EMM and MAM/MCM Enrollment Mode

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Dashboard	Total Non-Compliant Devices - Count	Available	Not available.
	Locations	Available	Not available.
	Compliance Chart	Available	Not available.
Reports	Compliance Action Report	Available	Not available. When a user is moved from EMM to MAM/MCM mode, old data(when user is in EMM mode) generated for compliance action will be shown in the report.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Enterprise Apps	iOS - Managed Apps Configuration	Available	Not available. When a user is moved from EMM to MAM/MCM, these will be revoked.
	iOS - VPN	Available	Not available. When a user is moved from EMM to MAM/MCM, VPN will be revoked.
	Windows - VPN	Available	Not available. When a user is moved from EMM to MAM/MCM, VPN will be revoked.
App Policies	App Usage - Device Policy	Available	Not available. Device policies will be revoked when device is moved from EMM to MAM/MCM.
VPP apps	VPP apps	Available	Not available. When device is moved from EMM to MAM/MCM, consumed app licenses will be released.
Device Sets	Device Sets	Available	Not available. When a user is moved from EMM to MAM/MCM the device will be removed from the device sets as well.
Device Enrollment	New Device	Available	Available
	Bulk Enroll Devices	Available	Available

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Device Policies	Device Policies	Available	Not available. When a user is moved from EMM to MAM/MCM, these will be revoked.
Application Settings	Usage Settings- Online Login - Web and Enterprise Store - Require captcha- Enterprise wipe	Available	Not available. When wrong captcha is given and wipe condition is met, nothing happens.
	VPP Apps	Available	Not available.

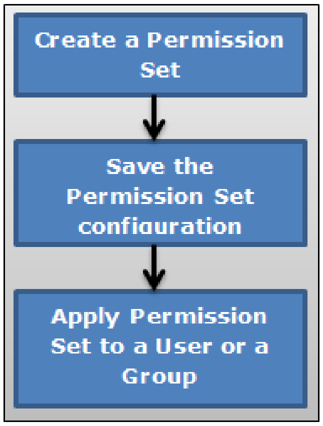
Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Device Settings	Usage Configuration- Heartbeat Settings	Available	Not available.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
	Usage Configuration- Enrollment Settings	Available	Not available.
	Usage Configuration- Watchdog Settings	Available	Not available.
	Usage Configuration- Tracking Settings - Enable viewing device location	Available	Not available.
	Usage Configuration- Tracking Settings - Allow Mock Location	Available	Not available.
	Usage Configuration- Tracking Settings- Allow User installed applications that have mock location permission	Available	Not available.
	Usage Configuration- Communication logs (SAFE, Android)	Available	Not available.
	Usage Configuration- SAFE Settings (Android)	Available	Not available.
	Usage Configuration- Mail+ for Enterprise	Available	Not available.

Kony Management Console Section	Feature Name	EMM Enrollment Mode	MAM/MCM Enrollment Mode
Exchange Services	Exchange Services	Available	Not available.
Enterprise Resources	Enterprise Resources	Available	Not available.
Even Log	Even Log	Available	Not available.

8.5 Permission Set

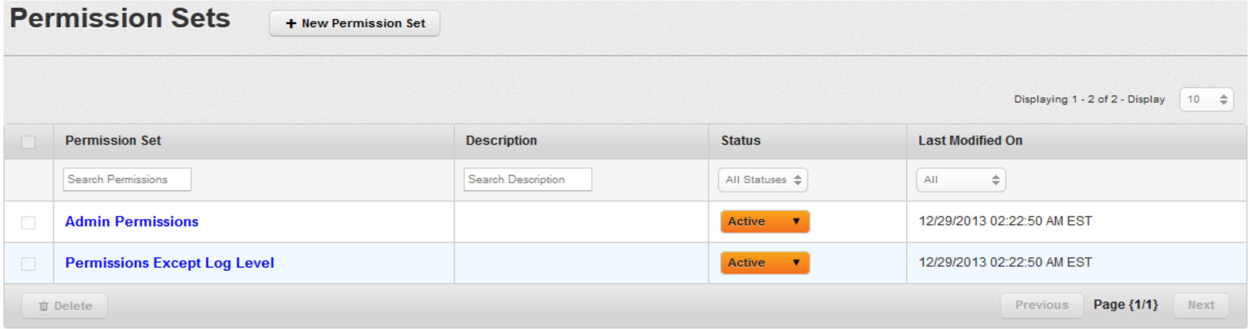
A permission set is a collection of settings that give users access to various functions on a page. Permission set may be granted to any number of users. For example, in the enrollment page, the User is allowed to add a new Device. While users can have only one profile, they can have multiple permission sets.


Create a Permission Set
Save the Permission Set configuration
Apply Permission Set to a User or a Group

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.



Displaying 1 - 2 of 2 - Display 10

□	Permission Set	Description	Status	Last Modified On
	Search Permissions	Search Description	All Statuses	All
□	Admin Permissions		Active	12/29/2013 02:22:50 AM EST
□	Permissions Except Log Level		Active	12/29/2013 02:22:50 AM EST

Page {1/1}

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.

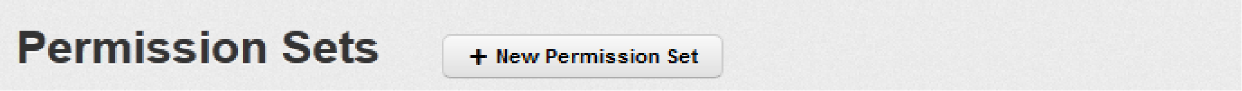
You can perform the following activities from the Permission Set page:

- Creating a Permission Set
- Updating a Permission Set
- Searching for Permission Sets
- Activating/Deactivating a Permission Set
- Deleting Permission Sets

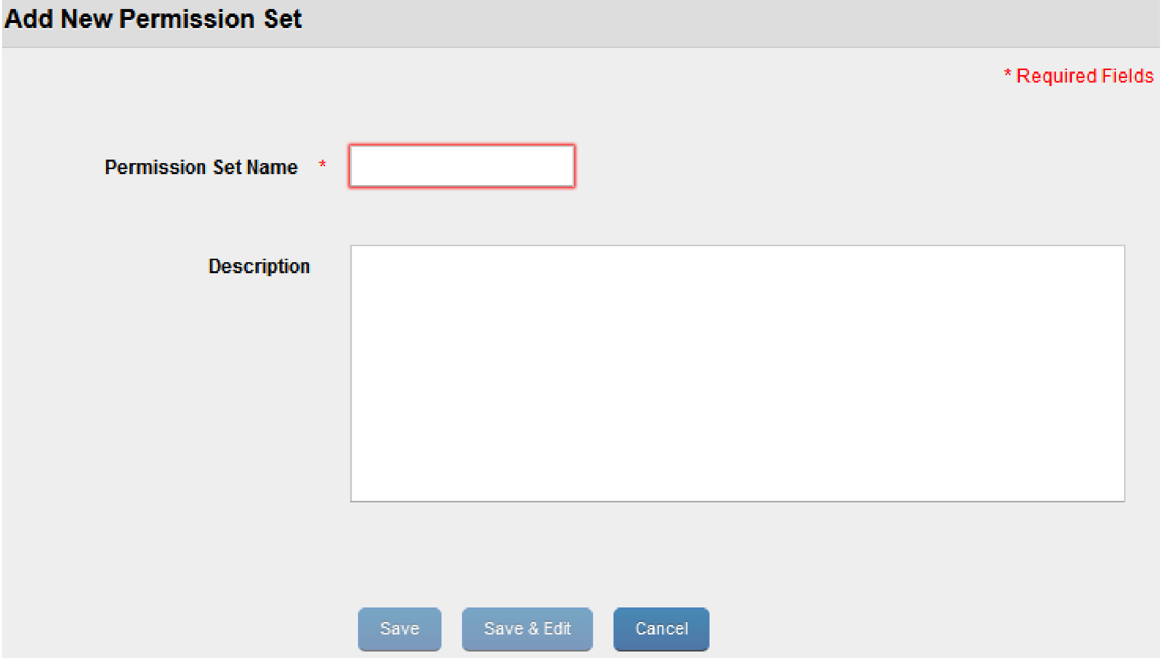
8.5.1 Creating a Permission Set

Only an Admin can create a Permission Set.

To create a Permission Set, follow these steps:



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 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.

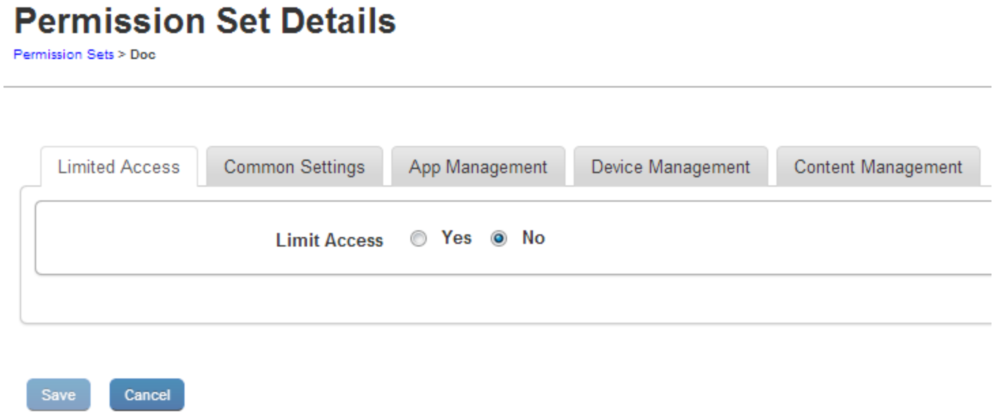
8.5.2 Adding/Updating a Permission Set

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

Limit Access ○ Yes ● No

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 polices.
  - **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.

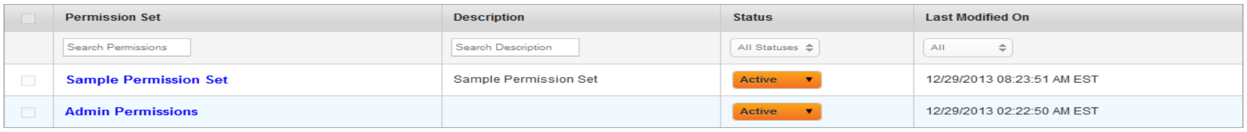
    - **Content Policies**: Set to **Yes** to view and access the link on the left navigation panel to the Content Policies page. This is a pre-requisite for Content Policy Details and all actions under Content Policies.
    - **Content Policies Details**: Set to **Yes** to view content policy details. This 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.

8.5.3 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.



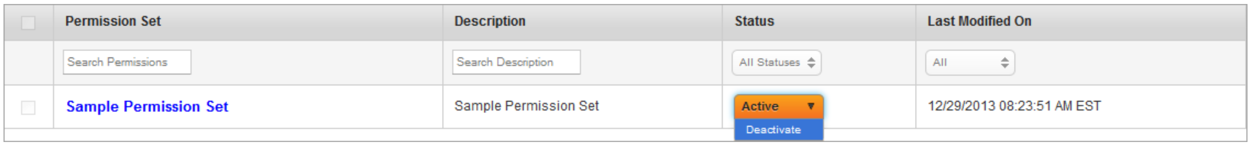
□	Permission Set	Description	Status	Last Modified On
	Search Permissions	Search Description	All Statuses ⬍	All ⬍
□	Sample Permission Set	Sample Permission Set	Active ▼	12/29/2013 08:23:51 AM EST
□	Admin Permissions		Active ▼	12/29/2013 02:22:50 AM EST

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.

8.5.4 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
	Search Permissions	Search Description	All Statuses	All
☐	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.

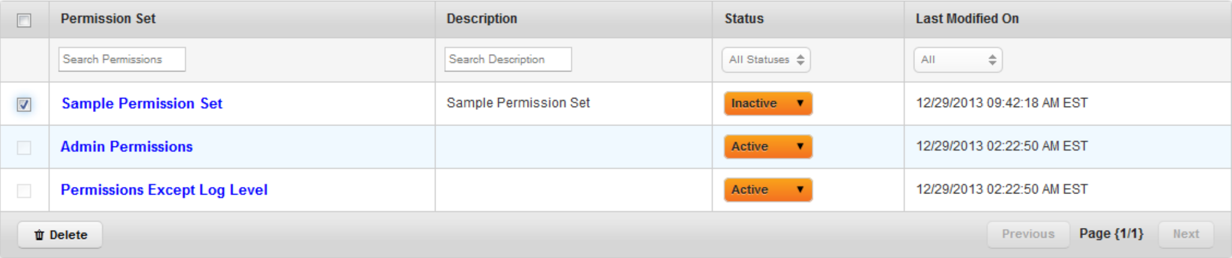
3. Click **OK** to return to the main page.

8.5.5 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:



□	Permission Set	Description	Status	Last Modified On
	Search Permissions	Search Description	All Statuses	All
☑	Sample Permission Set	Sample Permission Set	Inactive ▼	12/29/2013 09:42:18 AM EST
□	Admin Permissions		Active ▼	12/29/2013 02:22:50 AM EST
□	Permissions Except Log Level		Active ▼	12/29/2013 02:22:50 AM EST

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.

8.5.6 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

8.5.7 Limited Access to Users, Groups and Device List

EMM allows a super administrator to create permission sets that grant an administrator access to specific users, groups, and devices enrolled with those users and groups. Administrators who have a particular permission set can only view:

- Sources (In the Directories page) as granted.
- Groups (in the Group list) as granted.
- Users (in the User list) as granted.
  All Users that are part of the Groups selected or Users selected individually.
- Devices (in the Device list) that are enrolled with Users as specified above.
- Device Sets created by the limited administrator.
- User Space and Shared Space details for the Users in purview.
- Users and Groups in purview while targeting apps and content.
- Groups while trying to add groups into Enforce AD Group for Enrollment in Device Settings (Usage Settings).
- An administrator with limited access can still create a user and a group.

A super administrator uses permission sets to restrict access of an administrator. Typically these restrictions apply to support administrators.

> ***Note:*** If a role-based administrator wants access to manage an entire domain, the super-administrator needs to choose the domain and all users in a domain.

A limited access definition applies to the following pages:

- **Groups**: In the Groups List page, the administator can only see the groups to which access is granted. The administrator cannot modify the Group details for groups that are not granted access. By default, a limited administrator cannot add or import Groups. The buttons shall be invisible to them.

- **Users**: In the Users List page, the administrator can only see the users or users from groups to which access is granted. The administrator cannot modify the User details that are not granted. By default, a limited administrator cannot add or import Users. The buttons shall be invisible to them.
- **Device List**: The Device List page displays devices enrolled with users, and allows you to access their details.
- **Device Set**: A limited access administrator can access and modify devices created by other administrators with the same permission set. A limited access administrator cannot access other device sets (default device sets and device sets created by other limited access administrators with a different permission set).

If you do not want an administrator to have access to all users, it is recommended that you restrict access to pages and actions that have implications across all users.

- **Page Level Permissions:**
  - Enterprise Apps
  - VPP Apps
  - Device Set
  - Device Enrollment
  - Permission Set
  - All Settings sections
- **Action Level Permissions:**
  - Review/Approve App
  - Publish App

  - Approve Device Set
  - Publish/Unpublish Device Set

8.5.7.1 Limited Access Changes

Be aware of the following implications when you change a limited access:

- If new domains, users, and groups are added to limited access, current devices are updated with new access defined for all device sets associated with the limited access.
- If domains, users, and groups are removed from limited access:
  - If removed groups in device set do not have a direct reference, current devices automatically update.
  - If there is a direct reference to the removed users or groups in a device set, the device set status is unpublished, and the device set state changes to draft.
  - An email is sent to all administrators of a permission set when a device set is unpublished.
- If a user is assigned a different permission set:
  - Current devices are dependent on the permission set of the user that created it and not the device user. If a user’s permission set changes, the user cannot access the device set.
- If a permission set is deleted:
  - The device set state changes to draft and the status changes to unpublished.
  - An email will be sent to super-admin with details of deleted permission set along with details of affected device sets.
- If a permission set is deactivated, device set will not be affected. The device set retains the definition as if the permission set is still active.

Device Policy changes: An error will result if an administrator tries to modify a device policy without the required permissions.

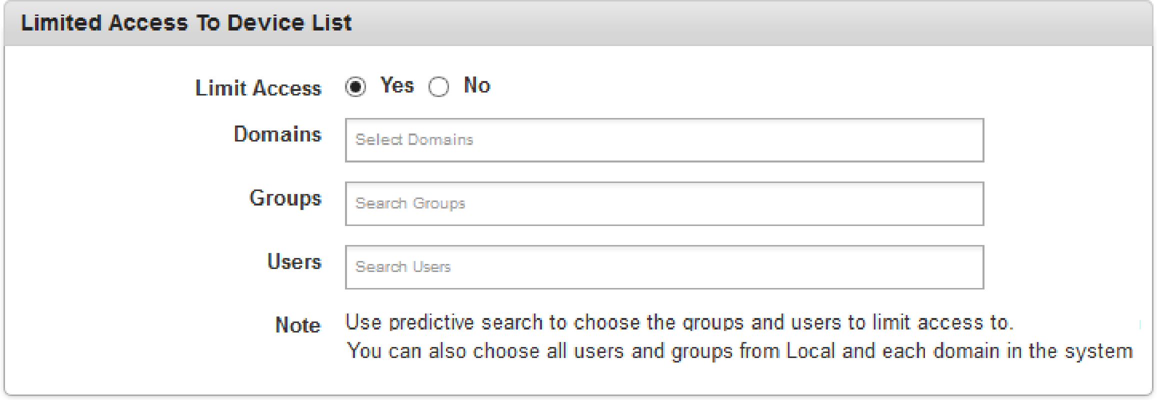
8.5.7.2 Configuring Limited Access to Device List

A user must define the following while configuring limited access to a device list.

- Domain - If an administrator adds a new domain, all users and groups that are part of the domain are under the purview. The users and groups will not show up in the respective lists below.
- Group - If a new domain is not added, then its constituent groups can be selected for groups. When a group is chosen, all users part of that group are also chosen.
- Users - If new users are added, groups they are part of are not automatically added. The groups must be added explicitly.

To configure Limited Access to a device list, follow these steps:

1. By default, the Limit Access option is set to **No**. If you select **Yes** in the Limited Access To Device List, the following details appear:



Limited Access To Device List

Limit Access	● Yes ○ No
Domains	Select Domains
Groups	Search Groups
Users	Search Users
Note	Use predictive search to choose the groups and users to limit access to. You can also choose all users and groups from Local and each domain in the system

   a. **Domains**: Click in the text box, and select the domains from the list.

   b. **Groups**: Click in the text box, and select the groups from the list.

c. **Users**: Click in the text box, and select the users from the list. Limited access to users and groups can also be set at the domain level.

> ***Note:*** Use a predictive search to choose users and groups to which you want to limit access. You can also choose all users and groups from local database and each domain in the system.

2. Configure the remaining settings from here in the Updating Permission Set section.

9. Device Enrollment

To control a device through assigned IT policies, it is essential to enroll it with Mobile Device Management server. Mobile Device Management allows organizations to remotely manage mobile devices, for example, your device can be remotely erased or wiped if it gets lost or stolen.

> *Important:* On your Android devices, ensure that the Developer Options feature is not enabled. If the Developer Options feature is enabled, your device enrollment may fail.

> *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.

> *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.

You have following options for device enrollment:

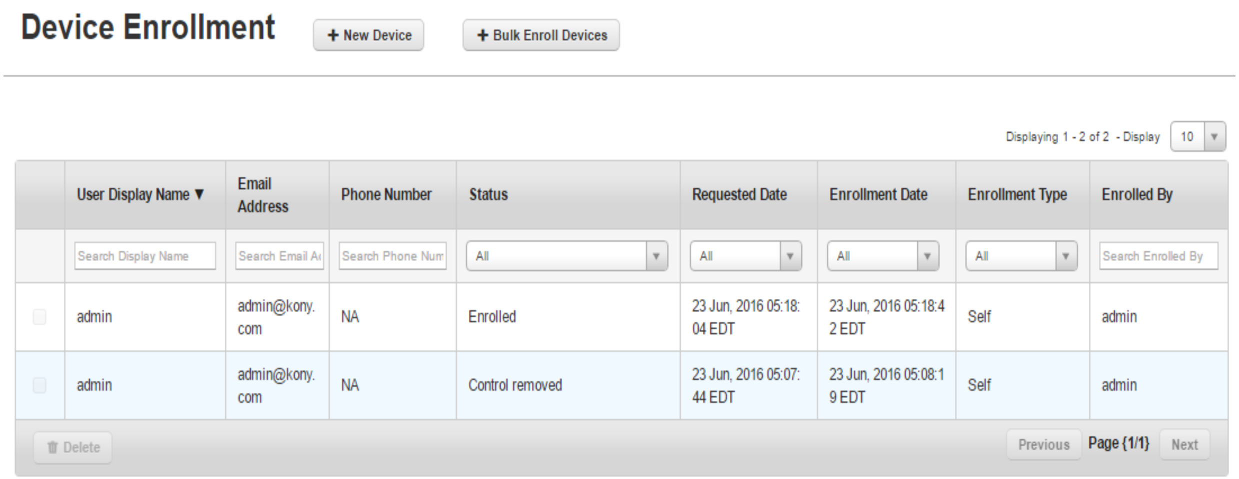
- Admin Initiated Enrollment: (Device enrollment for a single device as well as devices in bulk)
- Device Initiated Enrollment (if the download URL is known)
    - iOS Device initiated Enrollment
    - Android Device Initiated Enrollment
    - Windows Mobile 6.X Initiated Enrollment
    - Windows Phone 8 Initiated Enrollment

- Self Service Enrollment:

  Through the Self-Service console. For more details, refer Self Service Console > Devices

9.1 Admin Initiated Enrollment

From the **Device Management** section, click the **Device Enrollment** from the left panel. The Device Enrollment page appears with a list of actions performed by the user. A user can add new devices from this page. A user can also search for devices based on each column.



	User Display Name ▼	Email Address	Phone Number	Status	Requested Date	Enrollment Date	Enrollment Type	Enrolled By
	Search Display Name	Search Email A	Search Phone Num	All	All	All	All	Search Enrolled By
□	admin	admin@kony.com	NA	Enrolled	23 Jun, 2016 05:18:04 EDT	23 Jun, 2016 05:18:42 EDT	Self	admin
□	admin	admin@kony.com	NA	Control removed	23 Jun, 2016 05:07:44 EDT	23 Jun, 2016 05:08:19 EDT	Self	admin

The Device Enrollment list view displays the following columns:

Columns	Description
Select checkbox	The select checkbox is available for a device for which the enrollment is initiated and the status of the enrollment is **Request Sent**. When you select a device with Request Sent status, the **Delete** button is enabled. This feature provides the administrator an option to remove the enrollment request for a device. For example, if an administrator tries to enroll a device for a user other than the owner of the device, using this feature, the administrator can cancel the request.
User Display Name	Displays the unique identification name of the user and domain. The Device Enrollment can be sorted on the **Display Name** column.
Email Address	Displays the email address of the user.

Columns	Description
Phone Number	Displays the phone number of the user.
Status	Displays the current status of the device.
Requested Date	Displays the requested date for the enrollment of the device.
Enrollment Date	Displays the enrollment date of the device.
Enrollment Type	Displays the type of enrollment for the device.
Enrolled By	Displays the name of the admin who enrolled the device.
Delete	Selected device's enrollment request can be deleted. This button is only active if the check box next to User Display Name is selected.

You can perform the following activities from this page:

- Adding a New Device
- Adding Devices in Bulk
- Device Enrollment - Post Confirmation Details
- Searching for an Enrollment Entry

9.1.1 Adding a New Device

This process falls under Admin Enrollment. These devices are enrolled to EMM Server.

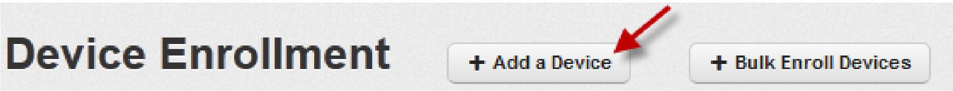
The **Add a Device** window includes three steps to enroll a new device to EMM.

- Step 1: User Information
- Step 2: Asset Information
- Step 3: Confirmation

9.1.1.1 Step 1: User Information

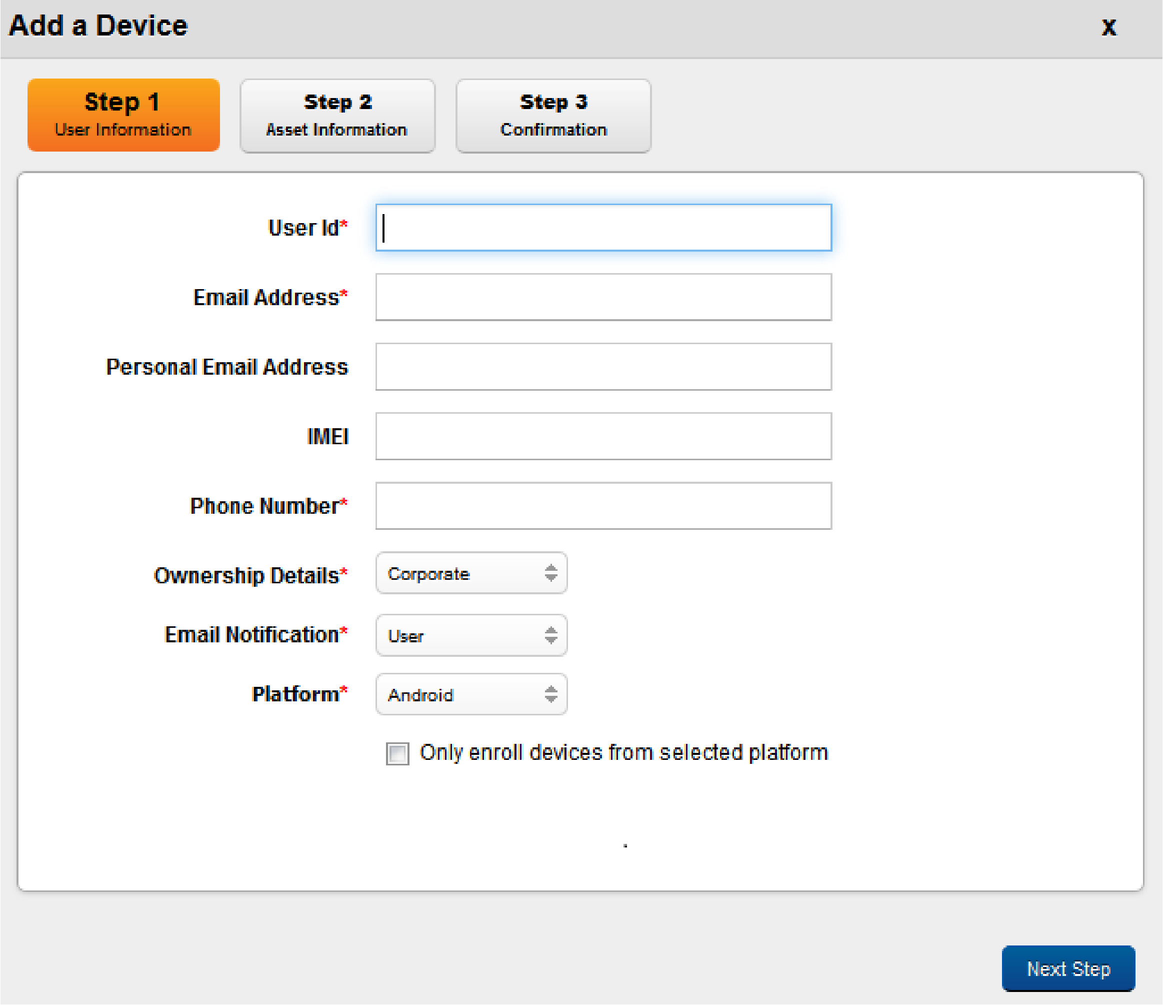
To add a new device, follow these steps:

1. To open the **Add a Device** window, click the **+ Add a Device** button next to the **Device Enrollment** label at the top of the page.

   The **Add a Device** window appears.

2. Enter the following details under Step One:



Add a Device

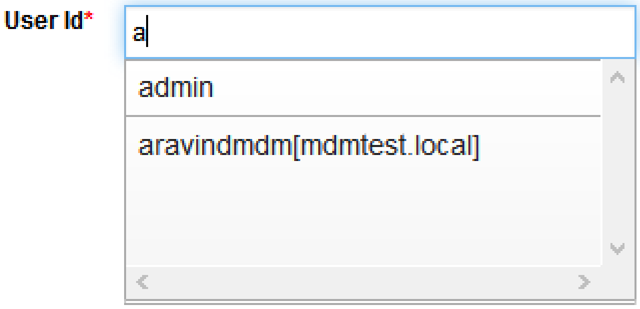
User Id*	
Email Address*	
Personal Email Address	
IMEI	
Phone Number*	
Ownership Details*	Corporate
Email Notification*	User
Platform*	Android

□ Only enroll devices from selected platform

3. **User ID**: Enter the partial name of the user and a pop-up window with a list of user names associated with Domains appears.

   For example: Username[Domain]

   > ***Note:*** Only Users that are enrolled with EMM are shown. This includes Active Directory Users as well as Kony Database Users. Select the name of the User whose device you wish to enroll.



User Id*

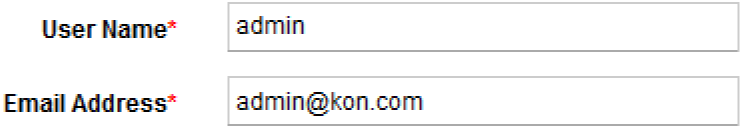
a

admin

aravindmdm[mdmtest.local]

4. **Email Address**: As per selected User name, the corresponding email address is populated in the **Email address** field.

   The enrollment request and registration instructions are sent to the user on this email address. This Email address is auto-populated from User details (as recorded while the User was enrolled).



User Name* admin

Email Address* admin@kon.com

5. **Personal Email Address:** The Admin must provide the personal email id of the employee - should they have it.

   Personal email id of the user is required for additional contact details.

6. **IMEI**: Enter the Mobile Equipment Identity Number.

> ***Note:*** If you enter IMEI in incorrect format, the following warning messages appears:
>
> - Please enter at least 15 characters.
> - Please enter only digits.

7. **Phone Number**: Enter the Phone Number.

   This is the phone number of the Device User as provided in User details; This is expected to be the phone number of the device. If you enter phone number in incorrect format, system displays warning message to enter at least 11 characters.

8. **Ownership Details**: Choose the type of Ownership of the device. There are three types: **Corporate**, **Employee** and **Shared**.

   This pertains to ownership of the device. The device can be owned by an employee, or Corporate, or shared. Shared refers to devices that are owned by the corporate but shared between multiple employees. An example is a device used by the testing team - different people use each device to test different aspects.

9. **Email Notification**: Choose the type of email notification. There are two types, **User** and **Admin and User.** The enrollment notification is sent to the specified personnel.

   Email notifications are sent to individual User regarding enrollment of the device and what further actions are required to accomplish the task.

10. **Platform**: Choose the appropriate Operating System that the device supports,

    If you wish to enroll devices from the selected platform only, then select the check box **Only enroll devices from selected platform**.

    The platform on which the device resides. The supported Device OS are: iOS, Android, Windows 6.x, and Windows Phone 8, Windows Phone 8.1, Windows 8 Pro (Windows Tablet), and Windows 8 RT (desktop).

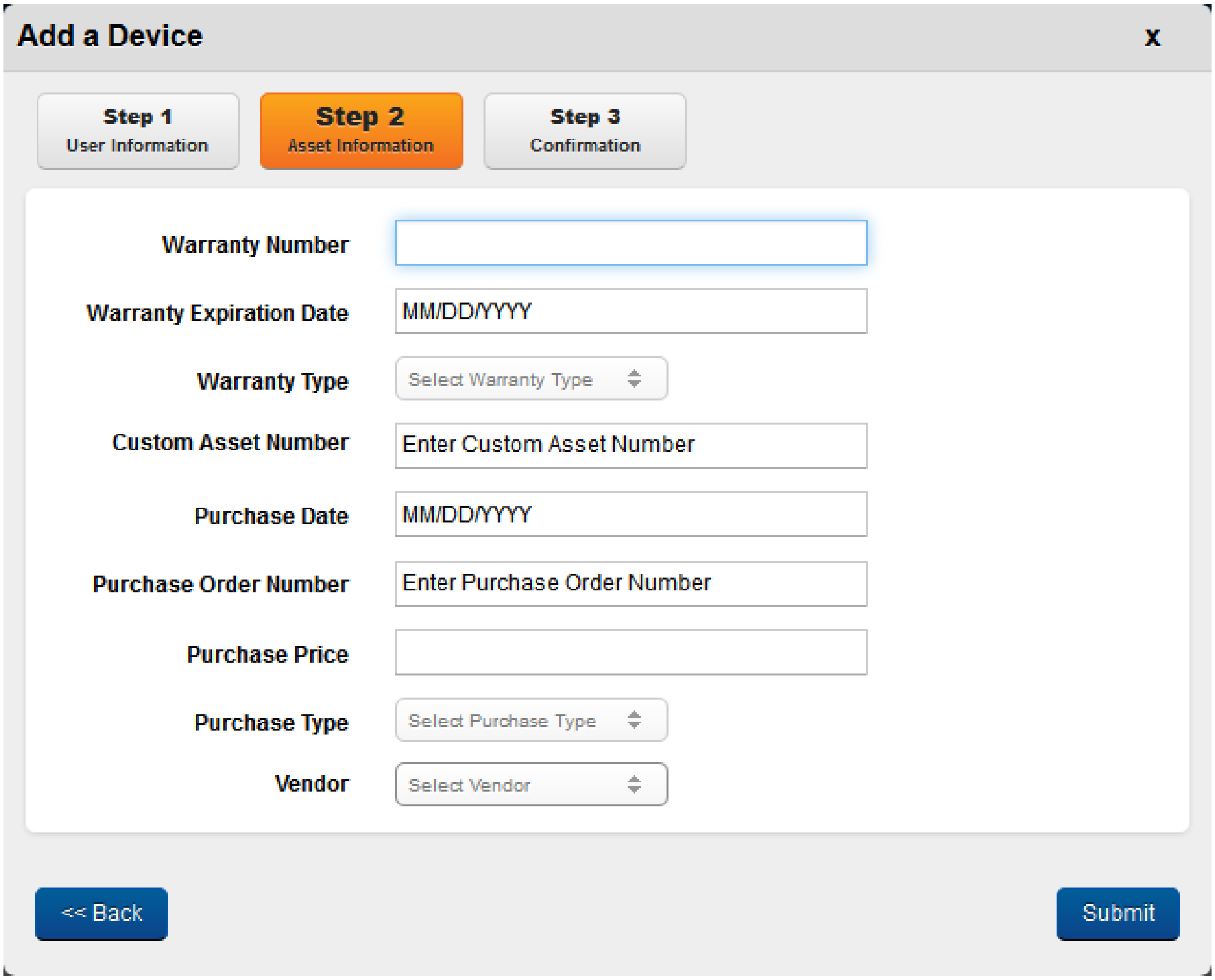
11. Click the **Next Step** button to open **Step 2** window.

> ***Important:*** If you provide IMEI number while adding a single device or adding devices in bulk, then the platform is immaterial.
>
> For example, if you provide IMEI number of an iOS device but select Device OS as Android and select Only Enroll devices from selected platform option. In this scenario, the OS details are discounted and you can proceed to add your device to EMM.

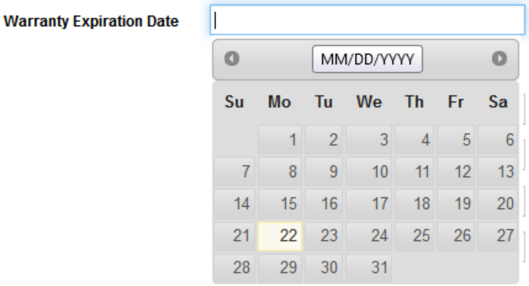
9.1.1.2 Step 2: Asset Information

Asset information is not the basic information of the device. It is required if the device needs repair and so on. This step is useful, if there is an asset tracking mechanism in the organization. None of the details in this step are mandatory.

Enter the following details in Step Two:



1. **Warranty Number**: Enter the valid warranty number. This is the unique identification number to identify the warranty type.



Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

2. **Warranty Expiration Date**: Enter the cursor in the **Warranty Expiration Date** field. A Calendar window with current month and current date as active, appears. Select the required date. The date is populated in the text field.

   After this date, the warranty expires.

3. **Warranty Type**: Select the appropriate warranty from the **Select Warranty Type** drop-down list.

   There are three warranty types respectively, Manufacturer warranty, Seller Warranty and the Extended Warranty.

4. **Custom Asset Number**: Enter the valid custom asset number in the **Enter Custom Asset Number** text field. This number is given by company to define asset information.

5. **Purchase Date**: Enter the cursor in the **Purchase Date** field. A Calendar window with current month and current date as active, appears. Select the required date. The date is populated in the text field.

   Purchase date cannot be in a future date.

6. **Purchase Order No**: Enter the purchase order number of the device in **Enter Purchase Order Number** text field.

7. **Purchase Price**: Enter a purchase order number is an alpha/numeric code that is assigned to a particular request to buy something. PO numbers are used internally to track purchases. valid purchase price for the device. If you enter wrong purchase price, a warning message to enter valid purchase price appears.

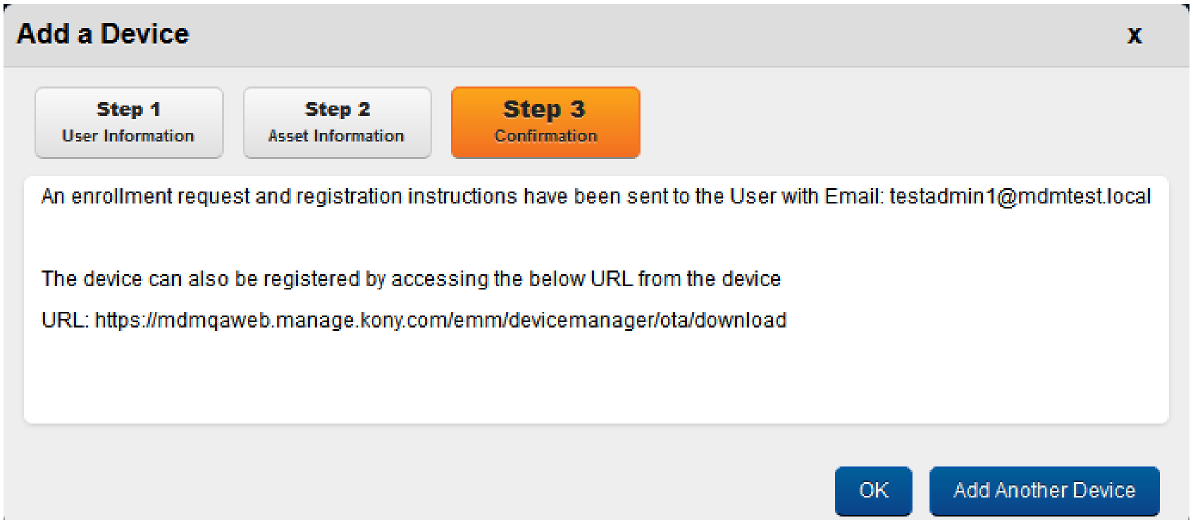
8. **Purchase Type**: Select Purchase Type as **Single Purchase** or **Volume Purchase** from the **Select Purchase Type** drop-down list.

9. Click the **Submit** button to open **Step 3** window.

   Click the **Back** button to navigate to **Step 1**.

9.1.1.3 Step 3: Confirmation

Step Three window displays confirmation message stating that the enrollment request and registration instructions are sent at the specified email address of the administrator.



An enrollment request and registration instructions have been sent to the User with Email: testadmin1@mdmtest.local

The device can also be registered by accessing the below URL from the device

URL: https://mdmqaweb.manage.kony.com/emm/devicemanager/ota/download

1. Click the **OK** button to proceed.

2. Click the **Add Another Device** button to open **Step 1** window to enroll a new device with EMM.

For a device where enrollment is initiated, if the associated user is deleted, the device enrollment status will change from **Request Sent** to **Request Deleted**.

9.1.2 Device Enrollment- Post Confirmation Details (Admin)

The next steps after receiving an email with a URL and details of how to enroll with EMM Server are as follows

- Enterprise Store Download
- Authentication
- Terms Acceptance
- Profile Download

9.1.2.1 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.

9.1.2.2 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 enrolled, not associated with any other user. Once this is established, the server signals the agent to proceed with the enrollment.

4. If Verification fails, device user receives a message. Device goes into the status based on type of verification failure.

9.1.2.3 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 enrollment 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.

9.1.2.4 Profile Download

1. Once the terms and conditions are accepted, Device Users are informed to download the application and install it.
2. Selecting to proceed automatically triggers the download and installation of the EMM Profile.
3. Device Users are requested to confirm any prompts by the application.
4. After completing the installation, Device Users receive a confirmation about installation of the profile and a success message about device enrollment.
5. If profile installation fails, Device Users are informed and requested to try the Download and installation again.

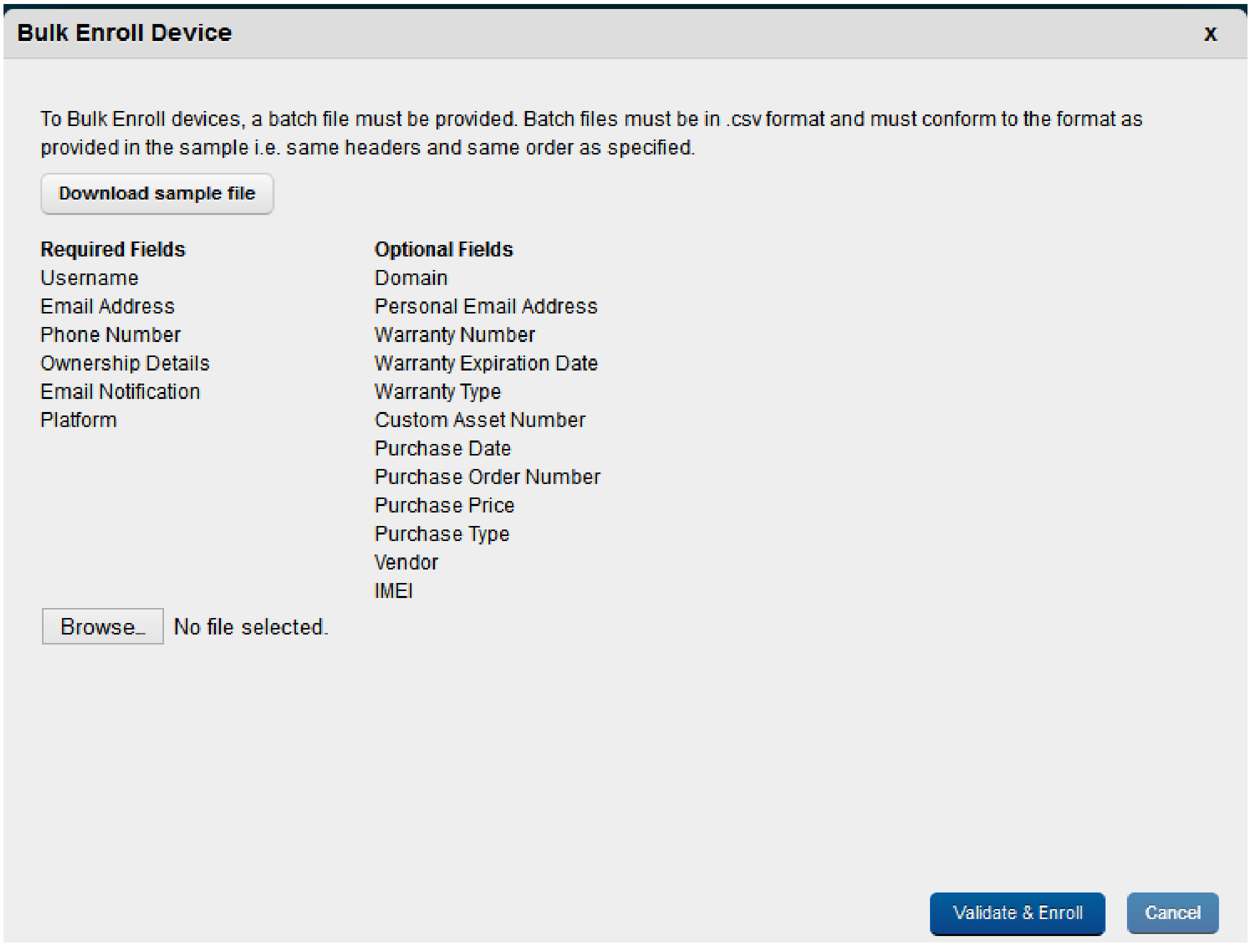
9.1.3 Adding Devices in Bulk

This process falls under Admin Enrollment. This option enables you to enroll several devices at the same time. You need to create a .csv file with the User Name, Email Address, Phone Number, Email Notification, Platform and Ownership details and upload the same. You can also provide optional details. Multiple entries should be in separate lines.

The EMM system validates details in the .csv file to ensure that the specified User is a part of the Domain else displays one of the following error messages:

> ***Note:*** Error messages are displayed against each enrollment entry at the last column in the .CSV based on the following situations:

- **Unable to reach Directory** (if unable to reach the Directory Server)
- **Domain Deleted** (if the Domain was recently deleted)
- **User not part of specified Domain** (If no entry of the User is available within the specified Domain)



Bulk Enroll Device

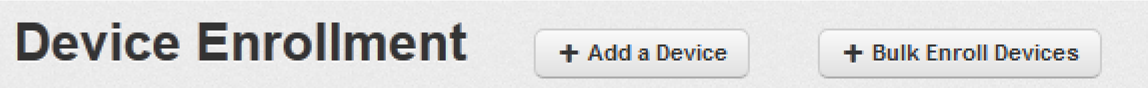
To Bulk Enroll devices, a batch file must be provided. Batch files must be in .csv format and must conform to the format as provided in the sample i.e. same headers and same order as specified.

Required Fields	**Optional Fields**
Username	Domain
Email Address	Personal Email Address
Phone Number	Warranty Number
Ownership Details	Warranty Expiration Date
Email Notification	Warranty Type
Platform	Custom Asset Number
	Purchase Date
	Purchase Order Number
	Purchase Price
	Purchase Type
	Vendor
	IMEI

No file selected.

To enroll devices through Bulk Enrollment, follow these steps:

1. To open the **Bulk Enroll Device** window, click the **+Bulk Enroll Devices** button next to the Device Enrollment label at the top of the page.



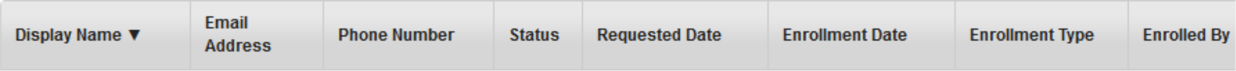
2. Click the **Browse** button to find the .csv file in your system to add. Select it, and click **Open**. The attached file appears next to the **Browse** button.

3. Click the **Validate and Enroll** button to import the same. The system displays the confirmation message. An Enrollment mail is sent to all the users listed in the csv file. The first line of the .csv is the column header and the columns can be in any order.

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

9.1.4 Searching for an Enrollment Entry

You can search for devices 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:



1. Enter or select details for following search filters:
   - **Display Name**: Enter partial or complete name of the user in the **Search user** field.
   - **Email Address**: Enter required email address in the **Search Email** field.
   - **Phone Number**: Enter required phone number of the user in the **Phone Number** field.
   - **Status**: Select the required **Status** from the drop-down list.
   - **Requested Date**: Select the required requested date from the drop-down list.

- **Enrollment Date**: Select the required enrollment date from the drop-down list.
- **Enrollment Type**: Select the required type of enrollment from the drop-down list.
- **Enrolled By**: Enter partial or complete name of the Admin in the Search field.

2. According to your search filters 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** drop-down list. You can also scroll the list view through **Previous** and the **Next** button.

9.2 Device Initiated Enrollment

This section describes the enrollment process through enterprise store. :

The generic process involves the following steps:

1. Enterprise storeDownload
2. Enrollment Request
3. Server Side Authentication and Verification
4. Terms and Conditions Acceptance
5. Profile Download / Policy Application

Device User initiates and completes the enrollment 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 enrollment for the following platforms:

- iOS Device initiated Enrollment
- Android Device initiated Enrollment
- Windows Device 6.x Initiated Enrollment Registration

9.2.1 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.

9.2.2 iOS Device initiated Enrollment

The entire process is driven on the device and the user need not leave the Enterprise Store. If enrollment is successful, the device should be enrolled and its status should change to Enrolled .

The generic process to enroll a device is as follows:

> *Note:* In EMM 2.5 onwards, while enrolling 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.

9.2.2.1 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.

9.2.2.2 Server Side Authentication and Verification

1. The details provided by the User are authenticated.

2. The EMM Server ensures that the device is not enrolled, not associated with any other user and allowed to enroll. Once this is ascertained, the server signals the agent to proceed with the enrollment.

9.2.2.3 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 enrollment process is aborted and the Device goes into the **Terms Not Accepted** state.

9.2.2.4 Download and Install Profile

User should download the EMM Profile and install the same to complete the process. You need to enable Cookies while downloading Kony EMM enterprise store.

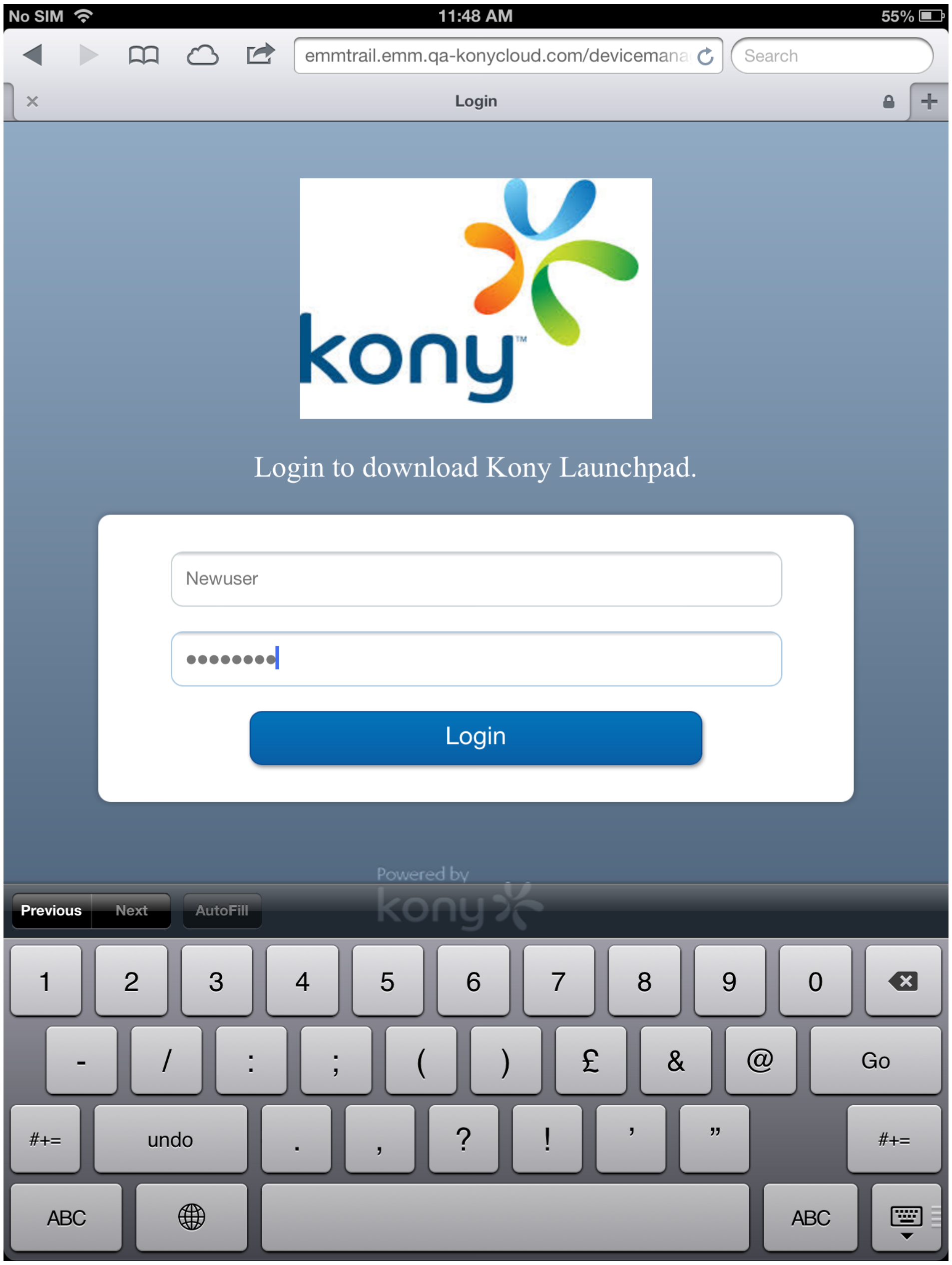
1. The User is requested to affirm any prompts by the application.

2. Once, the installation is complete, System displays the confirmation message that device is successfully enrolled with Kony EMM. This marks the completion of enrollment of the device.

> ***Important:*** If MDM profile is already installed, but device enrollment does not happen, then delete the MDM profile and try to enroll the device again. If you experience difficulties in removing MDM profiles, then restart the device, go to Airplane mode, and then remove the profile.

To perform iOS Device initiated Enrollment, follow these steps:

1. Enter application URL in the device based browser.



Login to download Kony Launchpad.

Newuser

••••••••

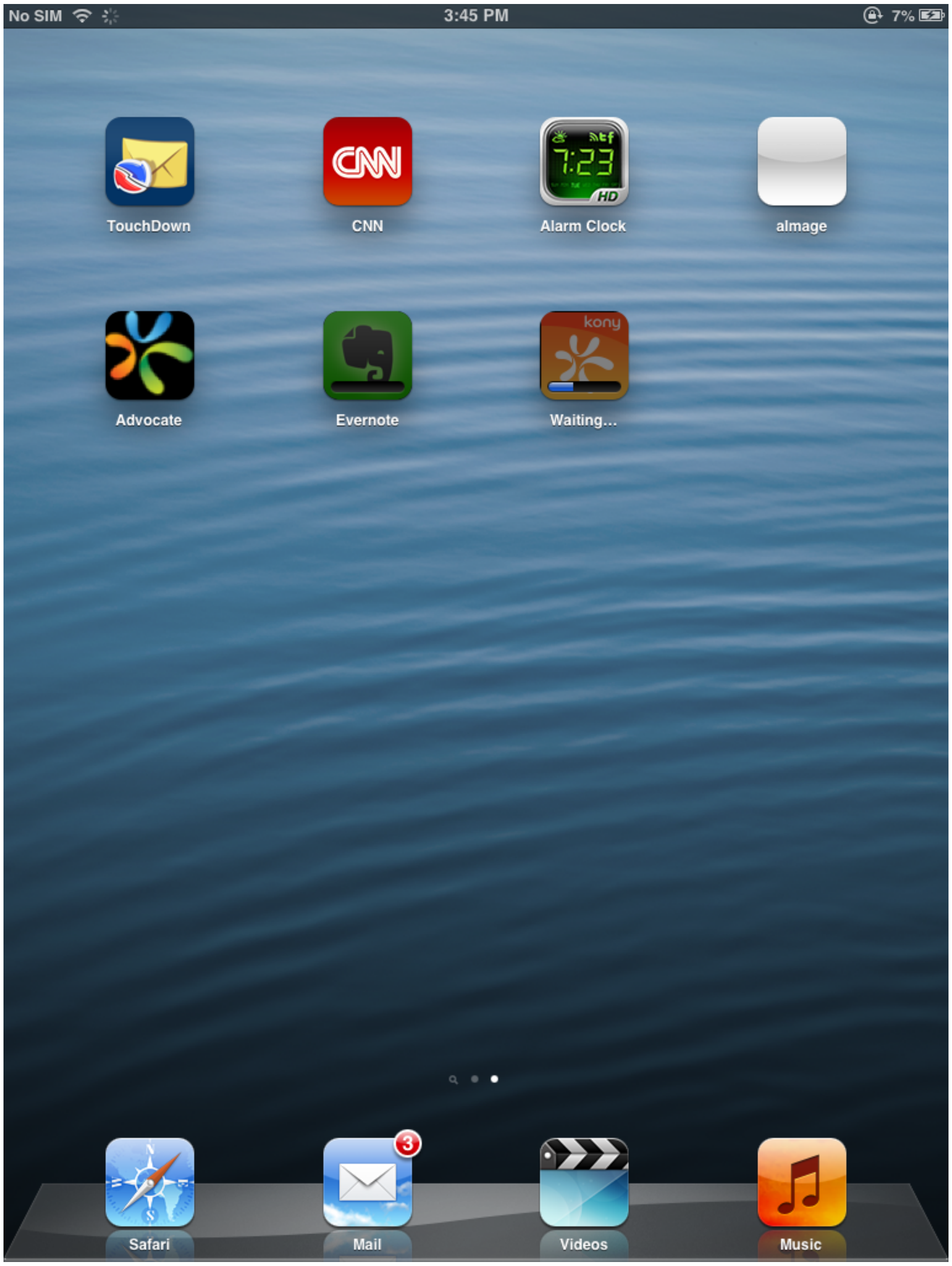
The Log-in page appears.

If JavaScript is turned off, the app logo image is not visible in the container download page in Safari browser.

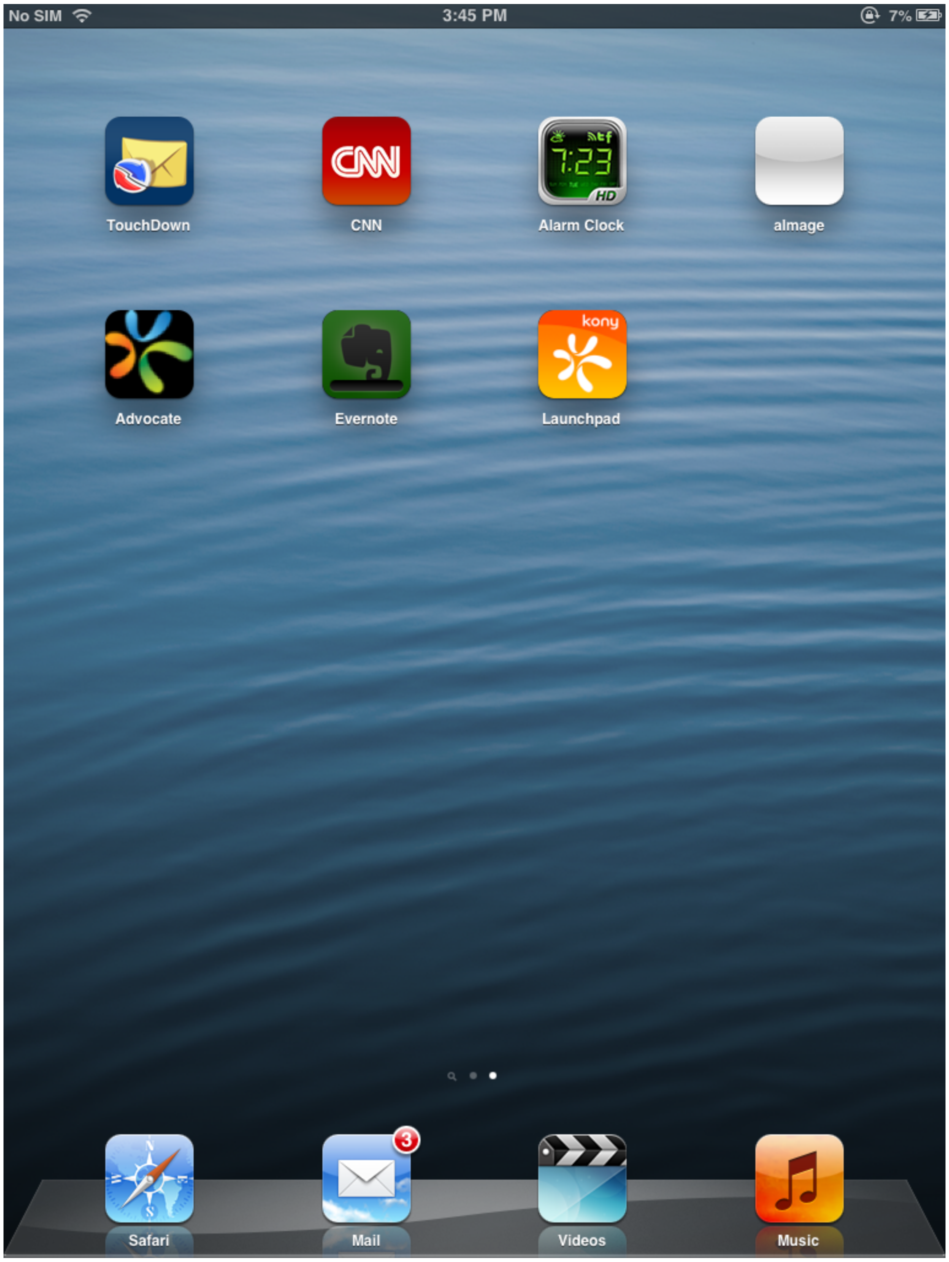
2. Enter your log-in credentials. These details are sent to the Server along with the device information.

> *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.

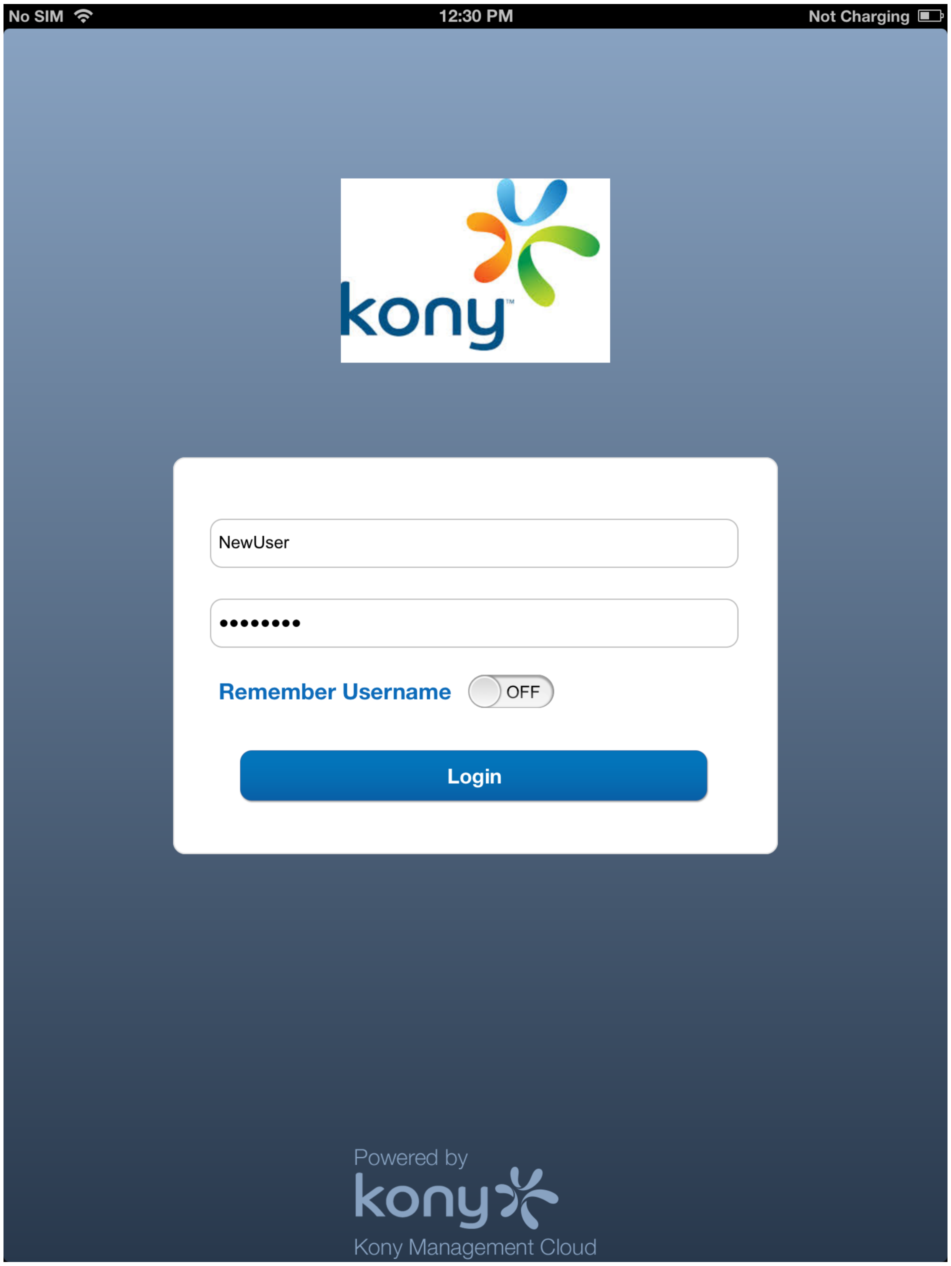


The above image indicates that installation process is in progress.



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 the click on **Trust {Profile Name}.**

5. 

NewUser

••••••••

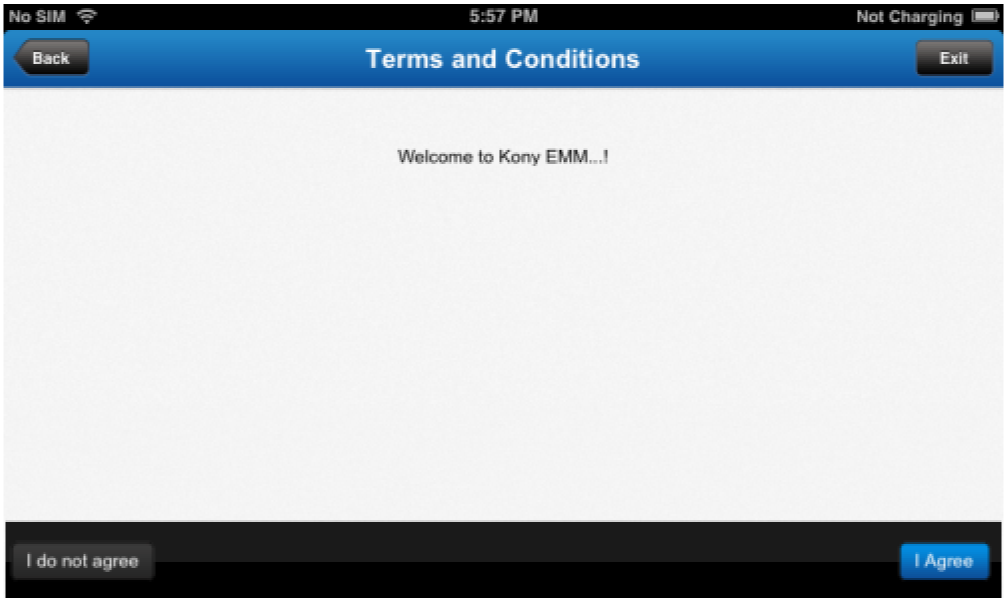
Remember Username OFF

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 enrolled,not associated with any other user and allowed to enroll. Once this is ascertained, the server signals the agent to proceed with enrollment. If Verification fails, The Device goes into the status based on type of verification failure.

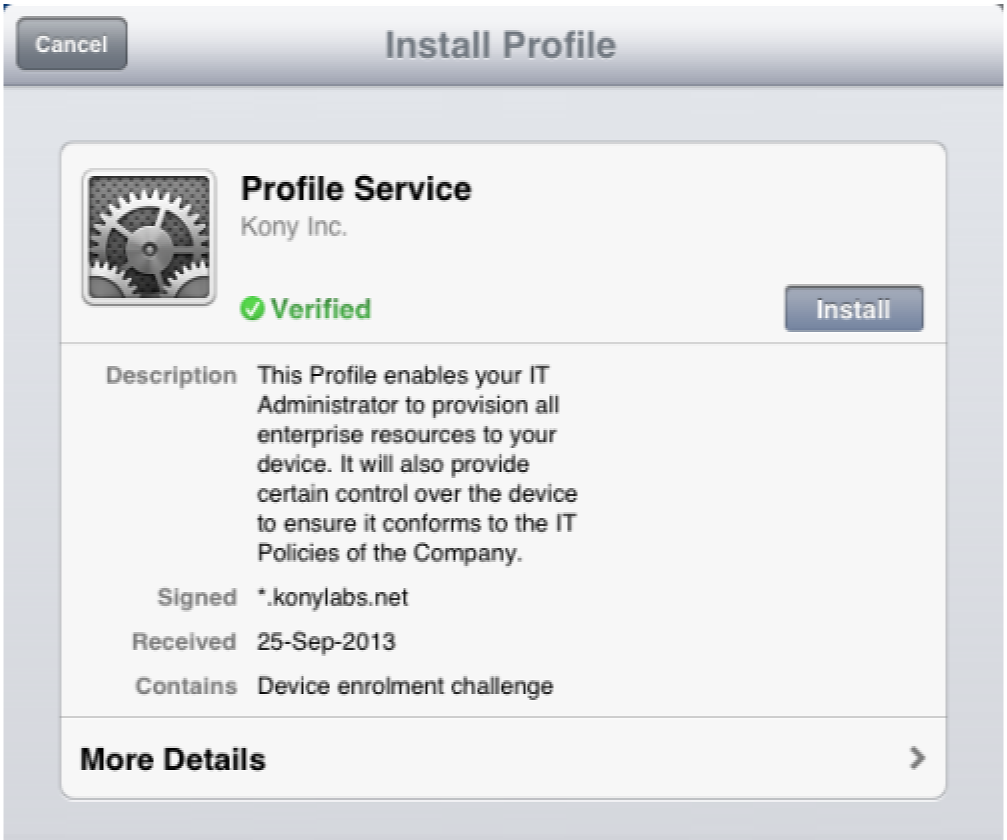
7. The system verifies the credentials. Once the authentication and verification is successful, system displays the Terms and Conditions.



Welcome to Kony EMM...!

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 enrollment process is aborted and the device goes into terms not accepted state.

> *Note:* If a user tries to re-enroll a completely wiped device listed under Enrollment Denied List, the device displays the Terms and Conditions page, in a loop every time a user tries to log in. In Enterprise wiped device it works as expected.



Profile Service

Kony Inc.

✓ Verified

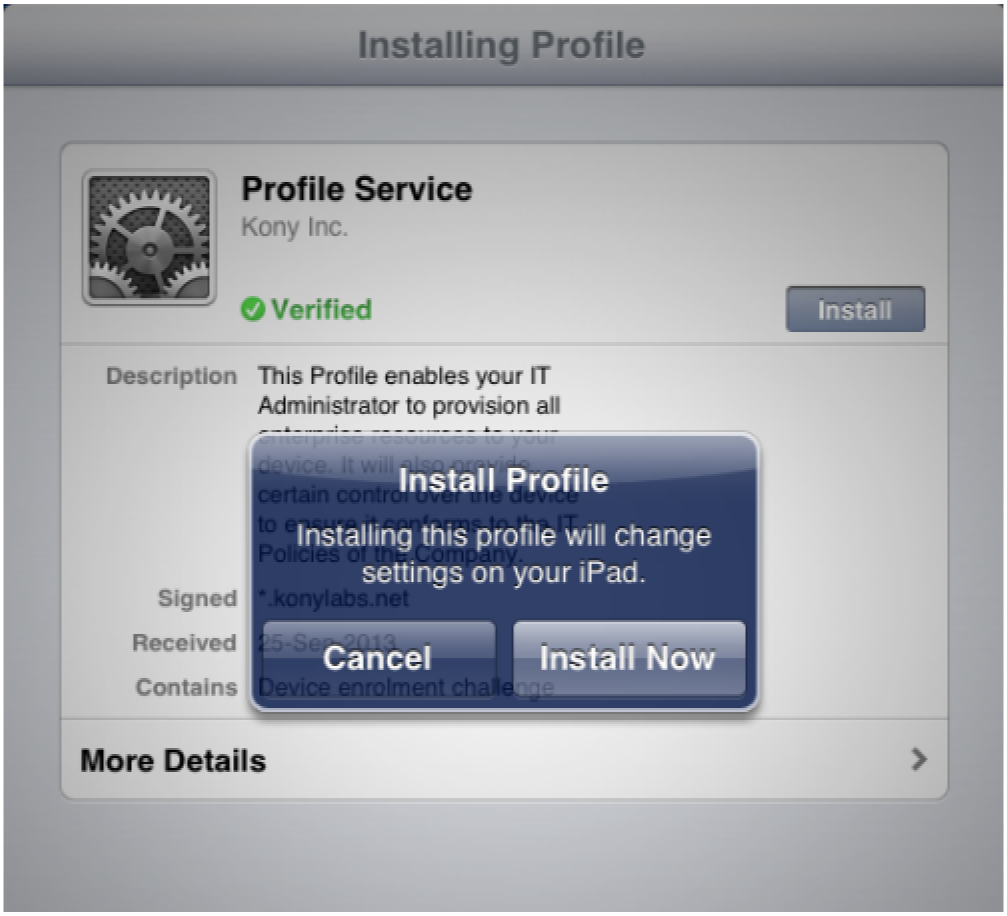
Description This Profile enables your IT Administrator to provision all enterprise resources to your device. It will also provide certain control over the device to ensure it conforms to the IT Policies of the Company.

Signed *.konylabs.net

Received 25-Sep-2013

Contains Device enrolment challenge

9. Click the **Install** button to install **Profile** on your device.



Installing Profile

Profile Service
Kony Inc.

✓ Verified

Description This Profile enables your IT Administrator to provision all enterprise resources to your device. It will also provide certain control over the device to ensure it conforms to the IT Policies of the Company.

Signed *.konylabs.net

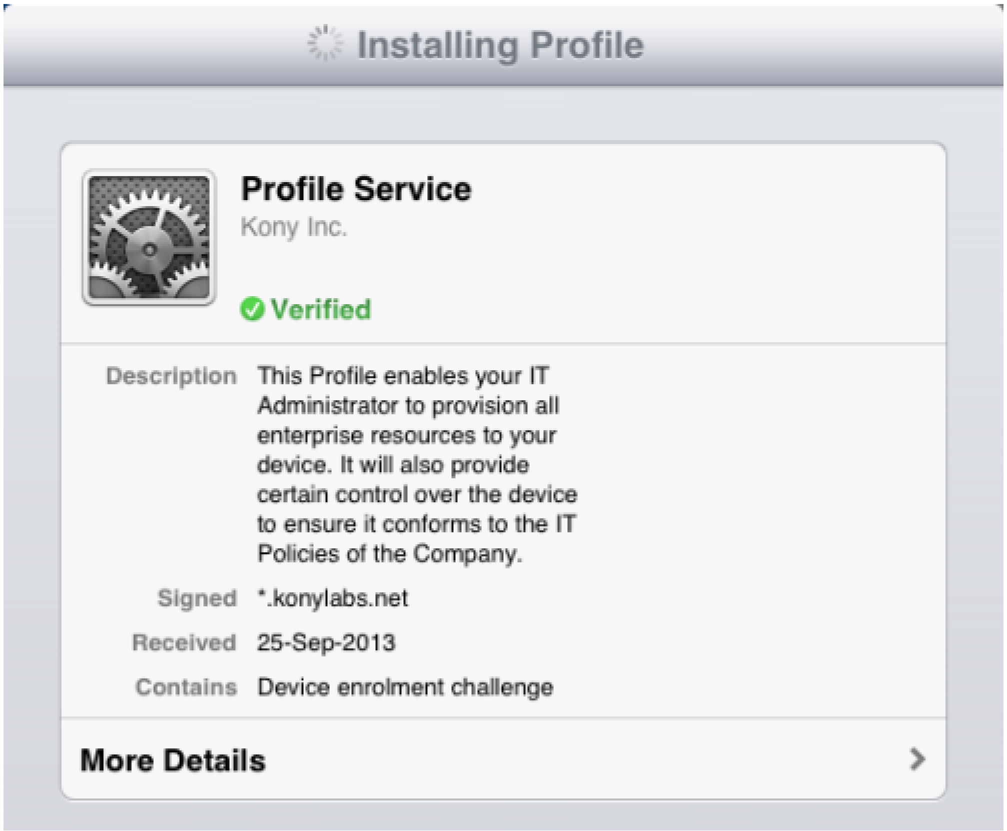
Received 25-Sep-2013

Contains Device enrolment challenge

Install Profile

Installing this profile will change settings on your iPad.

10. The System displays the Warning message. Click the **Install Now** button to proceed.



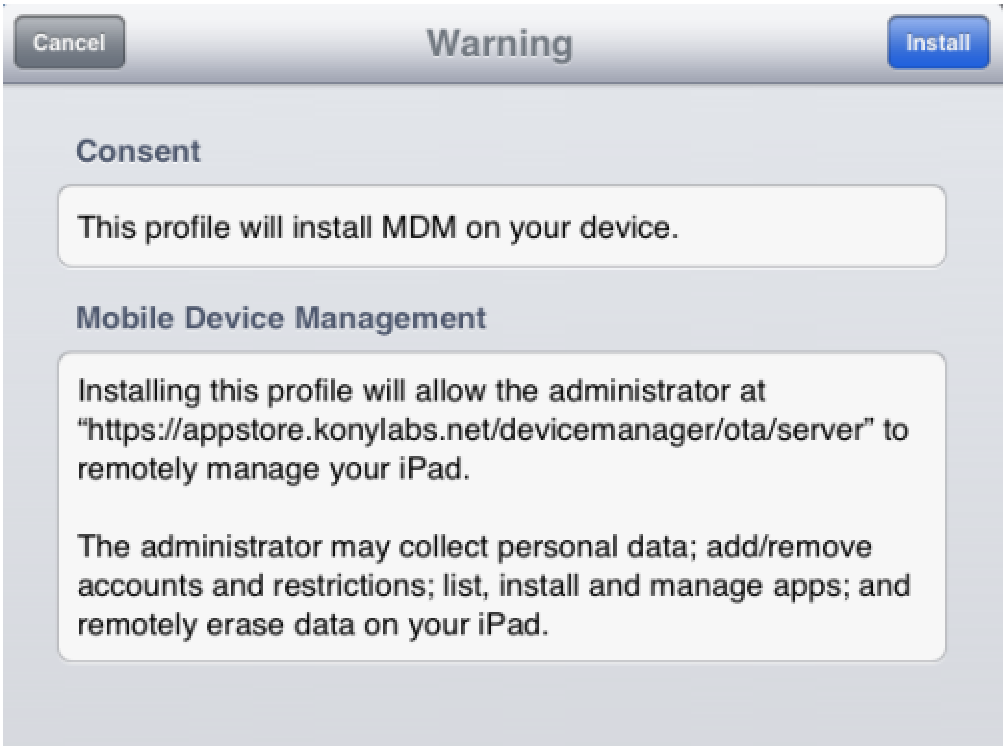
Installing Profile

Profile Service
Kony Inc.

✓ Verified

Description	This Profile enables your IT Administrator to provision all enterprise resources to your device. It will also provide certain control over the device to ensure it conforms to the IT Policies of the Company.
Signed	*.konylabs.net
Received	25-Sep-2013
Contains	Device enrolment challenge

The Profile is verified.



Consent

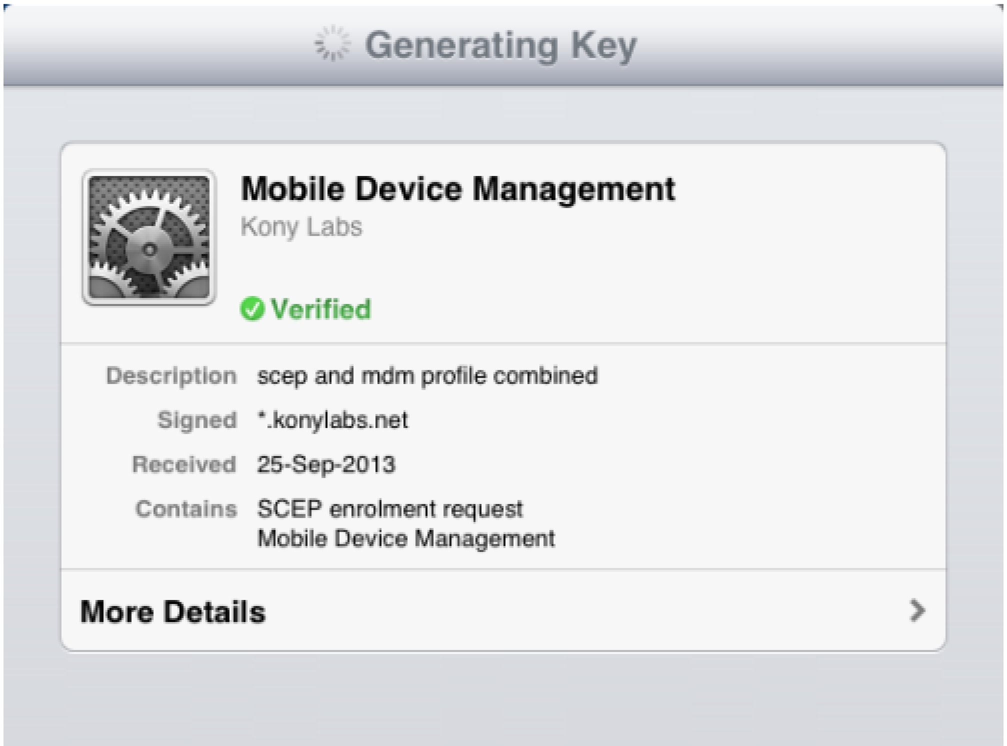
This profile will install MDM on your device.

Mobile Device Management

Installing this profile will allow the administrator at “https://appstore.konylabs.net/devicemanager/ota/server” to remotely manage your iPad.

The administrator may collect personal data; add/remove accounts and restrictions; list, install and manage apps; and remotely erase data on your iPad.

11. Read the Warning message carefully. Click the **Install** button to install Profile on your device.



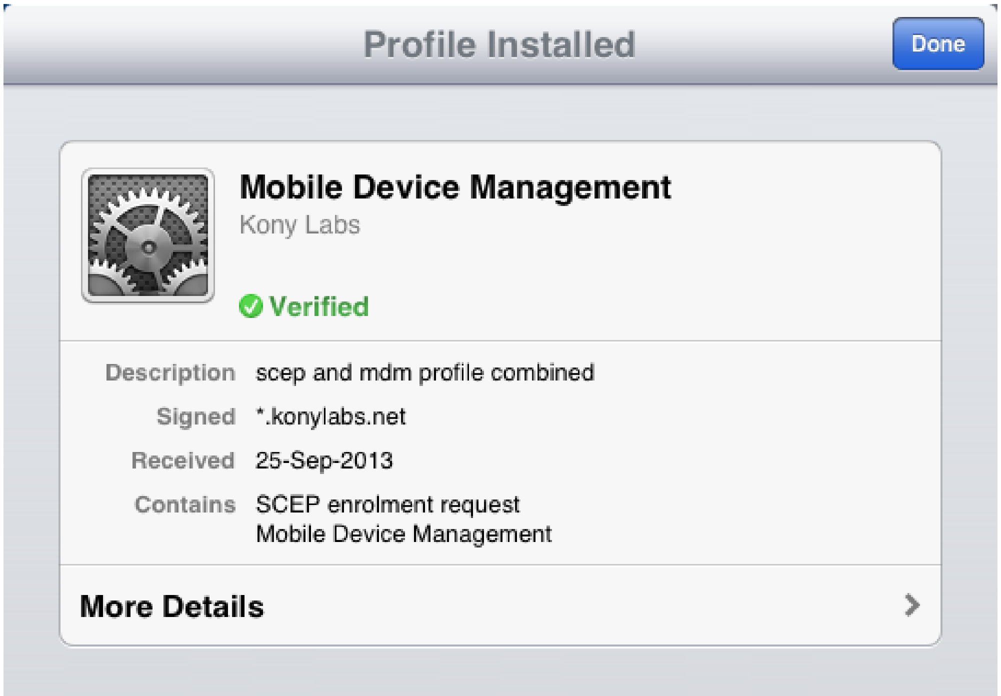
Generating Key

Mobile Device Management
Kony Labs
✓ Verified

Description	scep and mdm profile combined
Signed	*.konylabs.net
Received	25-Sep-2013
Contains	SCEP enrolment request Mobile Device Management

More Details

The system generates the key.



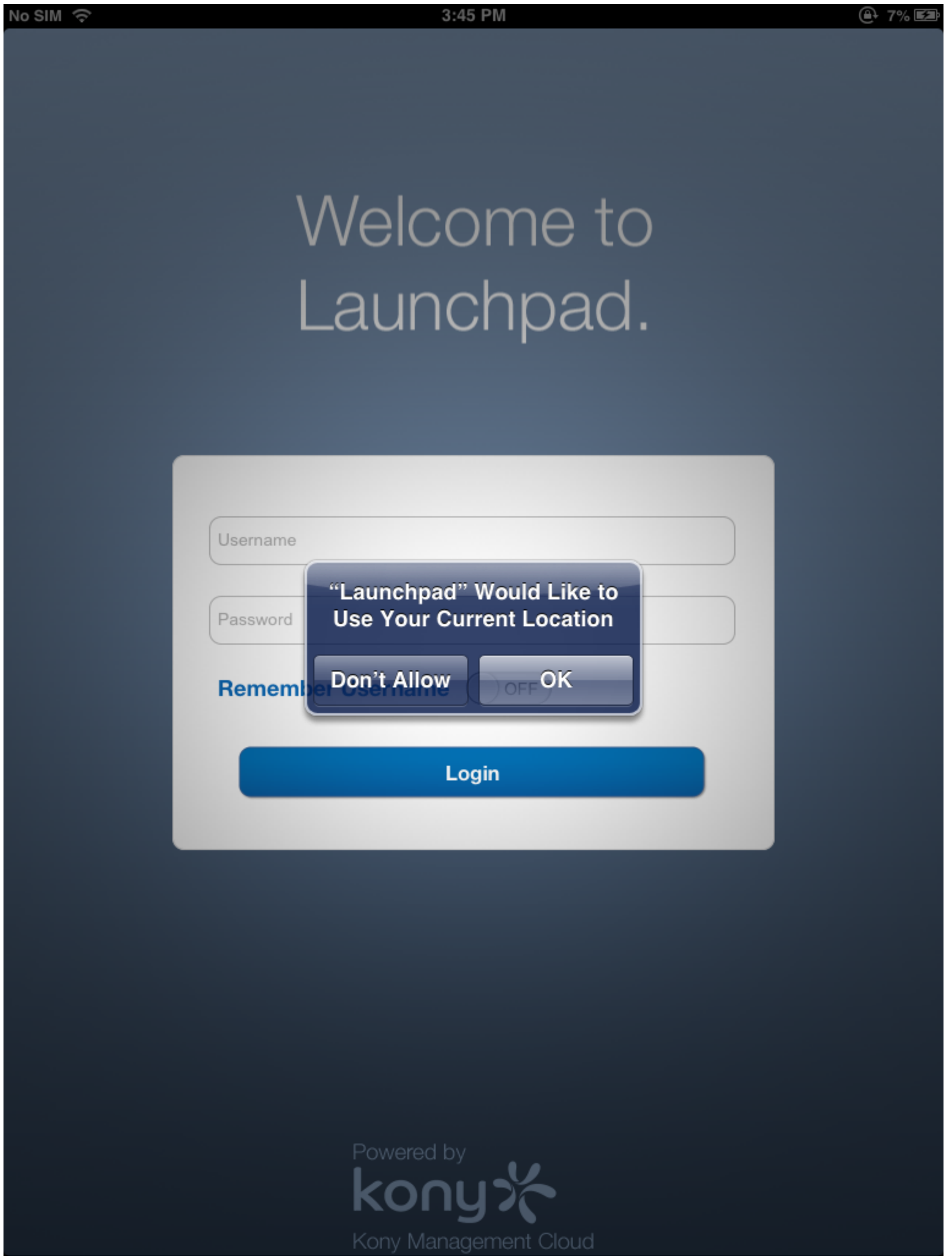
Profile Installed

Mobile Device Management
Kony Labs
✓ Verified

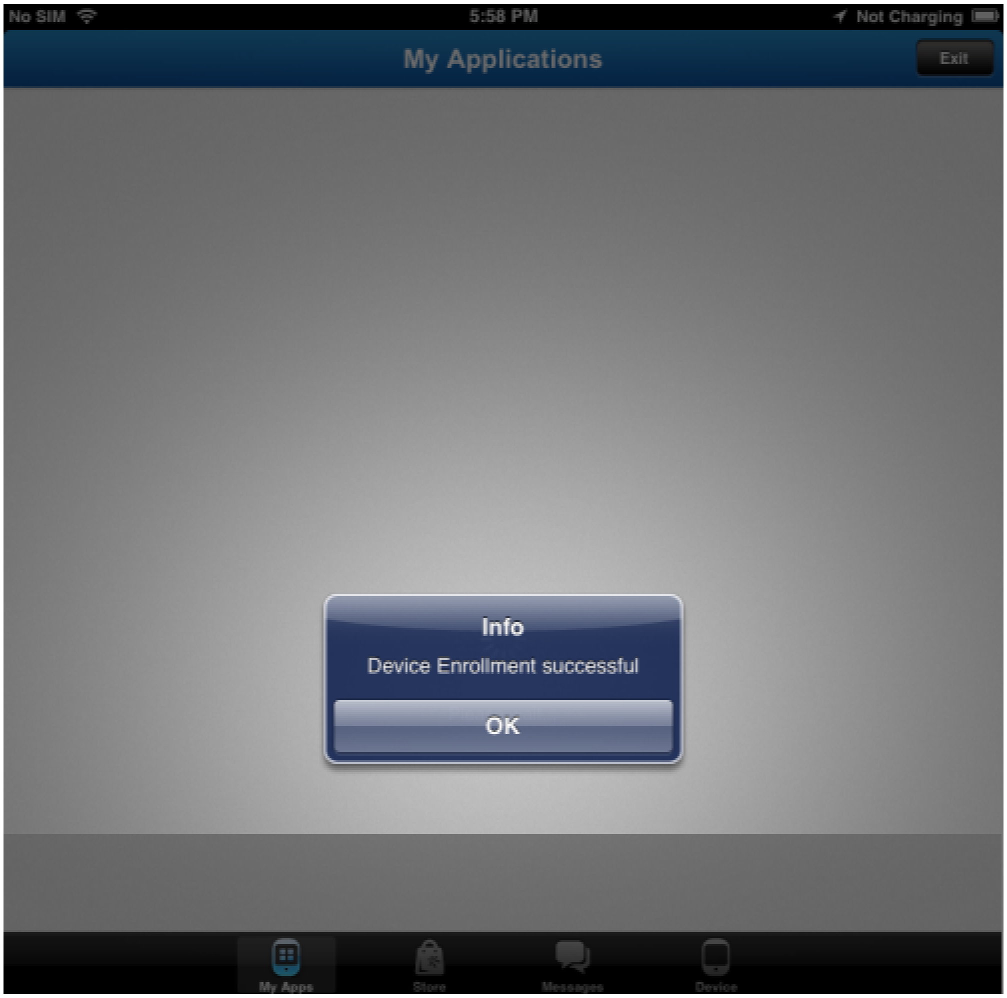
Description	scep and mdm profile combined
Signed	*.konylabs.net
Received	25-Sep-2013
Contains	SCEP enrolment request Mobile Device Management

More Details

12. The profile is installed on your device. Click the **Done** button.



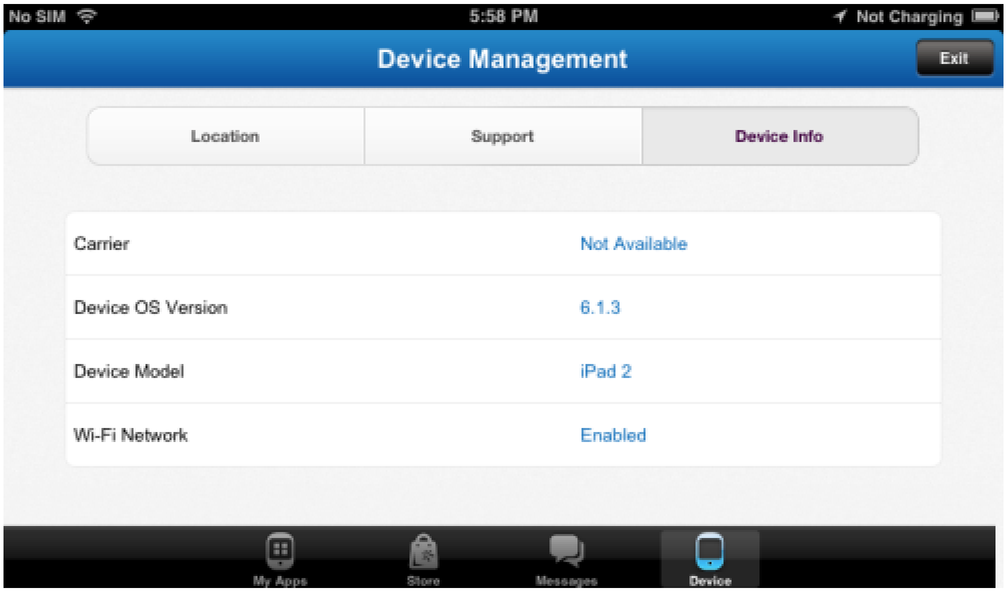
13. The system displays the confirmation message. Click **OK** to proceed.



Info

Device Enrollment successful

14. The system displays the confirmation message. Click **OK** to proceed.



Carrier	Not Available
Device OS Version	6.1.3
Device Model	iPad 2
Wi-Fi Network	Enabled

15. The system displays the Device particulars such as Device OS Version, Carrier and so on. Click the **Exit** button to close the window.

9.2.3 Android Device Initiated Enrollment

The entire enrollment is driven on the device, so a user need not leave the enterprise store. If the process is successful, the device is added, and its status changes to enrolled . 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:

9.2.3.1 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.

9.2.3.2 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 enrollment.

9.2.3.3 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 enrollment process is aborted, and the device goes into the **Terms Not Accepted** state.

9.2.3.4 Activating the Enterprise Store

1. The user must authorize the application to have adminstrator privileges over the device. The device throws a message with the details of control.

2. The user can either choose Accept to activate the device or Cancel.

3. If the user chooses accept, the system displays a confirmation message that the device is successfully enrolled with Kony EMM.

To perform Android Device-Initiated Enrollment,follow these steps:

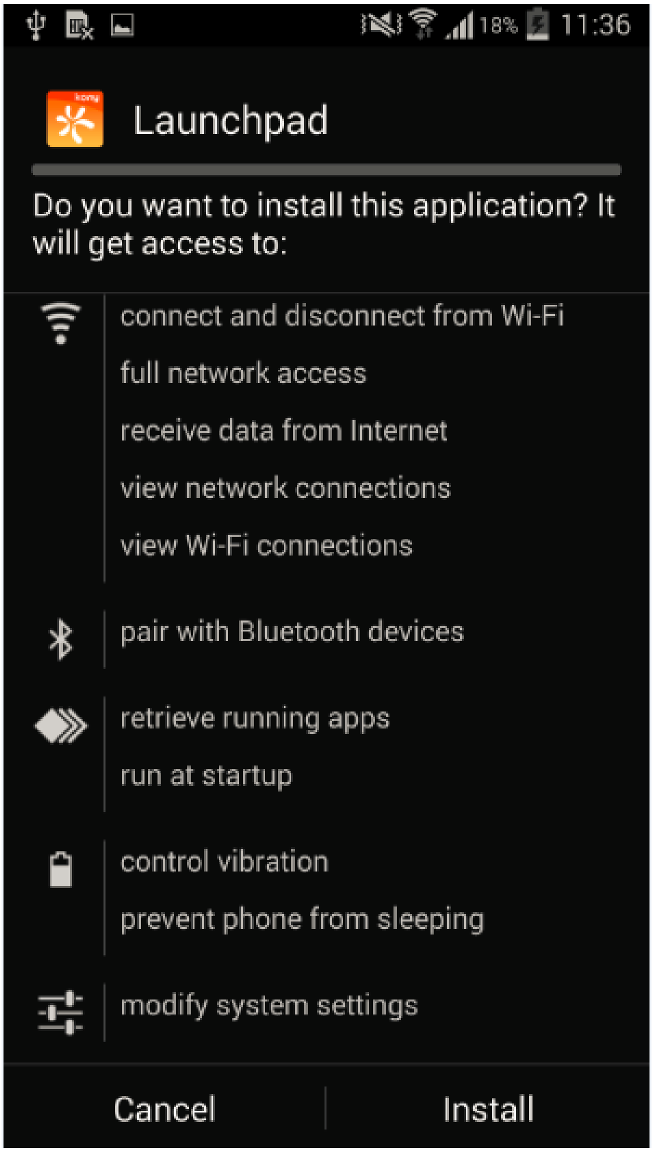
Prerequisite: A device user uses the device that should be enrolled. The device is an Android device.

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.



Launchpad

Do you want to install this application? It will get access to:

connect and disconnect from Wi-Fi
full network access
receive data from Internet
view network connections
view Wi-Fi connections

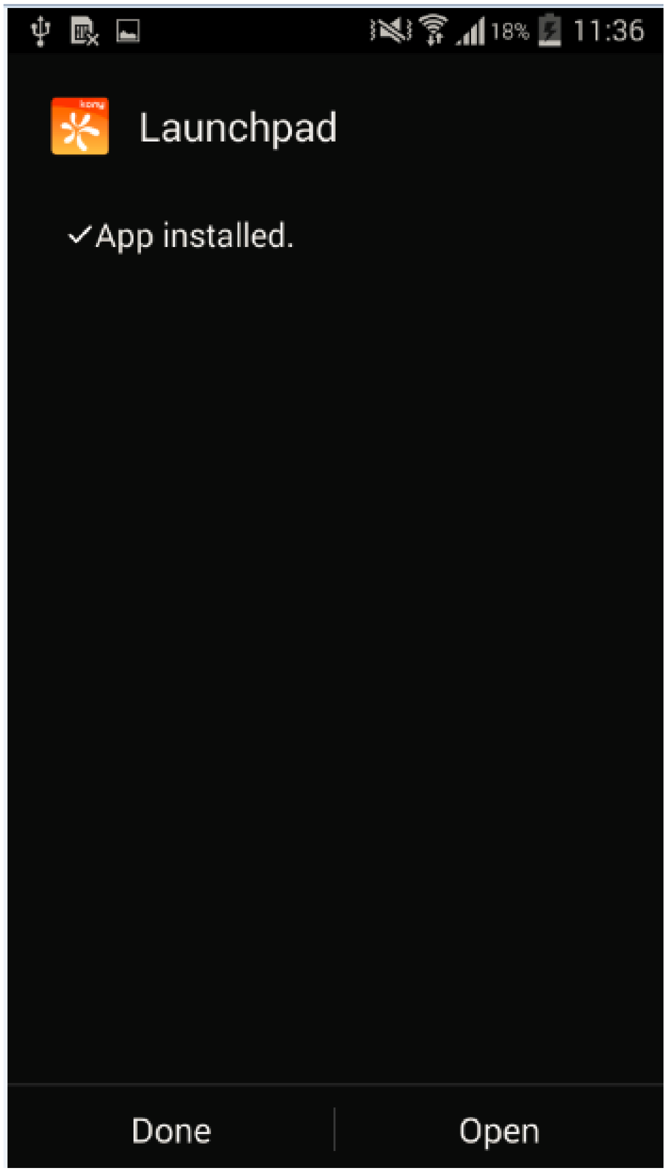
pair with Bluetooth devices

retrieve running apps
run at startup

control vibration
prevent phone from sleeping

modify system settings

3. Click the **Install** button. The installation starts.



Launchpad

✓App installed.

4. Click the **Open** button.

   Kony EMM Login page appears.

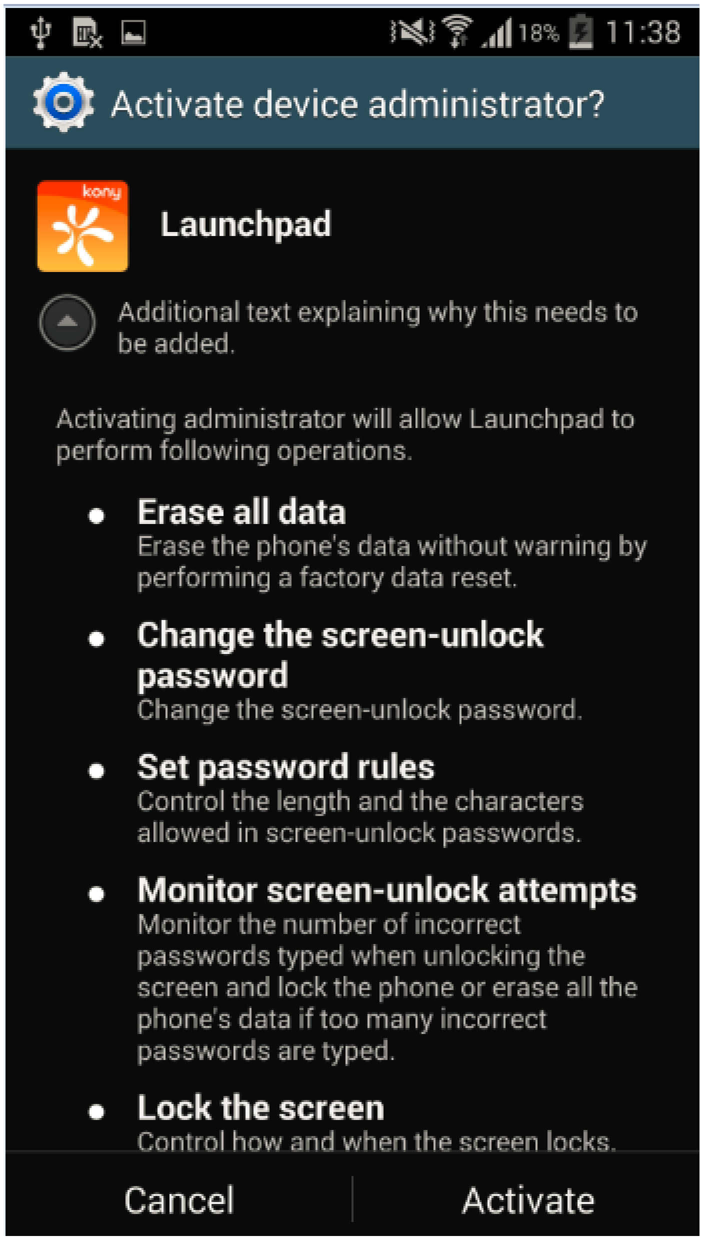
5. Enter your credentials in Username and Password fields.

> *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 enrolled or associated with other users, and is allowed to enroll. Once the server completes this task, the server signals the agent to proceed with enrollment. 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 enrollmentprocess is aborted. The device goes into the terms not accepted state.



11:38

Activate device administrator?

Launchpad

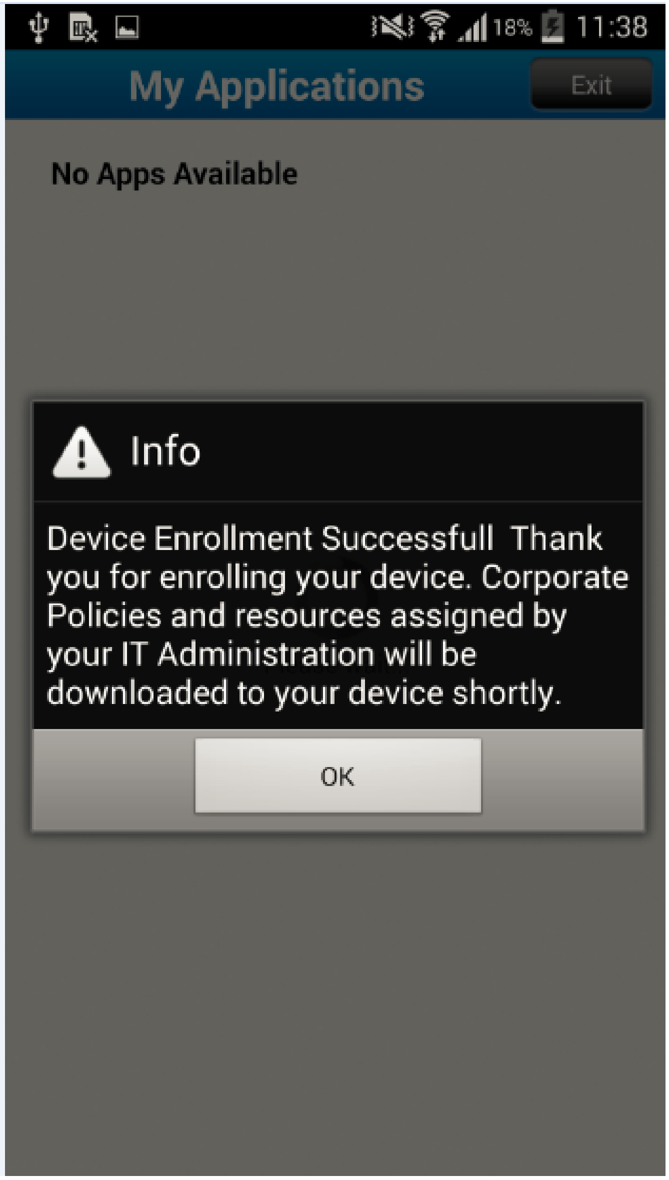
Additional text explaining why this needs to be added.

Activating administrator will allow Launchpad to perform following operations.

- **Erase all data**
  Erase the phone's data without warning by performing a factory data reset.
- **Change the screen-unlock password**
  Change the screen-unlock password.
- **Set password rules**
  Control the length and the characters allowed in screen-unlock passwords.
- **Monitor screen-unlock attempts**
  Monitor the number of incorrect passwords typed when unlocking the screen and lock the phone or erase all the phone's data if too many incorrect passwords are typed.
- **Lock the screen**
  Control how and when the screen locks.

8. The **Active Device Administrator** page appears. Click the **Activate** button.

9. **Installing MDM Profile**: The profile advises a user to download and install an application to complete the process. Choosing to progress automatically triggers the download and installation of the MDM Profile.



No Apps Available

Info

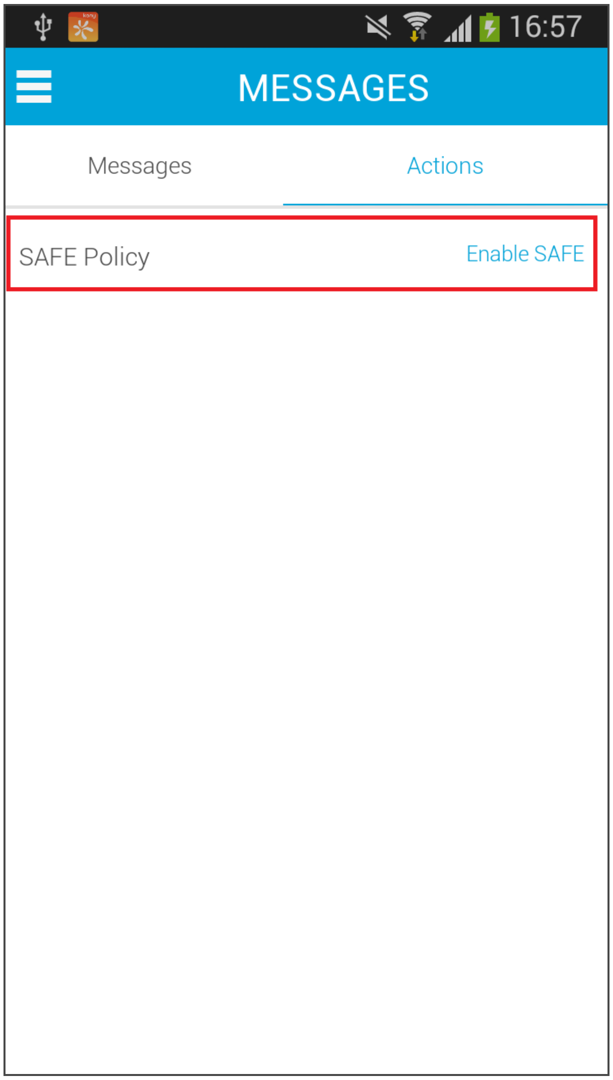
Device Enrollment Successfull Thank you for enrolling your device. Corporate Policies and resources assigned by your IT Administration will be downloaded to your device shortly.

10. 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.

9.2.3.5 SAFE Enrollment

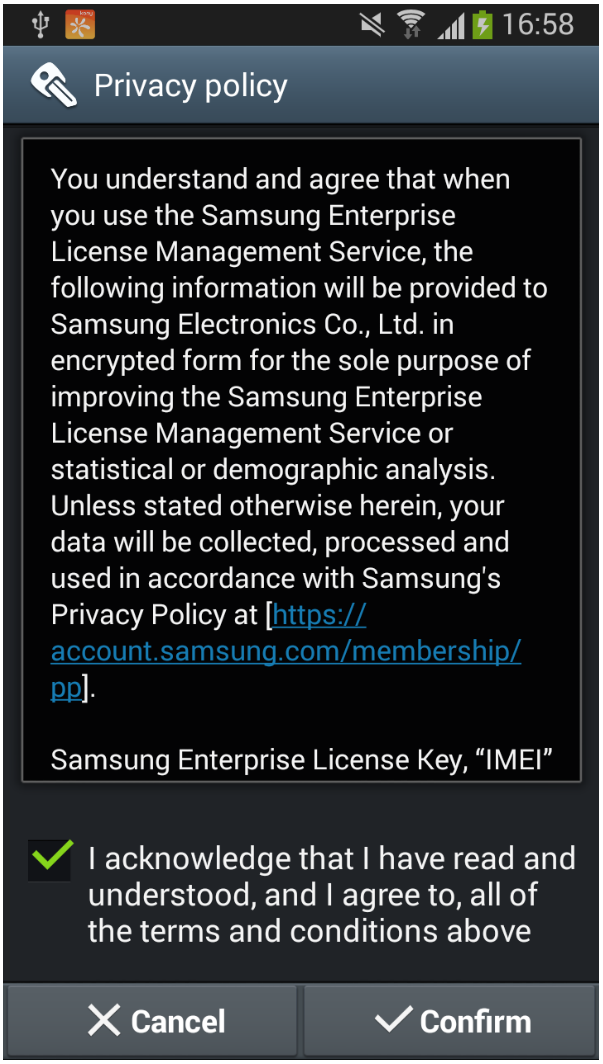
To activate SAFE on supported devices, the SAFE license must be configured at SAFE Settings. The enterprise store app need not be signed by Samsung.

Once SAFE is license configured, all SAFE-supported enrolled devices will receive a push notification shown below.



1. Click **Enable SAFE**. The Privacy Policy screen appears.

   .



Privacy policy

You understand and agree that when you use the Samsung Enterprise License Management Service, the following information will be provided to Samsung Electronics Co., Ltd. in encrypted form for the sole purpose of improving the Samsung Enterprise License Management Service or statistical or demographic analysis. Unless stated otherwise herein, your data will be collected, processed and used in accordance with Samsung's Privacy Policy at [https://account.samsung.com/membership/pp].

Samsung Enterprise License Key, “IMEI”

☑ I acknowledge that I have read and understood, and I agree to, all of the terms and conditions above

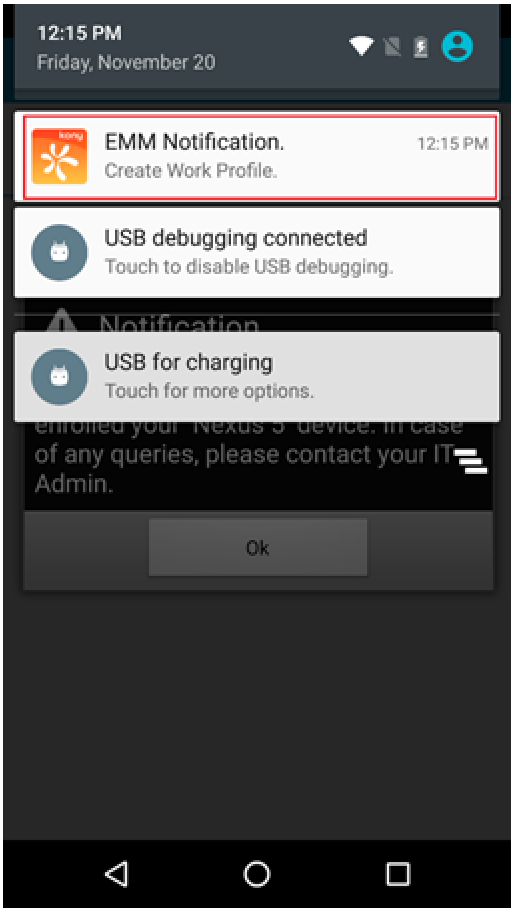
2. Click **Confirm**. The system displays **License Activated** message on the device.

9.2.3.6 Android For Work Settings

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:

1. Touch the notification to create work profile. The enterprise store opens.



12:15 PM
Friday, November 20

EMM Notification. 12:15 PM
Create Work Profile.

USB debugging connected
Touch to disable USB debugging.

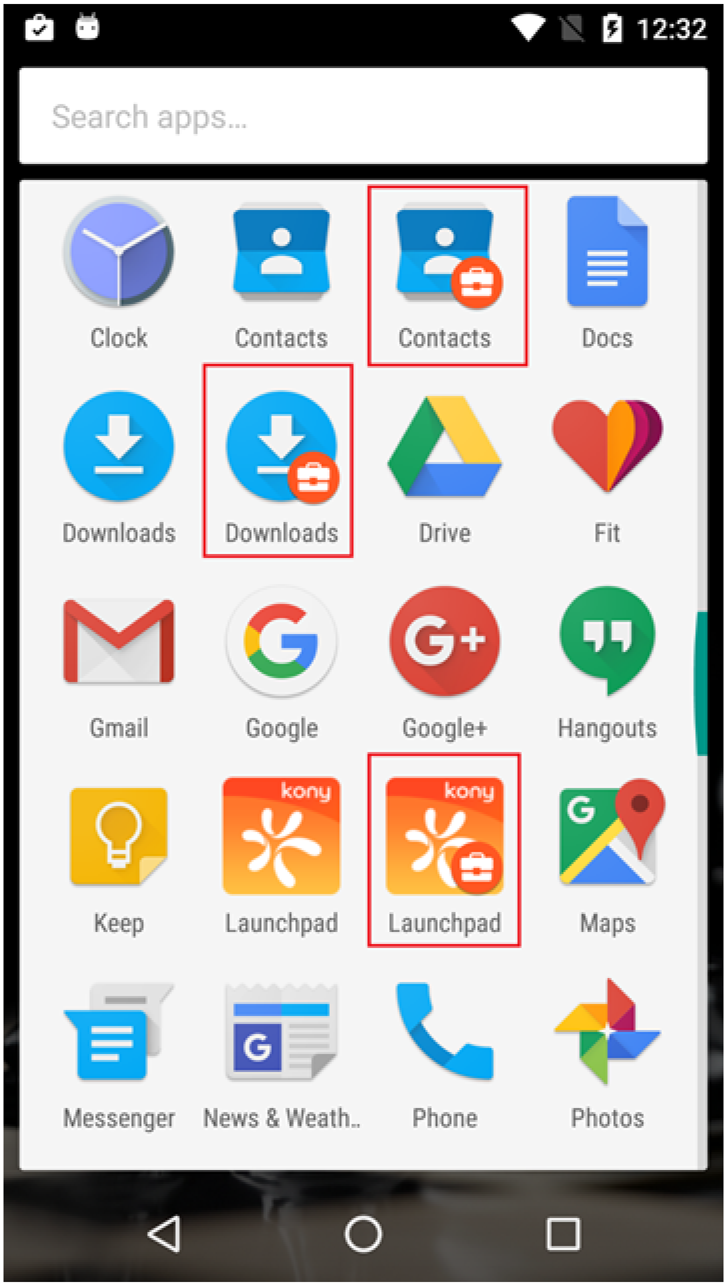
Notification

USB for charging
Touch for more options.

enrolled your Nexus 5 device. In case of any queries, please contact your IT Admin.

2. Navigate to **Messages** > **Actions**.
3. In the Actions page, touch **Create**. Follow the instructions on the device to create your work profile. When asked for, provide your work username and password.

   Once you have the work profile configured, all work profile apps will have an Android For Work icon to them.



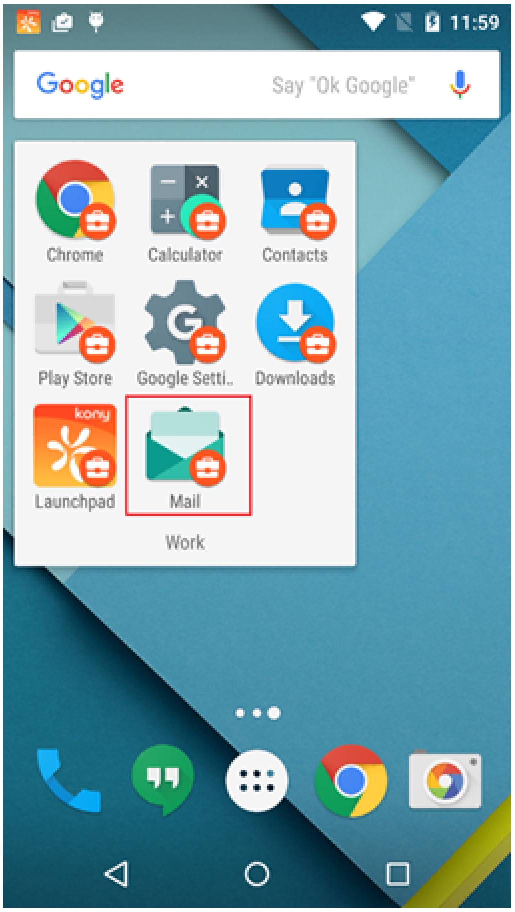
Once you create the work profile, if your Email policy for Android For Work Email is configured, you will receive a notification to download and install the Divide Productivity app.

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.



9.3 Device Enrollment for Windows 6.x

To enroll a device for Windows 6.x, Admin needs to import the required user from the Active Directory. Once the user is imported from Active Directory, Admin enrolls a new Device with user-id and email address of the required user.

See Importing a User from Active Directory.

Once the user is imported from active directory, continue to do the following.

9.3.1 Admin Initiated Enrollment

From the **Device Management** section, click the **Device Enrollment** from the left panel. The Device Enrollment page appears with a list of the users who have enrolled devices. The list view displays a list of all users along with their device enrollment details.

You can perform the following activities from this page:

- Adding a New Device

9.3.1.1 Adding a New Device

This process falls under Admin Enrollment. These devices are enrolled to EMM Server.

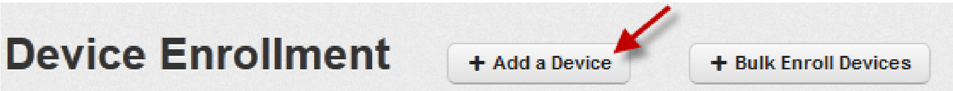
The **Add a Device** window includes three steps to enroll a new device to EMM.

- Step 1: User Information
- Step 2: Asset Information
- Step 3: Confirmation

Step 1: User Information

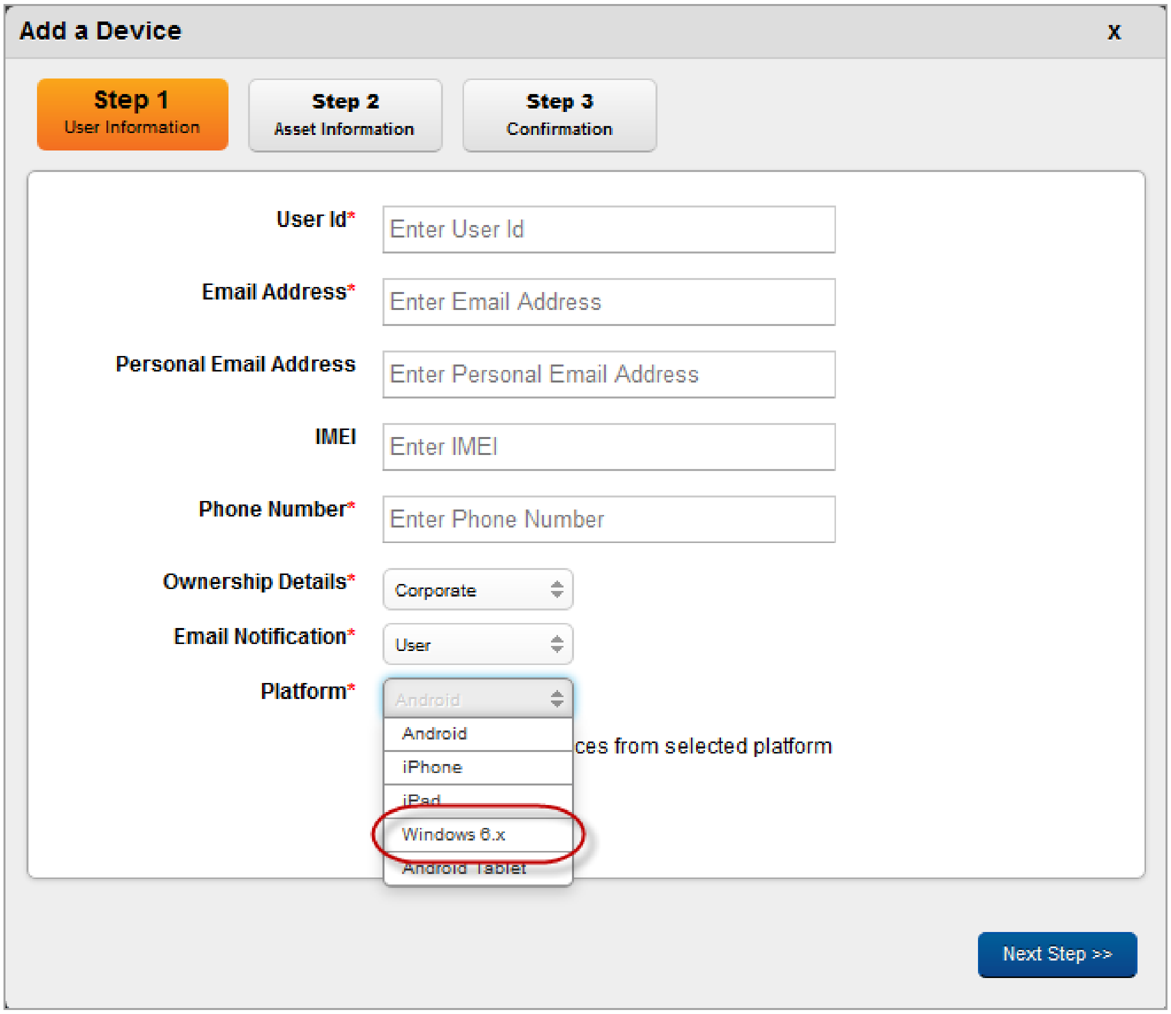
To add a new device, follow these steps:

1. To open the **Add a Device** window, click the **+ Add a Device** button next to the **Device Enrollment** label at the top of the page.



The **Add a Device** window appears.

2. Enter the following details under Step One:



Add a Device

User Id* Enter User Id

Email Address* Enter Email Address

Personal Email Address Enter Personal Email Address

IMEI Enter IMEI

Phone Number* Enter Phone Number

Ownership Details* Corporate

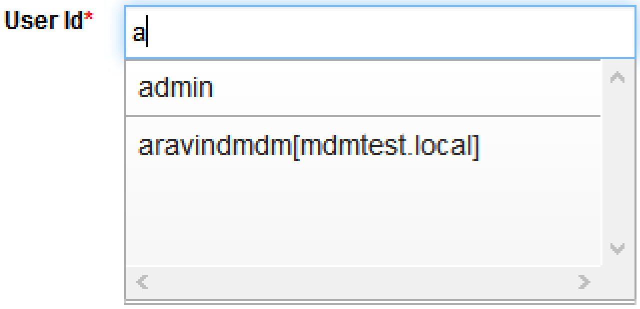
Email Notification* User

Platform* Android

ces from selected platform

3. **User ID**: Enter the partial name of the user and a pop-up window with a list of user names appears.

> *Note:* Only Users that are enrolled with EMM are shown. This includes Active Directory Users as well as Kony Database Users. Select the name of the User whose device you wish to enroll.



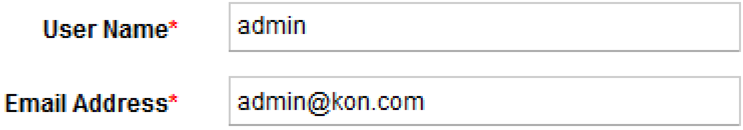
User Id* a

admin

aravindmdm[mdmtest.local]

4. **Email Address**: As per selected User name, the corresponding email address is populated in the **Email address** field.

   The enrollment request and registration instructions are sent to the user on this email address. This Email address is auto-populated from User details (as recorded while the User was enrolled).



User Name*	admin
Email Address*	admin@kon.com

5. **Personal Email Address:** The Admin must provide the personal email id of the employee - should they have it.

   Personal email id of the user is required for additional contact details.

6. **IMEI**: Enter the Mobile Equipment Identity Number.

   > ***Note:*** If you enter IMEI in incorrect format, the following warning messages appears:
   > • Please enter at least 15 characters.
   > • Please enter only digits.

7. **Phone Number**: Enter the Phone Number.

   This is the phone number of the Device User as provided in User details; This is expected to be the phone number of the device.If you enter phone number in incorrect format, system displays warning message to enter at least 11 characters.

8. **Ownership Details**: Choose the type of Ownership of the device. There are three types: **Corporate**, **Employee** and **Shared**.

   This pertains to ownership of the device. The device can be owned by an employee, or Corporate, or shared. Shared refers to devices that are owned by the corporate but shared between multiple employees. An example is a device used by the testing team - different people use each device to test different aspects.

9. **Email Notification**: Choose the type of email notification. There are two types, **User** and **Admin and User.** The enrollment notification is sent to the specified personnel.

   Email notifications are sent to individual User regarding enrollment of the device and what further actions are required to accomplish the task.

10. **Platform**: Choose the appropriate Operating System that the device supports.

    If you wish to enroll devices from the selected platform only, then select the check box **Only enroll devices from selected platform**.

    The platform on which the device resides. The supported Device OS are: iOS, Android, Windows 6.x, and Windows Phone 8.

    > ***Note:*** For Windows 6.x device only requests sent for Windows 6.x platform are allowed for enrollment. For other platforms, the system allows cross-platform requests for enrollment.

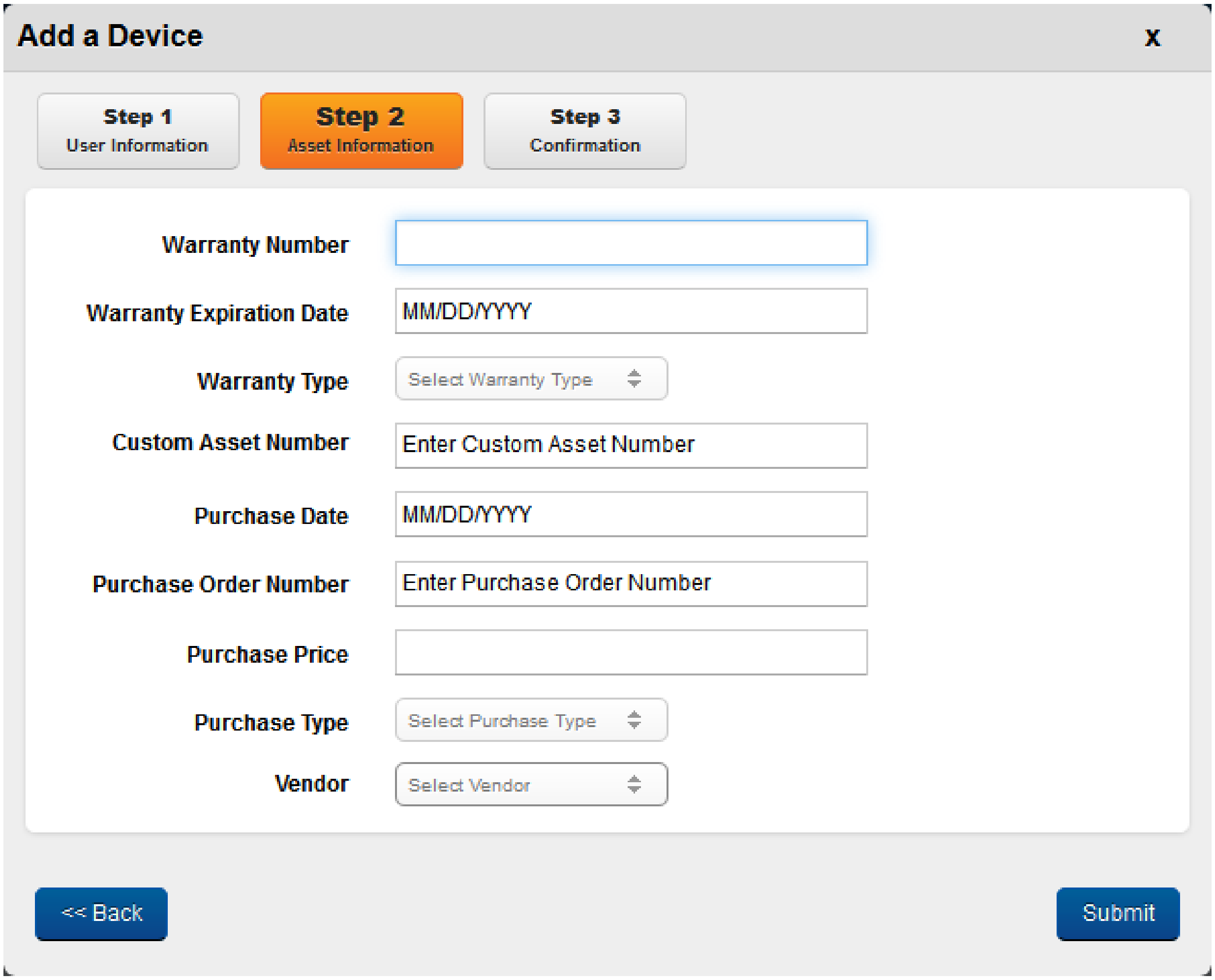
11. Click the **Next Step** button to open **Step 2** window.

    > ***Important:*** Windows 6.x devices can only be enrolled if the Admin initiated request specified the platform to be Windows 6.x. It cannot be enrolled if the request is raised against any other platform. It must also be ensured that the Windows MDM Server has no residual users in it before you begin Windows 6.x device enrollment. If there are any, such users are enrolled automatically.

Step 2: Asset Information

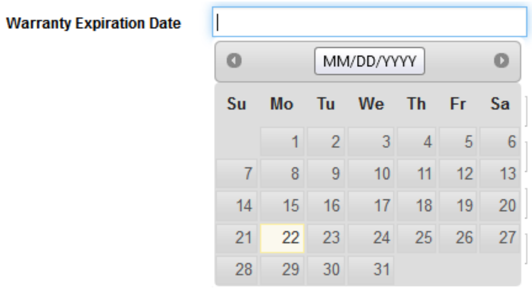
Asset information is not the basic information of the device. It is required if the device needs repair and so on. This step is useful, if there is an asset tracking mechanism in the organization. None of the details in this step are mandatory.

Enter the following details in Step Two:



Warranty Number	
Warranty Expiration Date	MM/DD/YYYY
Warranty Type	Select Warranty Type
Custom Asset Number	Enter Custom Asset Number
Purchase Date	MM/DD/YYYY
Purchase Order Number	Enter Purchase Order Number
Purchase Price	
Purchase Type	Select Purchase Type
Vendor	Select Vendor

1. **Warranty Number**: Enter the valid warranty number.This is the unique identification number to identify the warranty type.



Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

2. **Warranty Expiration Date**: Enter the cursor in the **Warranty Expiration Date** field. A Calendar window with current month and current date as active, appears. Select the required date. The date is populated in the text field.

   After this date, the warranty expires.

3. **Warranty Type**: Select the appropriate warranty from the **Select Warranty Type** drop-down list.

   There are three warranty types respectively, Manufacturer warranty, Seller Warranty and the Extended Warranty.

4. **Custom Asset Number**: Enter the valid custom asset number in the **Enter Custom Asset Number** text field. This number is given by company to define asset information.

5. **Purchase Date**:Enter the cursor in the **Purchase Date** field. A Calendar window with current month and current date as active, appears. Select the required date. The date is populated in the text field.

   Purchase date cannot be in a future date.

6. **Purchase Order No**: Enter the purchase order number of the device in **Enter Purchase Order Number** text field.A purchase order number is an alpha/numeric code that is assigned to a particular request to buy something. PO numbers are used internally to track purchases. valid purchase price for the device. If you enter wrong purchase price, a warning message to enter valid purchase price appears.

7. **Purchase Price**: Enter a purchase price.

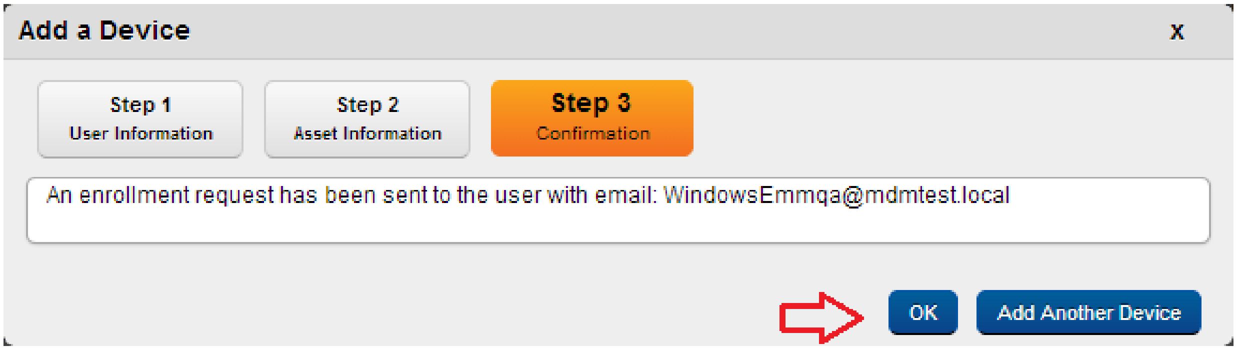
8. **Purchase Type**: Select Purchase Type as **Single Purchase** or **Volume Purchase** from the **Select Purchase Type** drop-down list.

9. Click the **Submit** button to open **Step 3** window.

   Click the **Back** button to navigate to **Step 1**.

Step 3: Confirmation

Step Three window displays confirmation message stating that the enrollment request and registration instructions are sent at the specified email address of the administrator.



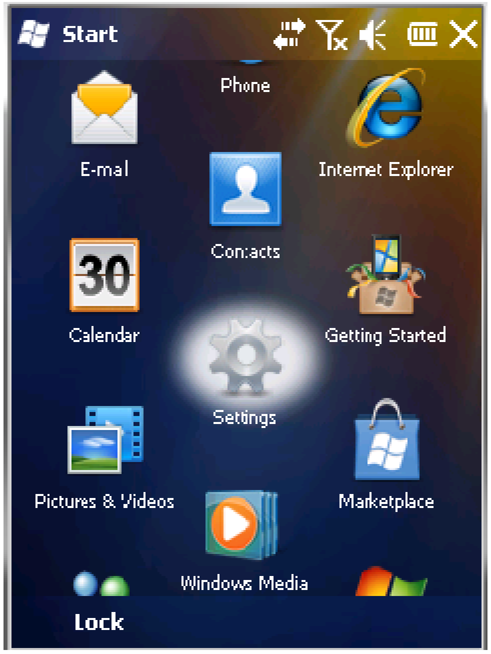
An enrollment request has been sent to the user with email: WindowsEmmqa@mdmtest.local

1. Click the **OK** button to proceed.

2. Click the **Add Another Device** button to open **Step 1** window to enroll a new device with EMM.

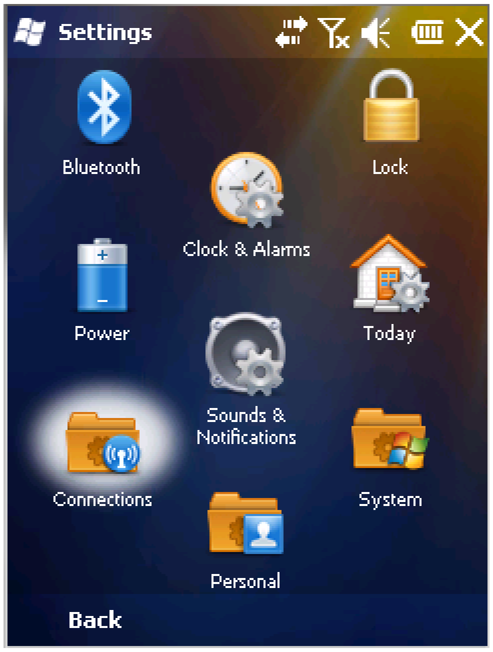
9.3.2 Windows 6.x device

Once the device details are provided in Kony EMM server, do the following to complete the device enrollment. For device enrollment with Kony EMM, user has to see previous chapters/sections.



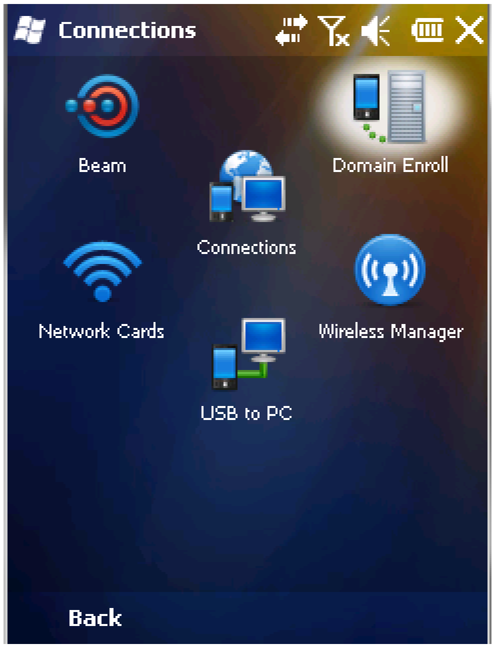
Windows 6.x device displays various icons on **Start** screen.

1. Click **Settings** icon to open the Settings screen.



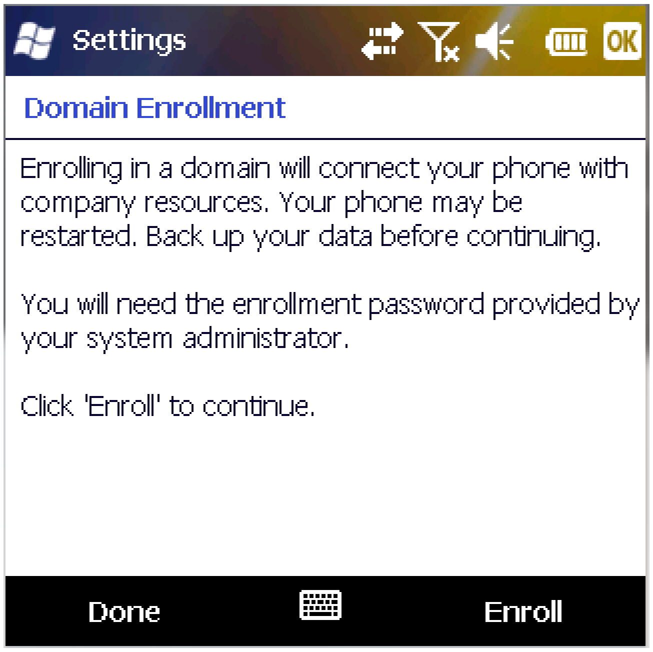
2. when you click Settings icon,**Connection** icon is displayed on screen.

3. Click the **Connections** icon to open the Connections screen.



Connection screen appears.

4. Click the **Domain Enroll** icon.



Domain Enrollment

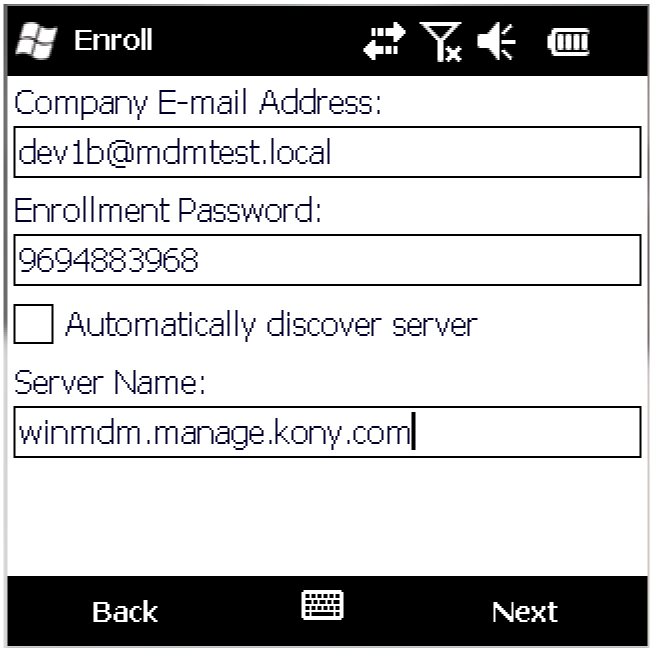
Enrolling in a domain will connect your phone with company resources. Your phone may be restarted. Back up your data before continuing.

You will need the enrollment password provided by your system administrator.

Click 'Enroll' to continue.

Settings screen appears with instructions about Domain Enrollment.

5. Click **Enroll** to continue.



Company E-mail Address:
dev1b@mdmtest.local

Enrollment Password:
9694883968

□ Automatically discover server

Server Name:
winmdm.manage.kony.com

Enroll screen appears.

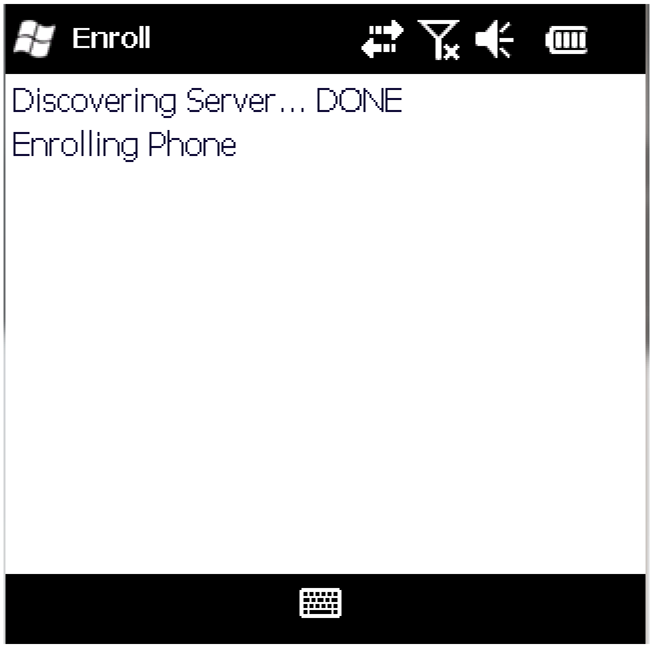
6. Enter details for the following fields:

   a. **Company E-mail Address**: Enter your email address.

   b. **Enrollment Password**: Enter your password. This password is provided by the Admin.

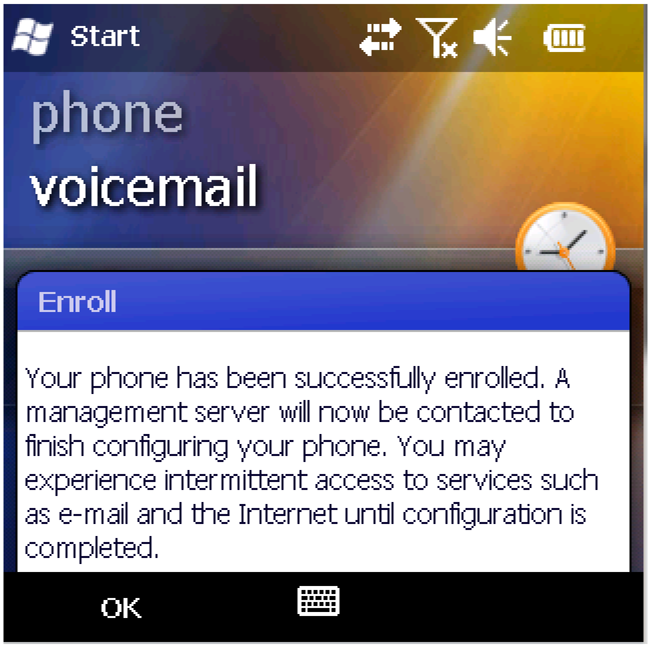
   c. **Automatically Discover Server**: Leave this option as default.

   d. **Server Name**: Enter the server name.



Discovering Server… DONE
Enrolling Phone

7. Click **Next** to continue. The enrollment process begins.



Your phone has been successfully enrolled. A management server will now be contacted to finish configuring your phone. You may experience intermittent access to services such as e-mail and the Internet until configuration is completed.

A success message about device enrollment is displayed on screen.

8. Click **OK** to continue.

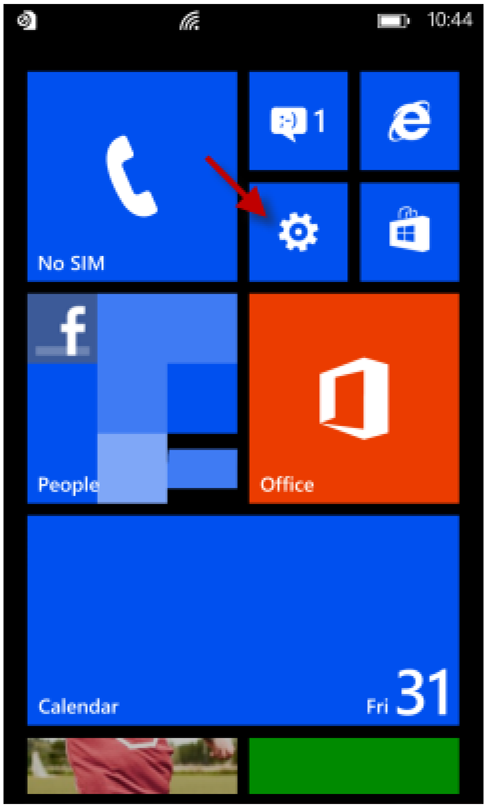
9.4 Enroll Windows Phone 8 Devices

To enroll Windows Phone 8 devices, follow these steps:

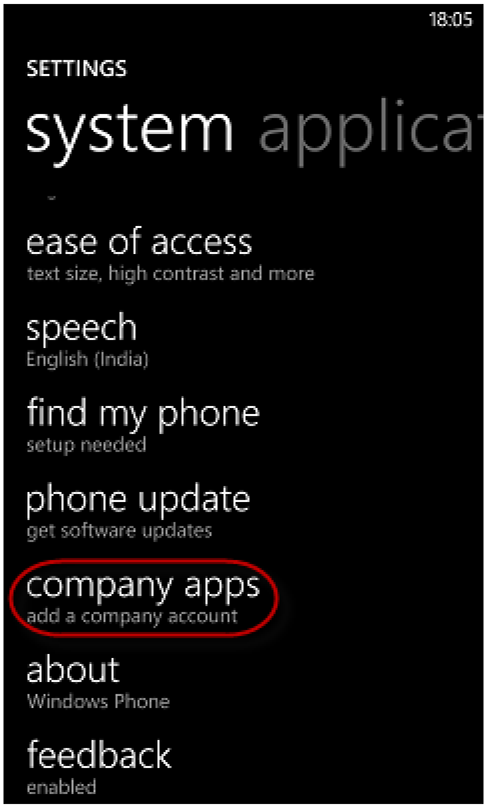
> ***Note:*** If an enrolled phone 8 device is upgraded to phone 8.1, the user's device record on EMM must be deactivated by the administrator and the user should enroll again.

9.4.1 Enrollment

The built-in MDM agent in the operating system is used to enroll the device. After the device enrolls successfully, system pushes the enterprise store application onto the device.



1. Tap the **Settings** icon to open Settings screen on the device.



18:05

SETTINGS

system applica

ease of access
text size, high contrast and more

speech
English (India)

find my phone
setup needed

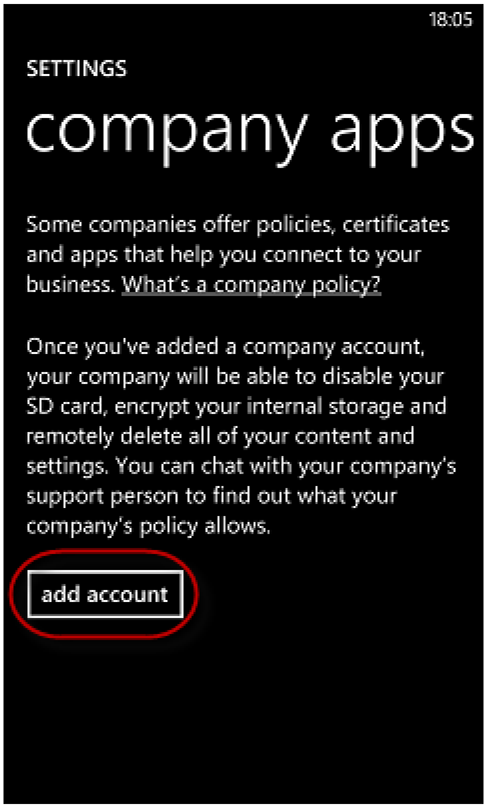
phone update
get software updates

company apps
add a company account

about
Windows Phone

feedback
enabled

2. Tap the **company apps** link to open company apps screen.



18:05

SETTINGS

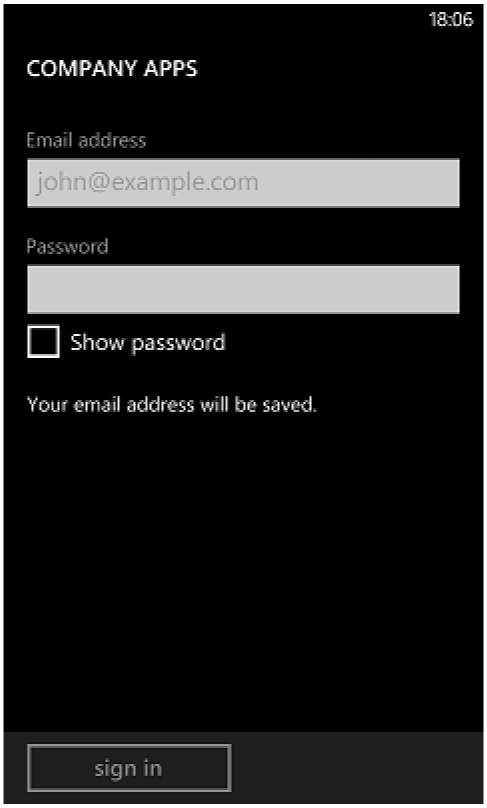
company apps

Some companies offer policies, certificates and apps that help you connect to your business. What's a company policy?

Once you've added a company account, your company will be able to disable your SD card, encrypt your internal storage and remotely delete all of your content and settings. You can chat with your company's support person to find out what your company's policy allows.

3. Tap **add account** to continue.

> *Important:* For Nokia Windows Phone 8 device enrollments, Nokia account registration is a pre-requisite.



18:06

COMPANY APPS

Email address

john@example.com

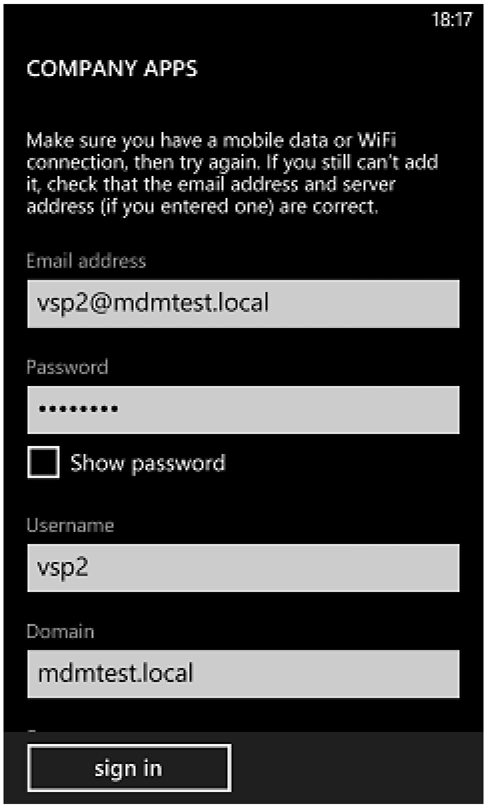
Password

□ Show password

Your email address will be saved.

4. Enter your credentials in the following fields:
    a. **Email Address**: Enter your email address.
    b. **Password**: Enter your password.

5. Tap **Sign in** to continue.



18:17

COMPANY APPS

Make sure you have a mobile data or WiFi connection, then try again. If you still can't add it, check that the email address and server address (if you entered one) are correct.

Email address: vsp2@mdmtest.local

Password: ••••••••

□ Show password

Username: vsp2

Domain: mdmtest.local

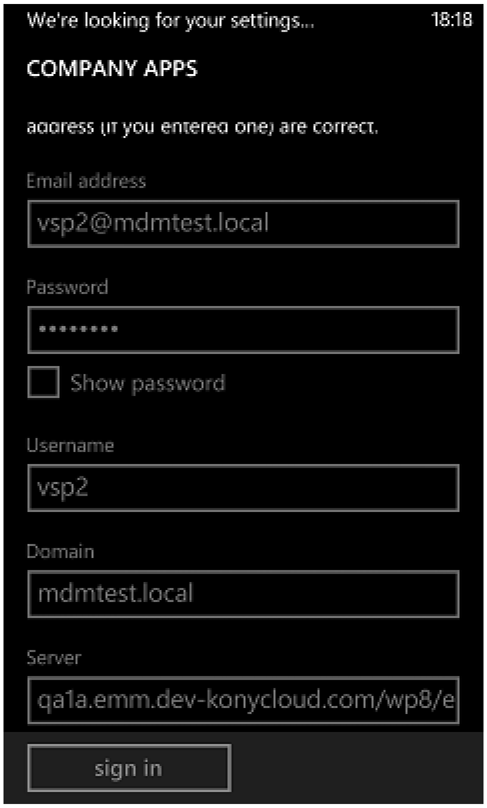
Username, Domain and Server fields appear.

6. Enter details in the following fields:

   a. **Username**: Enter your User name.

   b. **Domain**: Enter your domain.

7. Enter the Server address and tap **sign in** to continue.



We're looking for your settings... 18:18

COMPANY APPS

aaaress (IT you enterea one) are correct.

Email address

vsp2@mdmtest.local

Password

••••••••

□ Show password

Username

vsp2

Domain

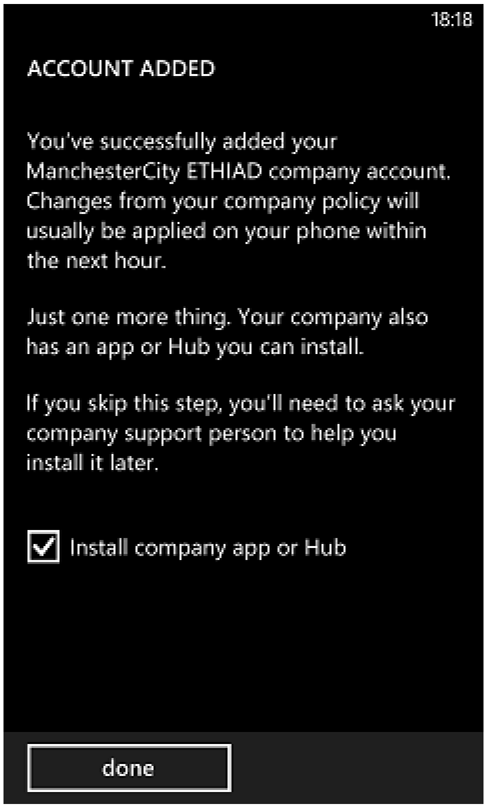
mdmtest.local

Server

qa1a.emm.dev-konycloud.com/wp8/e

System verifies the entered credentials and displays the confirmation message.

> ***Important:*** Server name is should be your server URL, device name and your enroll enrollment endpoint. For example, *yourcompany.com/wp8/enroll*



18:18

ACCOUNT ADDED

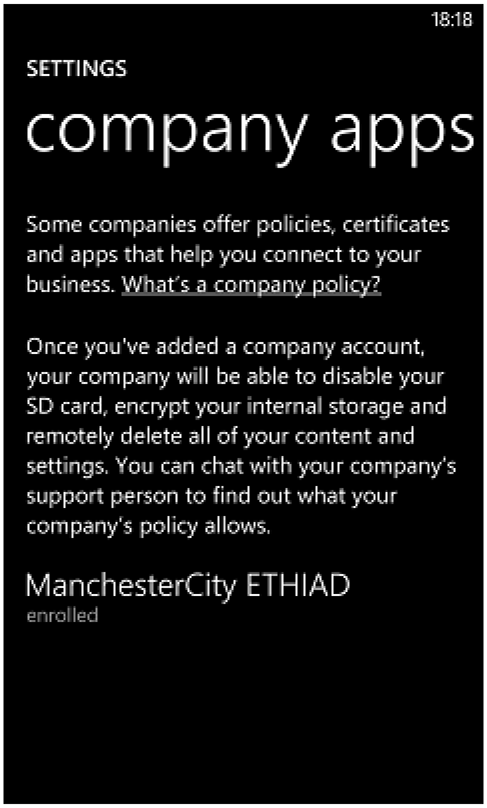
You've successfully added your ManchesterCity ETHIAD company account. Changes from your company policy will usually be applied on your phone within the next hour.

Just one more thing. Your company also has an app or Hub you can install.

If you skip this step, you'll need to ask your company support person to help you install it later.

☑ Install company app or Hub

8. Once, credentials are verified, **Account Added** message is displayed. Tap **done**. The enrollment process is now complete.



SETTINGS

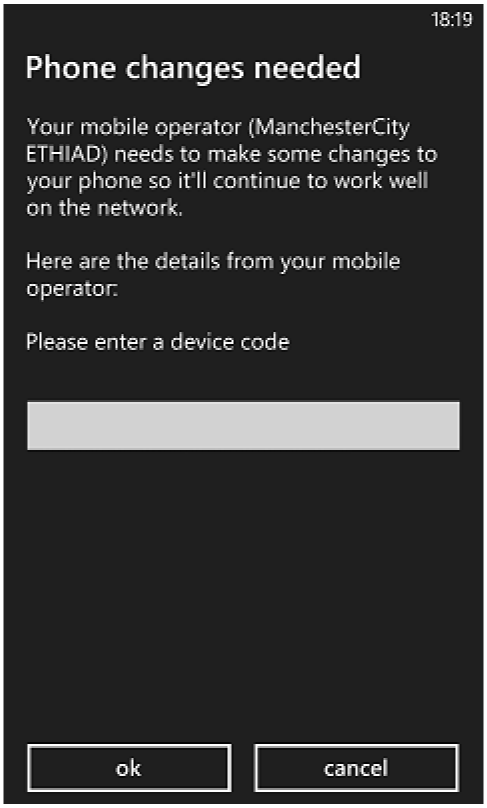
company apps

Some companies offer policies, certificates and apps that help you connect to your business. What's a company policy?

Once you've added a company account, your company will be able to disable your SD card, encrypt your internal storage and remotely delete all of your content and settings. You can chat with your company's support person to find out what your company's policy allows.

ManchesterCity ETHIAD
enrolled

9. You can return to the home screen.



18:19

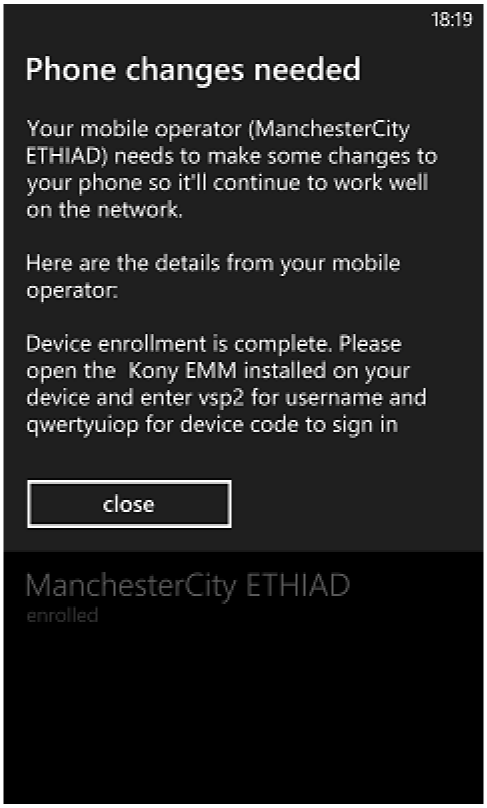
Phone changes needed

Your mobile operator (ManchesterCity ETHIAD) needs to make some changes to your phone so it'll continue to work well on the network.

Here are the details from your mobile operator:

Please enter a device code

10. Enter a code of your choice and remember to enter the same when prompted from the enterprise store application.Tap **OK** to continue.



18:19

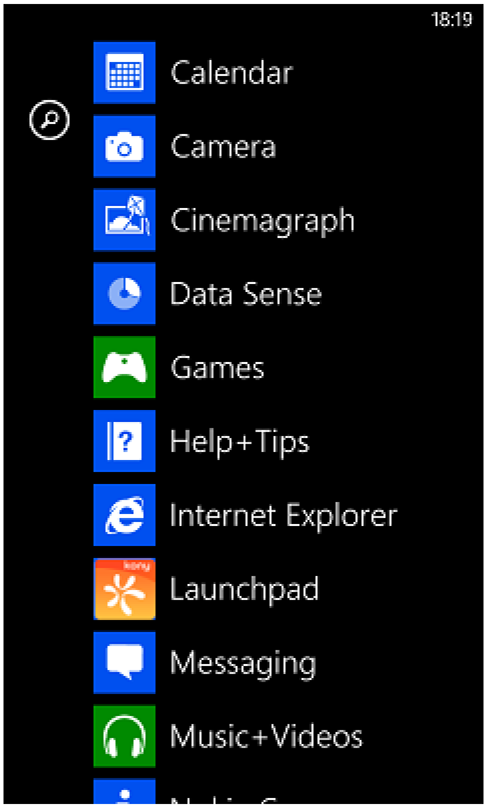
Phone changes needed

Your mobile operator (ManchesterCity ETHIAD) needs to make some changes to your phone so it'll continue to work well on the network.

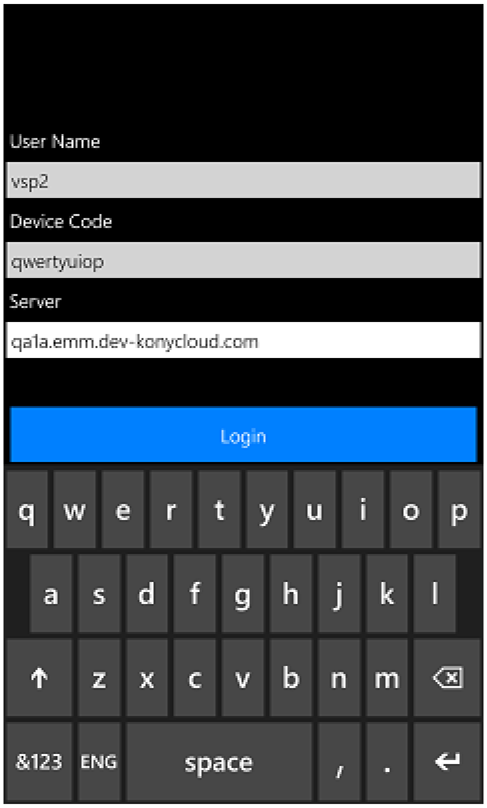
Here are the details from your mobile operator:

Device enrollment is complete. Please open the Kony EMM installed on your device and enter vsp2 for username and qwertyuiop for device code to sign in

11. Tap **close**. Your device is now enrolled.



Device screen displays all the available icons.



User Name
vsp2

Device Code
qwertyuiop

Server
qa1a.emm.dev-konycloud.com

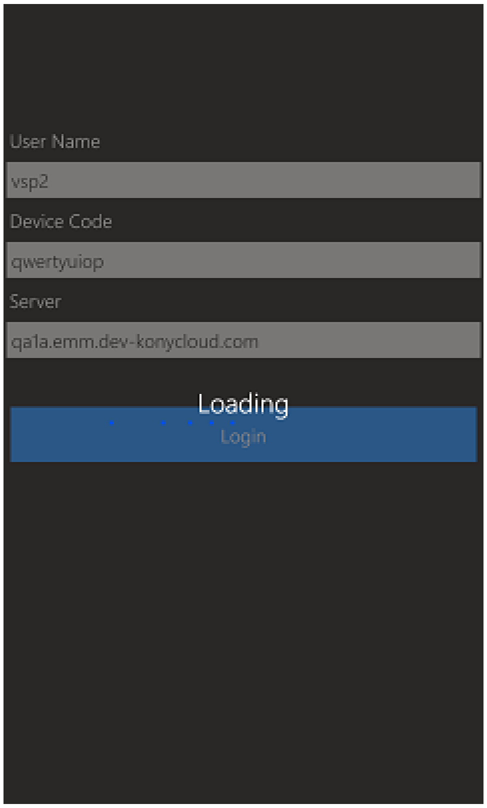
12. Once enrollment is complete you need to open the enterprise store application and enter the necessary details.Enter details for the following fields:

    a. **User Name**: Enter the user name.

    b. **Device Code**: Enter the device code. (The same code of your choice you entered while enrolling). Only ASCII characters are accepted and no other special characters.

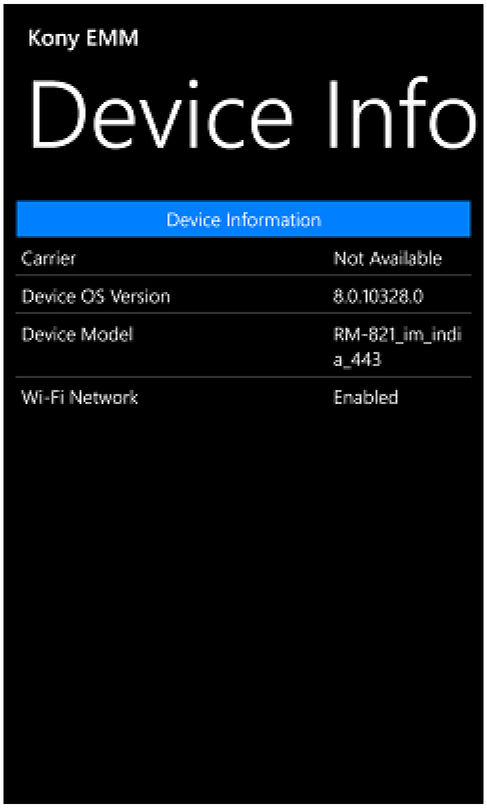
    c. **Server**: Enter the server address.

13. Tap **Login** to continue.



User Name
vsp2
Device Code
qwertyuiop
Server
qa1a.emm.dev-konycloud.com

System validates the entered credentials.



Kony EMM

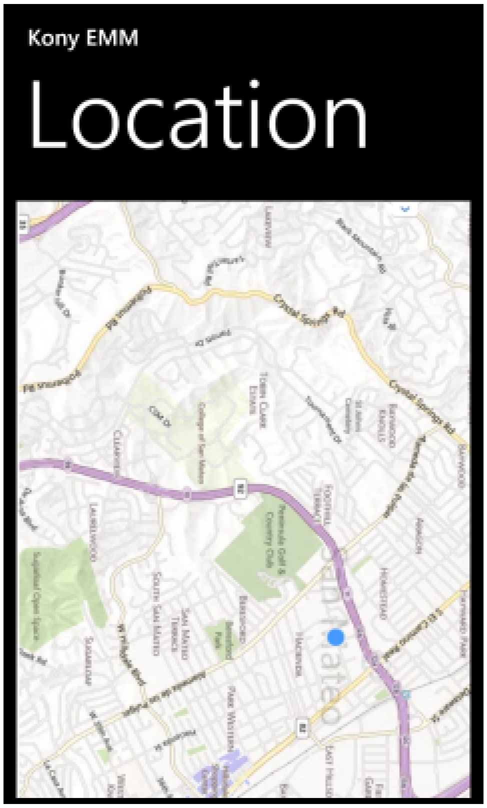
Device Info

Device Information	
Carrier	Not Available
Device OS Version	8.0.10328.0
Device Model	RM-821_im_india_443
Wi-Fi Network	Enabled

Device info screen appears with following details

The Device Info page displays the complete information of the device. The page displays the following details:

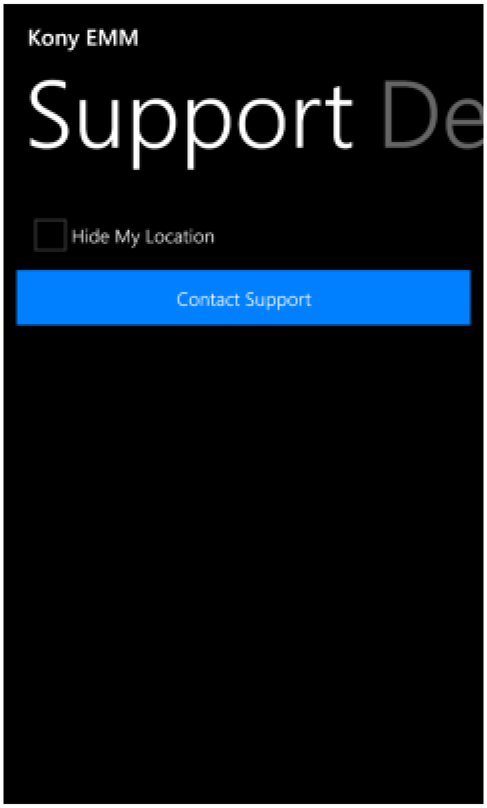
- **Carrier** (Service Provider with which the device currently works.)
- **Device OS Version** (Current device OS version)
- **Device Model**
- **WiFi Network** (it only defines if the WiFi is enabled or not)



Kony EMM

Location

14. Tap the Menu button to navigate to the **Location** screen. This screen displays the location details on a map. You can use the zoom tool to change the size of the visible area.



15. Tap the Menu button to navigate to the **Support** screen. When a user wishes to get support through the device agent, the communication is enabled through email option only.

9.4.2 Enroll Windows Phone 8X Devices

Windows 8X devices can be enrolled through a server and the device. The following sections review the process:

- User Initiated Device Enrollment
- Administrator Initiated Enrollment

> ***Note:*** If an enrolled Windows Phone 8 device is upgraded to Window Phone 8.1, the record for a user's Windows Phone 8X device must be deactivated by the administrator. The user must re-enroll.

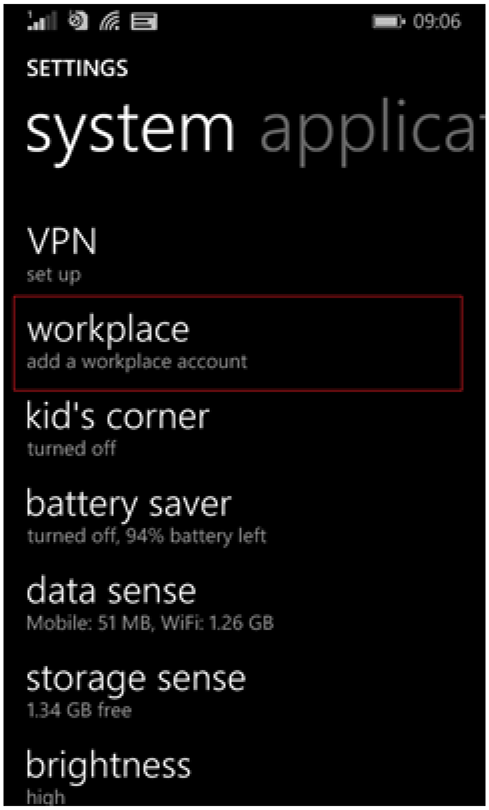
9.4.2.1 User Initiated Enrollment

The built-in MDM agent in the operating system enrolls the device. After the device enrolls successfully, the system pushes the enterprise store application onto the device.

To enroll a Windows Phone 8X device follow these steps:

1. Navigate to the enrollment URL provided by your administrator using Internet Explorer on the device. Instructions on how to enroll the device appear.
2. Make a note of server and endpoint details.
3. Navigate to **Settings**.

4. Tap the **Settings** icon to open the device's Settings screen.



09:06

SETTINGS

system applica

VPN
set up

workplace
add a workplace account

kid's corner
turned off

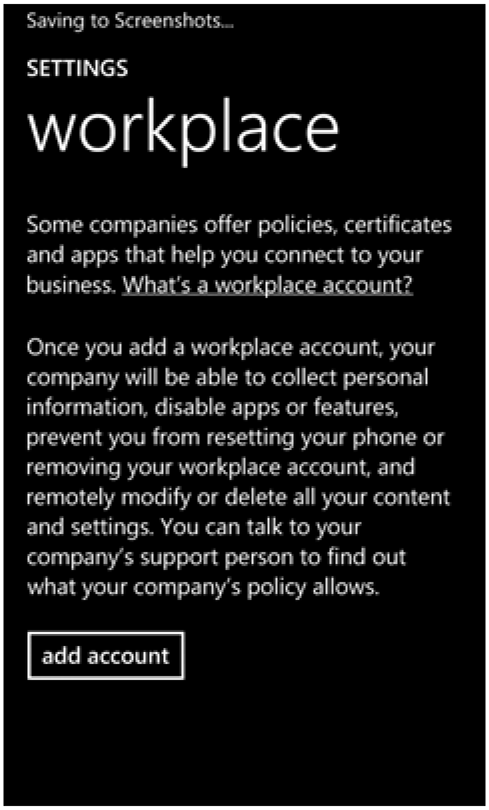
battery saver
turned off, 94% battery left

data sense
Mobile: 51 MB, WiFi: 1.26 GB

storage sense
1.34 GB free

brightness
high

5. Tap the **Workplace** link to open workplace screen.



Saving to Screenshots...

SETTINGS

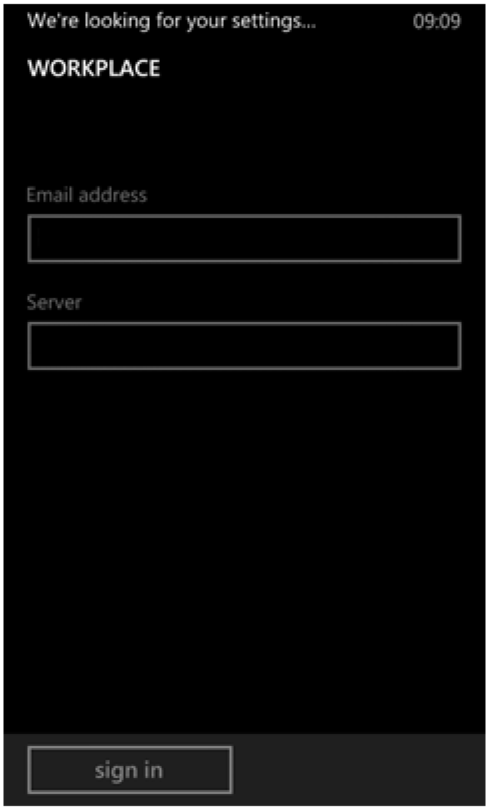
workplace

Some companies offer policies, certificates and apps that help you connect to your business. What's a workplace account?

Once you add a workplace account, your company will be able to collect personal information, disable apps or features, prevent you from resetting your phone or removing your workplace account, and remotely modify or delete all your content and settings. You can talk to your company's support person to find out what your company's policy allows.

6. Tap **add account** to continue.

> *Important:* For enrollments of Nokia Windows Phone 8X devices, Nokia account registration is required.



7. Enter your credentials in the following fields:

   a. **Email Address**: Enter your email address.

   b. **Server**: Enter your server details with endpoint. Contact your administrator for details if you do not have the details.

> *Important:* The server name is your server URL, device name, and your enrollment endpoint. For example, *yourcompany.com/wp8/enroll*

> *Note:* The device will try to auto-discover enrollment server using domain details in your email address. If the device does not display auto-discover enrollment server option, do the following:
> 1. Run the **redgedit** command prompt in Windows.
> 2. Navigate to registry path **HKEY_LOCAL_**

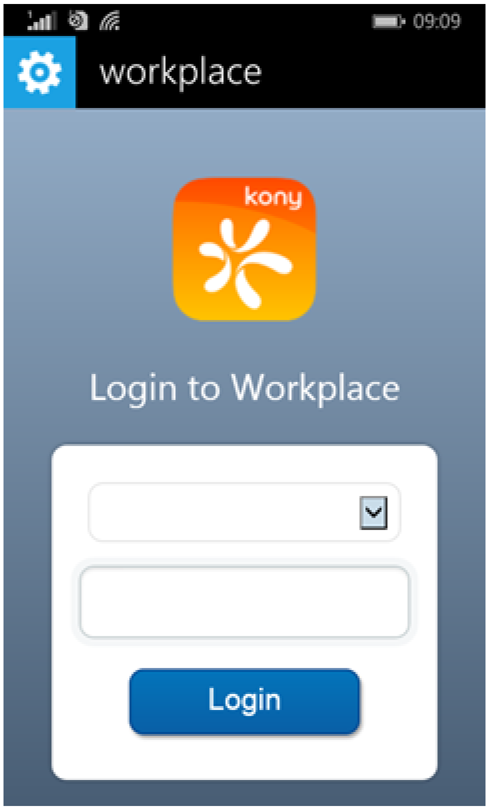
> **MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion**
>
> 3. Right-click on current version and select **New** > **Key**.
>
> 4. Name the key **MDM** and press enter.
>
> 5. Right-click on **MDM** and select, **New** > **String Value**.
>
> 6. Name the string value **Discovery Service** and press enter.
>
> 7. Right-click on Discovery service, select **Modify**.
>
> 8. Enter the server details in the **Value data** text box. If you don't know server details, contact your administrator.

8. Tap **Sign in** to continue.

9. Enter details in the following fields:

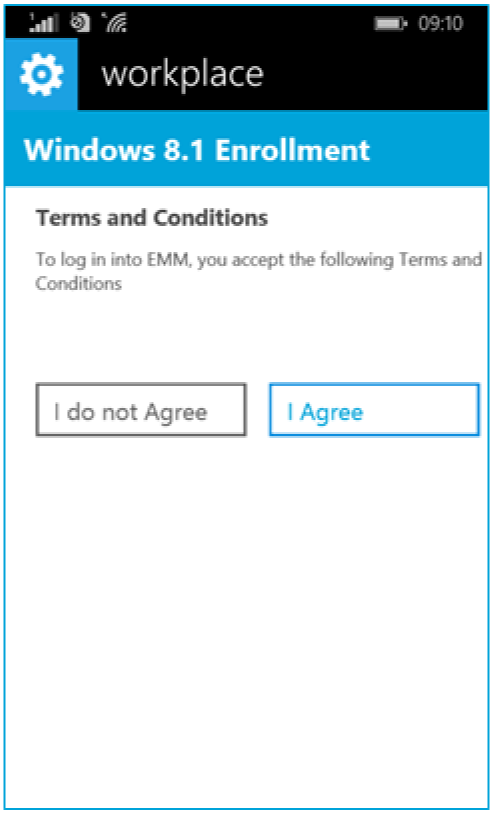
   a. **Username**: Enter your user name.

   b. **Password**: Enter your password.



10. Tap **Login** to continue.

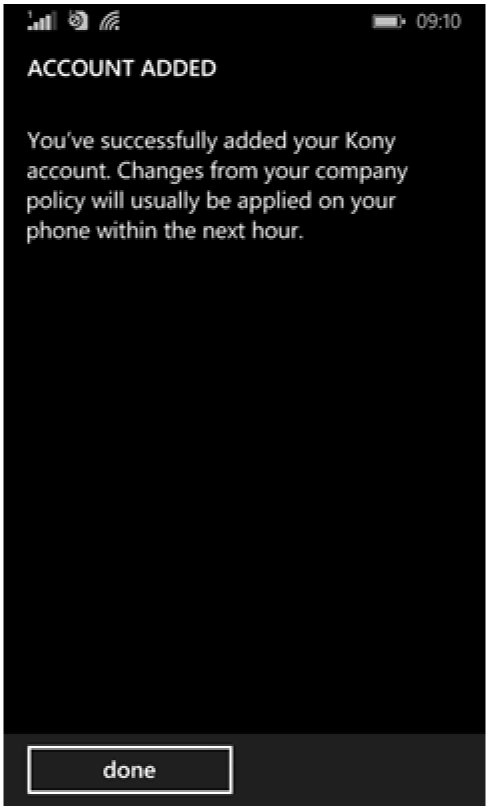
11. The system displays terms and conditions. Tap **I Agree**.



Terms and Conditions

To log in into EMM, you accept the following Terms and Conditions

12. The **Account Added** message is displayed. Tap **done**.

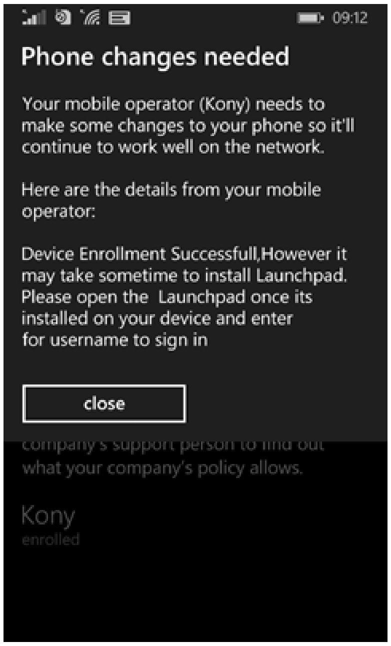


09:10

ACCOUNT ADDED

You've successfully added your Kony account. Changes from your company policy will usually be applied on your phone within the next hour.

13. The Phone changes needed page appears. Tap **close**.



09:12

Phone changes needed

Your mobile operator (Kony) needs to make some changes to your phone so it'll continue to work well on the network.

Here are the details from your mobile operator:

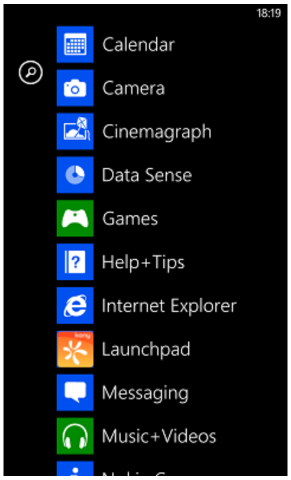
Device Enrollment Successfull,However it may take sometime to install Launchpad. Please open the Launchpad once its installed on your device and enter for username to sign in

close
company's support person to find out
what your company's policy allows.
Kony
enrolled

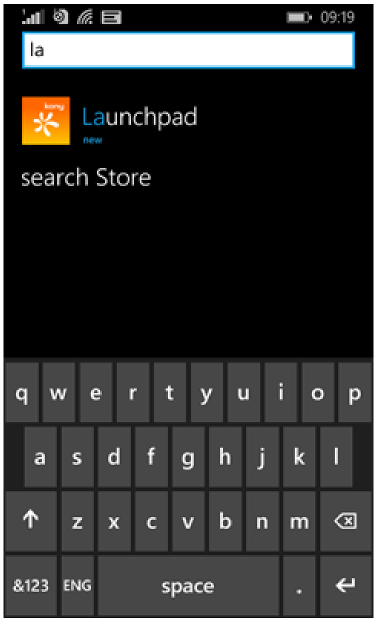
Important: If you have not provided a Symantec Enterprise App Signing Certificate for Windows Phone 8X, after enrollment, enterprise store will not install on the device. Device location, Geo-fence, Time-fence, and Enterprise application management features will not work for the device in the management console. Once the Symantec certificate is provided, from the next ping session, enterprise store will be installed on the device.

Note: Once the enrollment is complete, device will sync with your EMM server. Do not tap the delete button while the device is syncing. If you tap delete, even though the account is deleted on the device, EMM server will continue to consider the device as enrolled and will display its details.

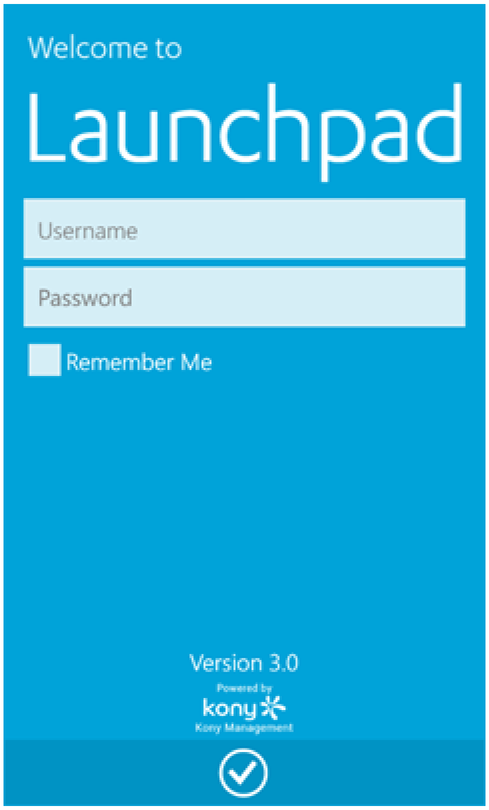
14. The device screen displays all available icons.



Search for enterprise store and open it.

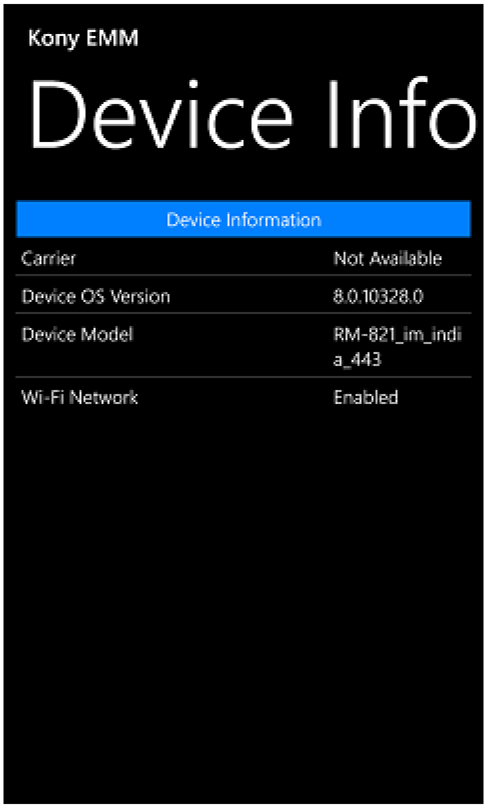


15. enterprise store opens. Enter your user credentials, and then click the login icon.



Your device is now enrolled.

16. The system validates the entered credentials.



Kony EMM

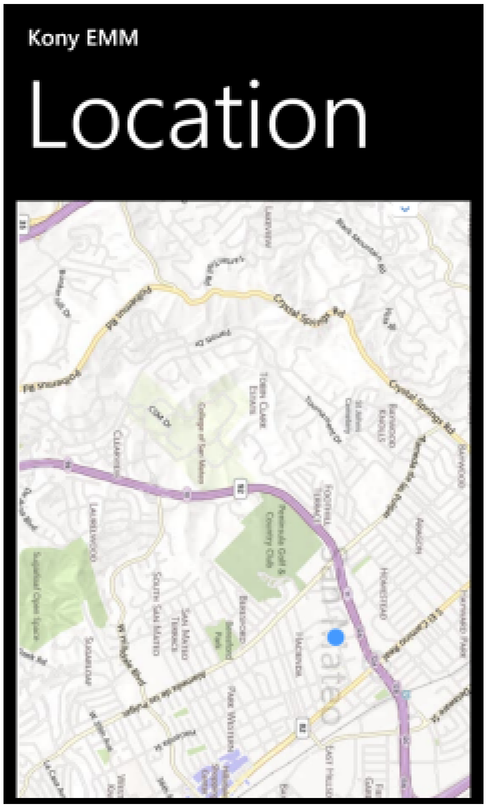
Device Info

Device Information	
Carrier	Not Available
Device OS Version	8.0.10328.0
Device Model	RM-821_im_india_443
Wi-Fi Network	Enabled

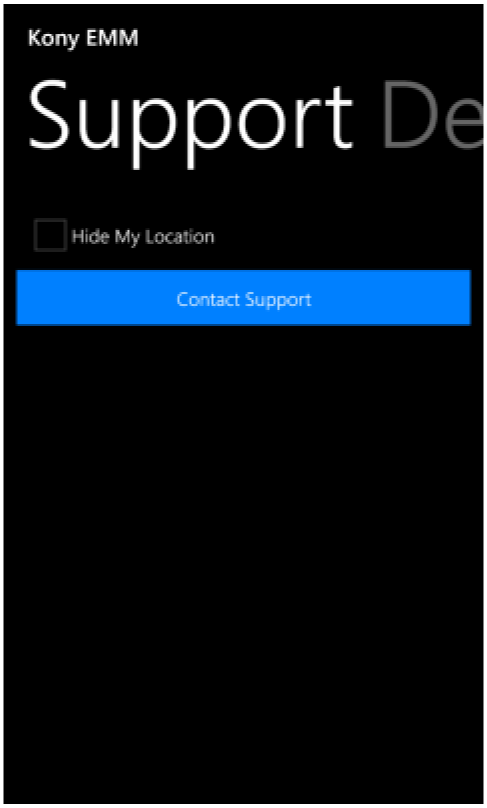
Device info screen appears with following details

The Device Info page displays the complete information of the device. The page displays the following details:

- **Carrier** (Service Provider with which the device currently works.)
- **Device OS Version** (Current device OS version)
- **Device Model**
- **WiFi Network** (it only defines if the WiFi is enabled or not)



17. Tap the Menu button to navigate to the **Location** screen. This screen displays the location details on a map. You can use the zoom tool to change the size of the visible area.



18. Tap the Menu button to navigate to the **Support** screen. When a user wishes to get support through the device agent, the communication is enabled through email option only.

> ***Note:*** During the enrollment process, if your Server SSL certificate is not trusted by the device or if the device date and time are incorrect, a jargon alert will appear.

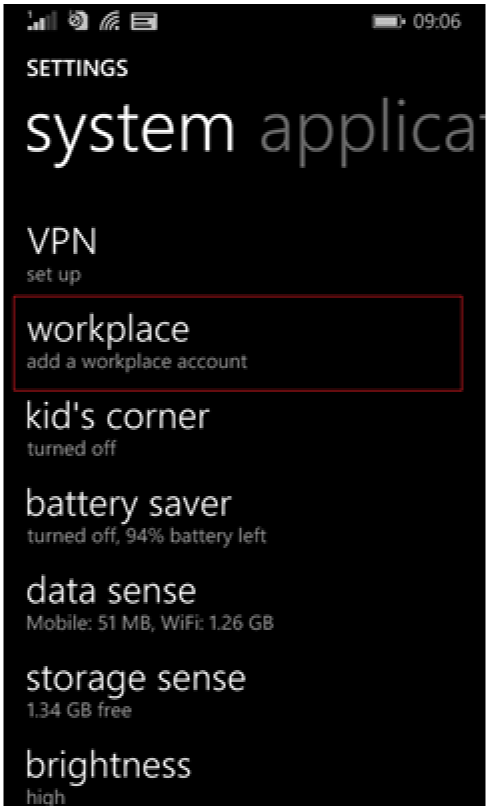
9.4.2.2 Administrator Initiated Enrollment

For administrator initiated enrollment,

1. Click on the link provided to you in the email by the server administrator. Internet Explorer will open.
2. Enter your user name and password. Enrollment page with instructions appears. Follow the instructions and configure your workplace account.

3. Copy the server link and navigate to your phone's settings screen.

4. Tap the **Settings** icon to open Settings screen on the device.



SETTINGS

system applica

VPN
set up

workplace
add a workplace account

kid's corner
turned off

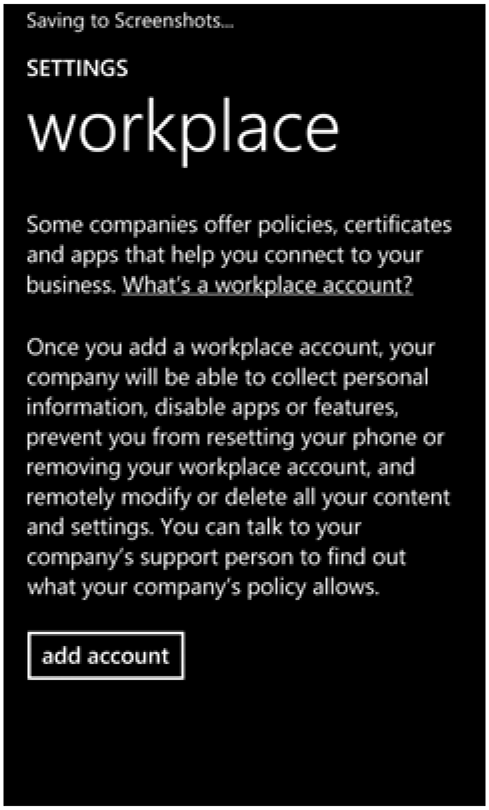
battery saver
turned off, 94% battery left

data sense
Mobile: 51 MB, WiFi: 1.26 GB

storage sense
1.34 GB free

brightness
high

5. Tap the **Workplace** link to open company apps screen.



Saving to Screenshots...

SETTINGS

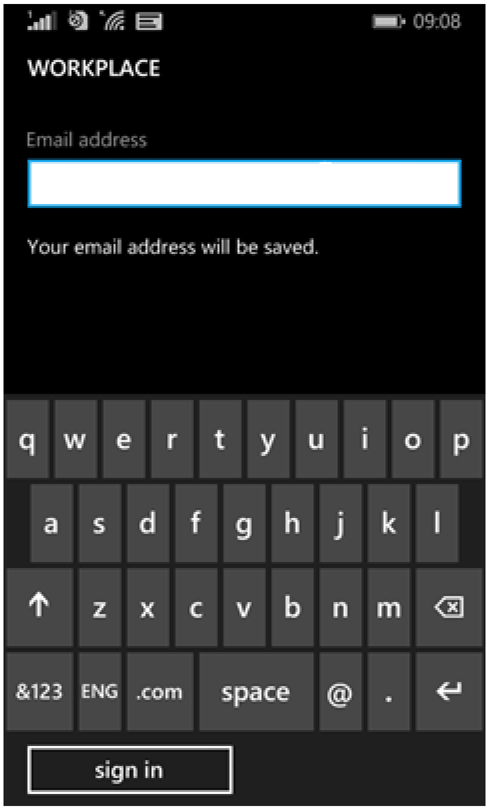
workplace

Some companies offer policies, certificates and apps that help you connect to your business. What's a workplace account?

Once you add a workplace account, your company will be able to collect personal information, disable apps or features, prevent you from resetting your phone or removing your workplace account, and remotely modify or delete all your content and settings. You can talk to your company's support person to find out what your company's policy allows.

6. Tap **add account** to continue.

> *Important:* For Nokia Windows Phone 8.x device enrollments, Nokia account registration is a pre-requisite.

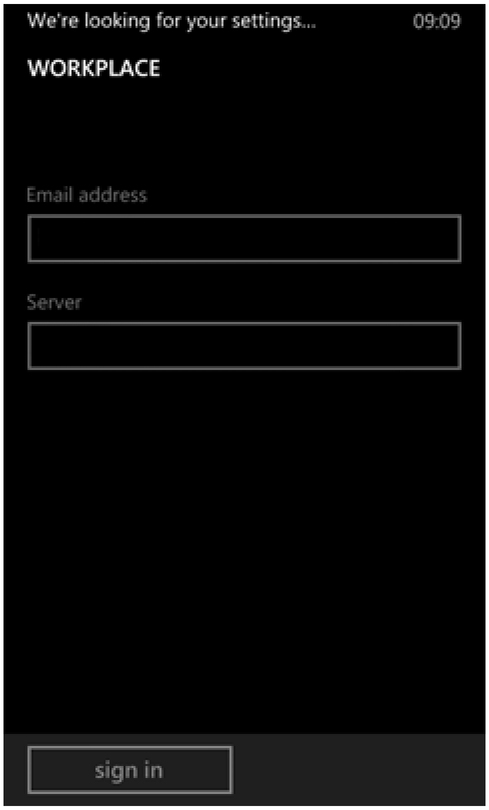


7. Enter your credentials in the following fields:

    a. **Email Address**: Enter your email address.

    b. **Server**: Enter your server details with endpoint. Contact your administrator for details if you don’t have them.

8. Tap **Sign in** to continue.



We're looking for your settings... 09:09

WORKPLACE

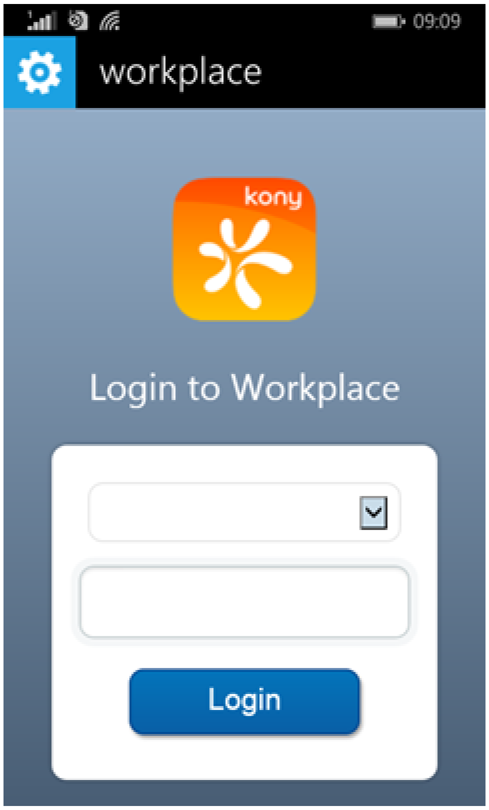
Email address

Server

9. Enter details in the following fields:

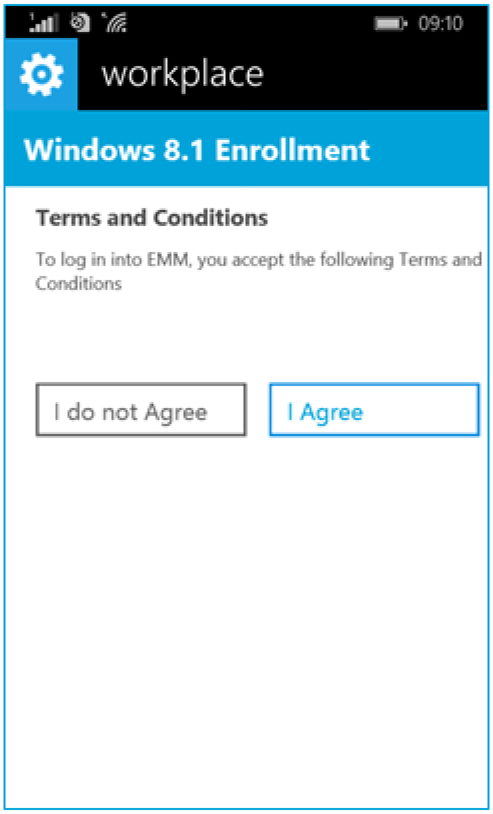
   a. **Username**: Enter your User name.

   b. **Password**: Enter your password.



10. Tap **Login** to continue.

11. System displays Terms and Conditions. Tap **I Agree**.

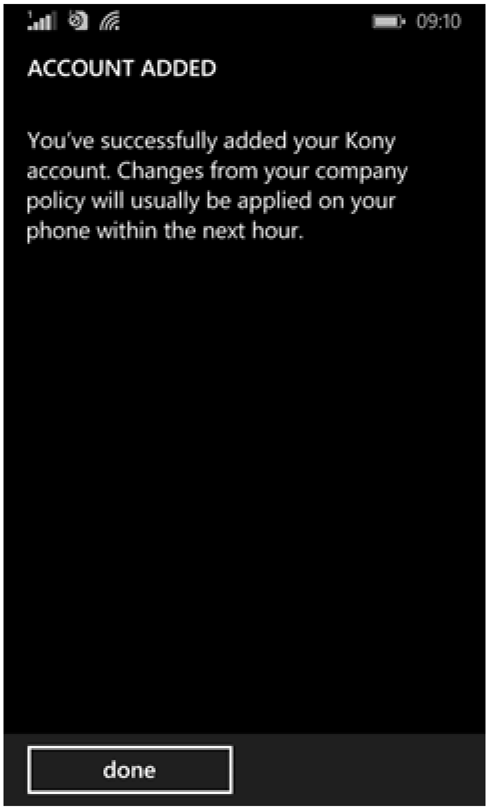


Windows 8.1 Enrollment

Terms and Conditions

To log in into EMM, you accept the following Terms and Conditions

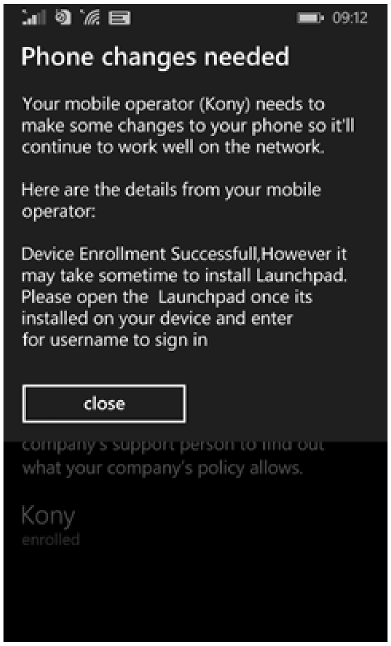
12. **Account Added** message is displayed. Tap **done**.



ACCOUNT ADDED

You've successfully added your Kony account. Changes from your company policy will usually be applied on your phone within the next hour.

13. Phone changes needed page appears. Tap **close**.



09:12

Phone changes needed

Your mobile operator (Kony) needs to make some changes to your phone so it'll continue to work well on the network.

Here are the details from your mobile operator:

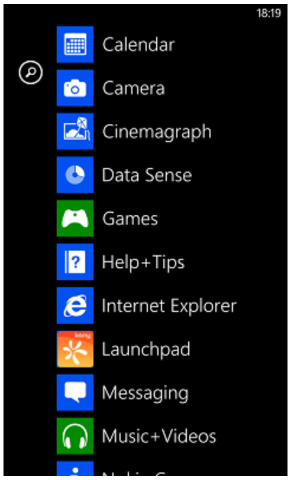
Device Enrollment Successfull,However it may take sometime to install Launchpad. Please open the Launchpad once its installed on your device and enter for username to sign in

close
company's support person to find out what your company's policy allows.
Kony
enrolled

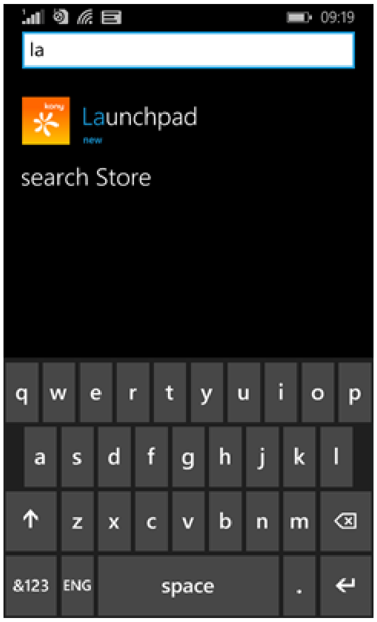
14. Device screen displays all the available icons.

> ***Important:*** If you have not provided a Symantec Enterprise App Signing Certificate for Windows Phone 8.x, after enrollment, enterprise store will not install on the device. Device location, Geo-fence, Time-fence, and Enterprise application management features will not work for the device in the management console. Once the Symantec certificate is provided, from the next ping session, device will get enterprise store and after logging in to the enterprise store, all services (Device location, Geo-fence, Time-fence, and Enterprise application management) will work.

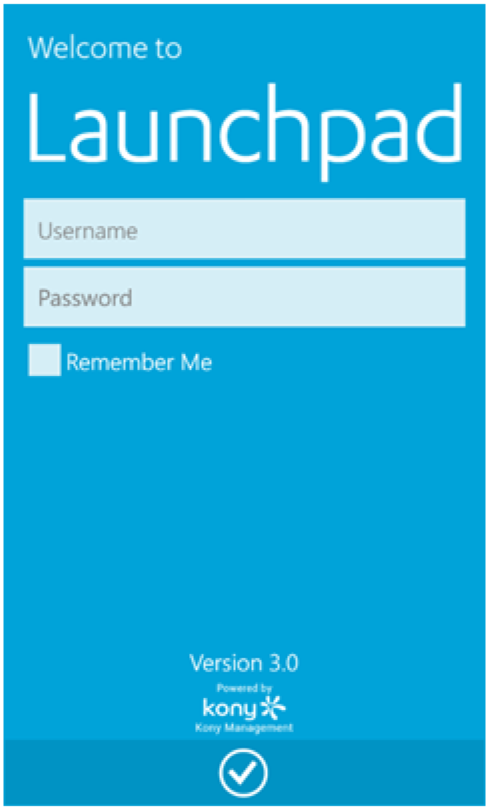
> ***Note:*** Once the enrollment is complete, device will sync with your EMM server. Do not tap the delete button while the device is syncing. If you tap delete, even though the account is deleted on the device, EMM server will continue to consider the device as enrolled and will display its details.



Search for enterprise store and open it.

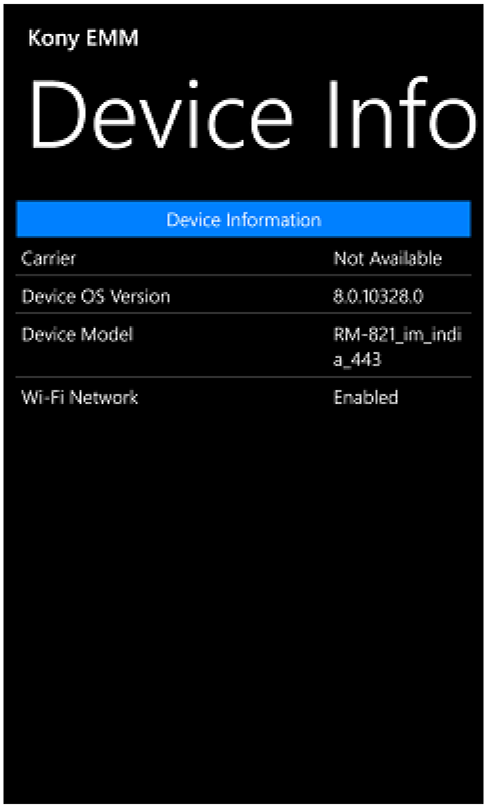


15. enterprise store opens. Enter your user credentials and then click login icon.



Your device is now enrolled.

16. System validates entered credentials.



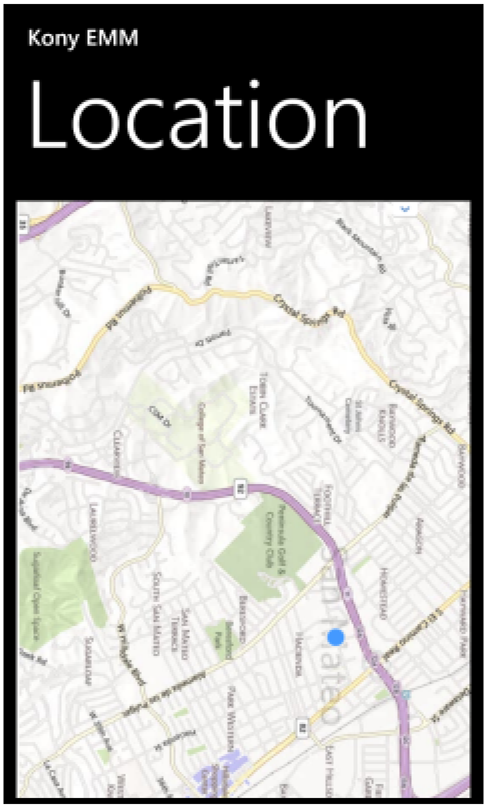
Kony EMM

Device Info

Device Information	
Carrier	Not Available
Device OS Version	8.0.10328.0
Device Model	RM-821_im_india_443
Wi-Fi Network	Enabled

The Device Info page displays the complete information of the device. The page displays the following details:

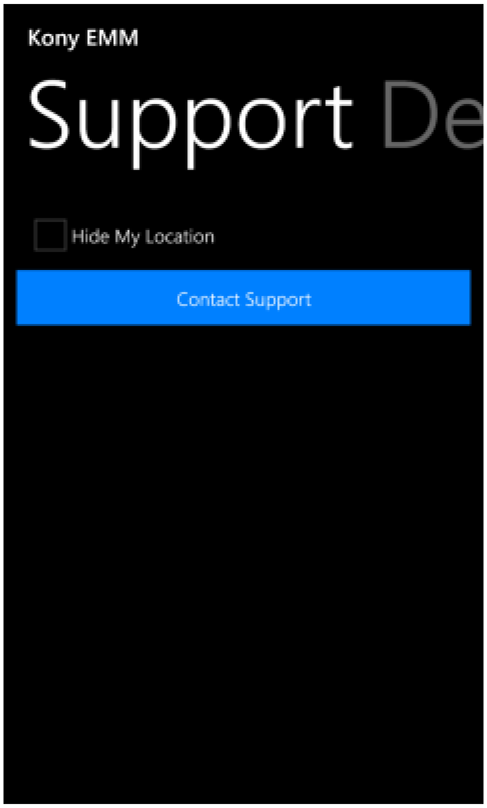
- **Carrier** (Service Provider with which the device currently works.)
- **Device OS Version** (Current device OS version)
- **Device Model**
- **WiFi Network** (it only defines if the WiFi is enabled or not)



Kony EMM

Location

17. Tap the Menu button to navigate to the **Location** screen. This screen displays location details on a map. You can use the zoom tool to change the size of the visible area.



18. Tap the Menu button to navigate to the **Support** screen. When a user wants to get support through the device agent, communication is enabled only through email option.

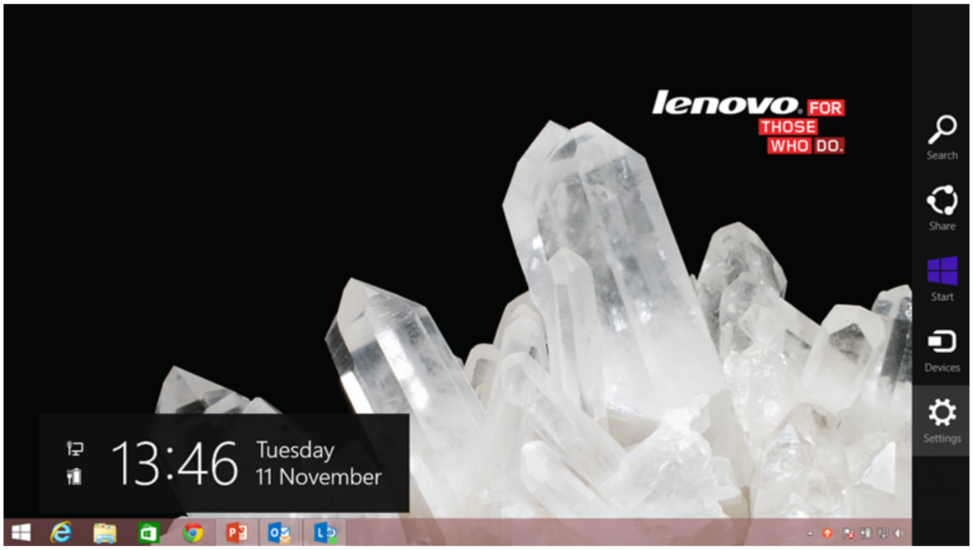
> ***Note:*** During the enrollment process, if your Server SSL certificate is not trusted by the device or if the device date and time are incorrect, a jargon alert will appear.

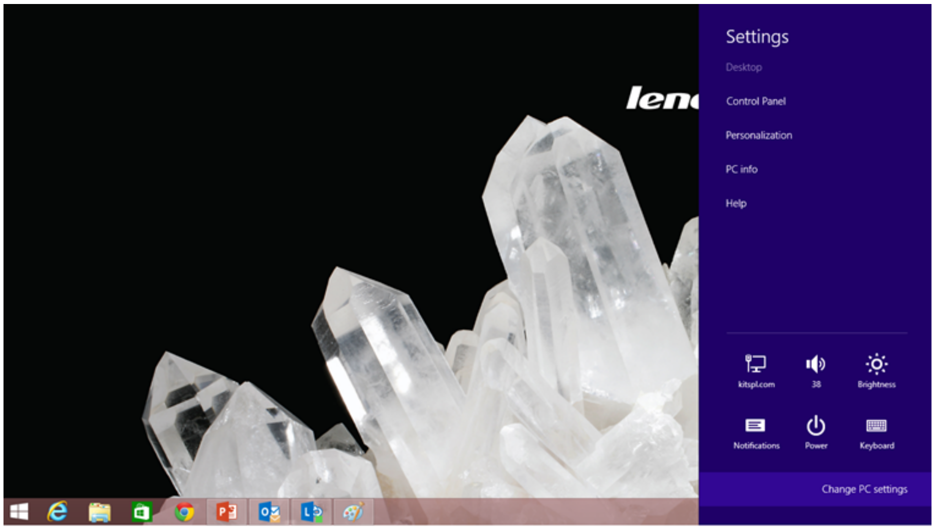
9.4.3 Enroll Windows 8.1 Devices

Windows 8.1 devices that are part of the enterprise domain are not supported.

To enroll Windows 8.1 devices, follow these steps:

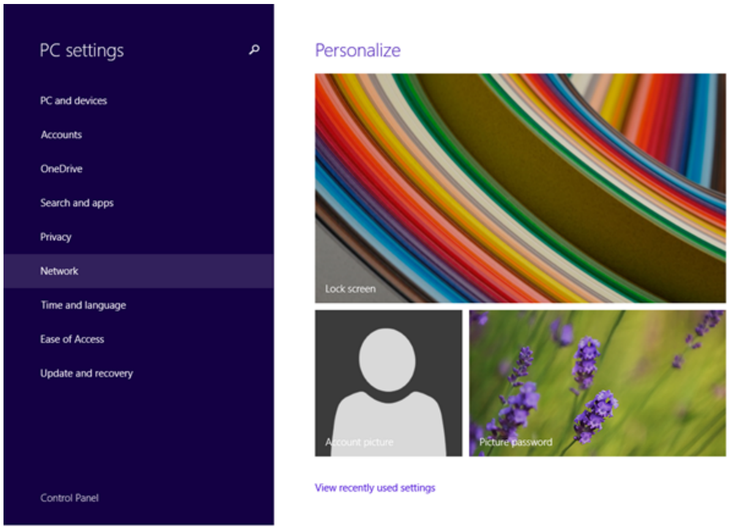
1. Navigate to the **Settings** page on your Windows 8.1 device. The Settings page appears.



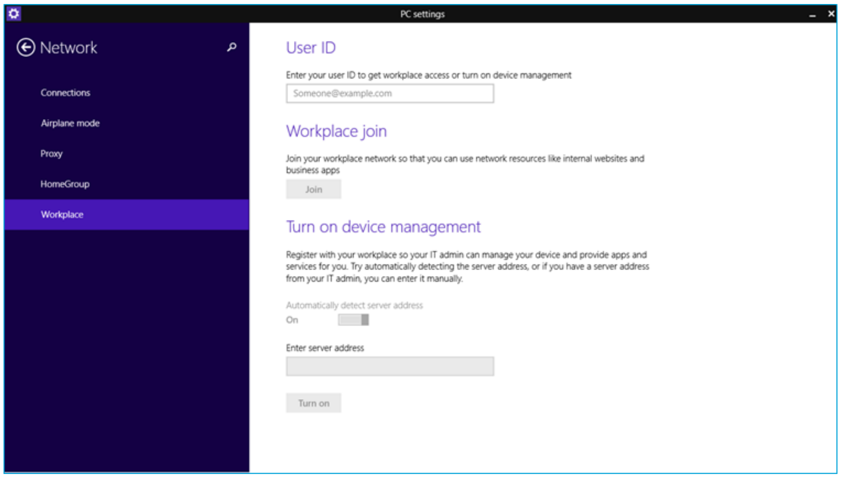


2. Click **Change PC Settings**. The PC Settings page appears.

3. Click **Network**. The Network page details appear.



4. Click **Workplace**. The Workplace details appear.



Enter your user ID to get workplace access or turn on device management

Someone@example.com

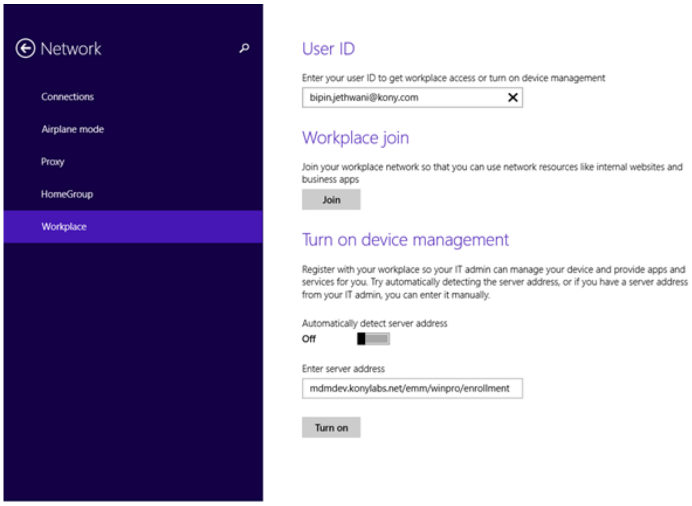
Join your workplace network so that you can use network resources like internal websites and business apps

Register with your workplace so your IT admin can manage your device and provide apps and services for you. Try automatically detecting the server address, or if you have a server address from your IT admin, you can enter it manually.

Automatically detect server address
On

Enter server address

5. Enter **User ID**.



User ID

Enter your user ID to get workplace access or turn on device management

bipin.jethwani@kony.com

Workplace join

Join your workplace network so that you can use network resources like internal websites and business apps

Turn on device management

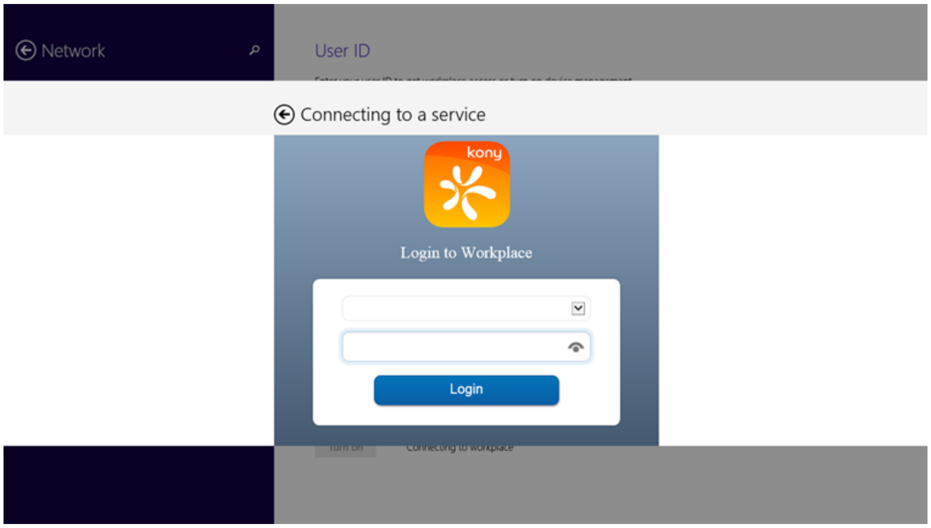
Register with your workplace so your IT admin can manage your device and provide apps and services for you. Try automatically detecting the server address, or if you have a server address from your IT admin, you can enter it manually.

Automatically detect server address
Off

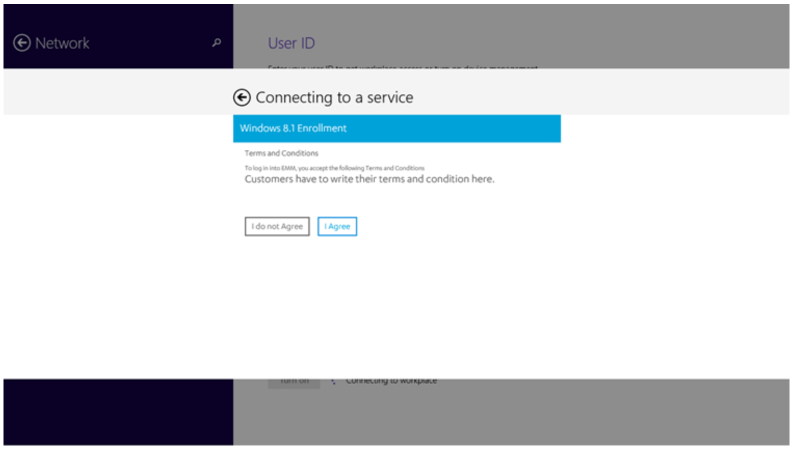
Enter server address
mdmdev.konylabs.net/emm/winpro/enrollment

> ***Important:*** The server name is your server URL, device name, and your enrollment endpoint. For example, *yourcompany.com/winpro/enrollment*

6. Click **Join**. The Connecting to a service page appears.



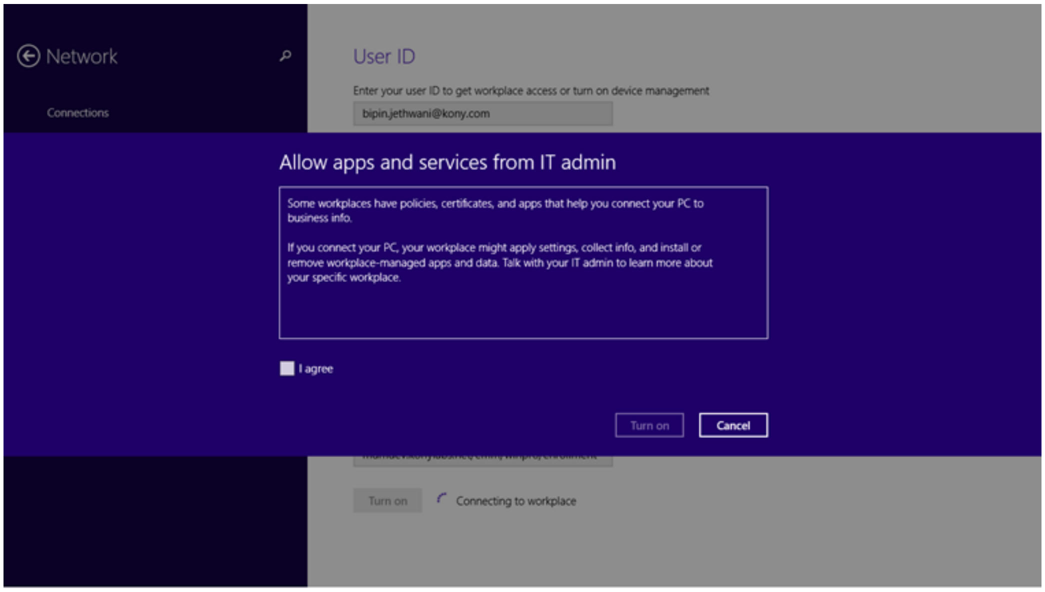
7. Enter user name and password, and then click **Login**. The Terms and Conditions page appears.



To log in into EMM, you accept the following Terms and Conditions

Customers have to write their terms and condition here.

8. Click **I Agree**. The Allow apps and services from IT admin page appears.



Enter your user ID to get workplace access or turn on device management

bipin.jethwani@kony.com

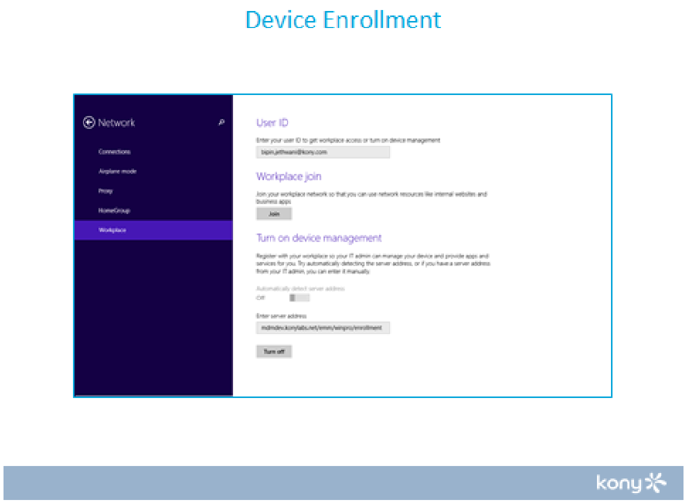
Allow apps and services from IT admin

Some workplaces have policies, certificates, and apps that help you connect your PC to business info.

If you connect your PC, your workplace might apply settings, collect info, and install or remove workplace-managed apps and data. Talk with your IT admin to learn more about your specific workplace.

□ I agree

9. Select **I agree**, and then click **Turn On**. The Workplace details page appears. The **Turn Off** button activates.



Device Enrollment

User ID

Enter your user ID to get workplace access or turn on device management

bipin.jethwani@kony.com

Workplace join

Join your workplace network so that you can use network resources like internal websites and business apps

Turn on device management

Register with your workplace so your IT admin can manage your device and provide apps and services for you. Try automatically detecting the server address, or if you have a server address from your IT admin, you can enter it manually.

Automatically detect server address: Off

Enter server address: mdmdev.konylabs.net/emm/winpro/enrollment

Your device is now enrolled.

9.5 Enterprise Store

Kony Management Suite enterprise store is an app that is installed on a device to enroll 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.

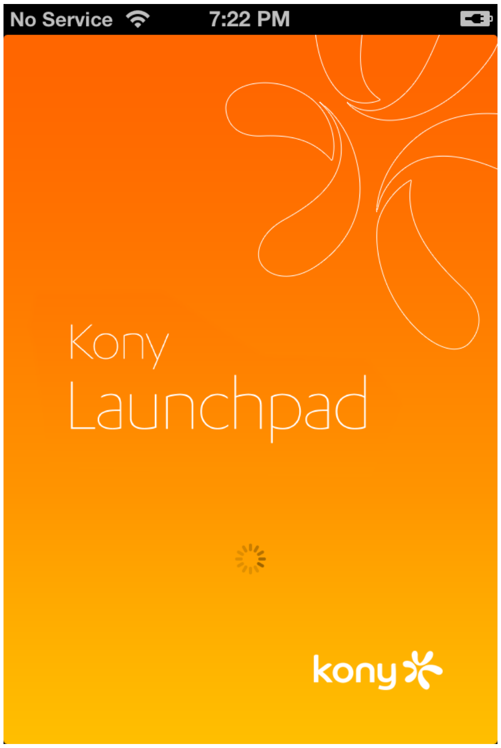
- Resources that require an online connection will no longer be available.
- An app that is not installed on the device will not be available in the apps tab.
- Content that is not downloaded to the device will not appear in the content tab.

- Messages will not be available.
- A banner that enterprise store is offline will appear within the enterprise store.

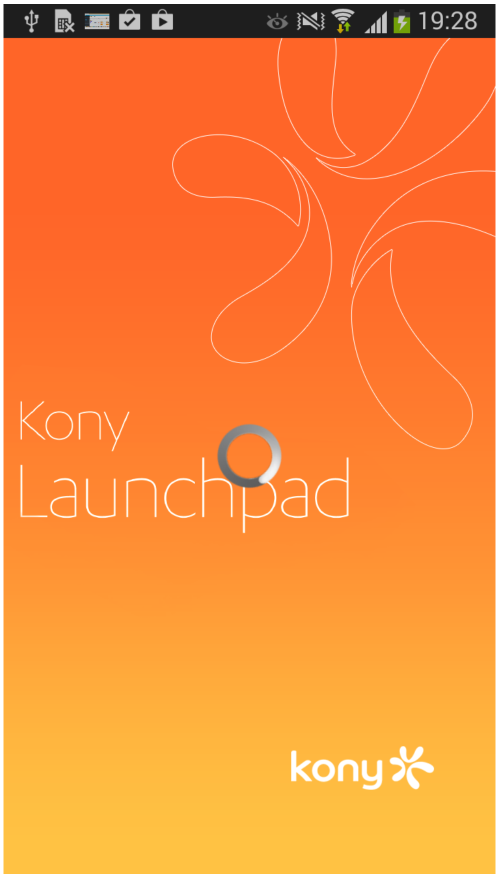
9.5.1 Splash Screen

When the enterprise store App is launched, a splash screen is shown to the user.

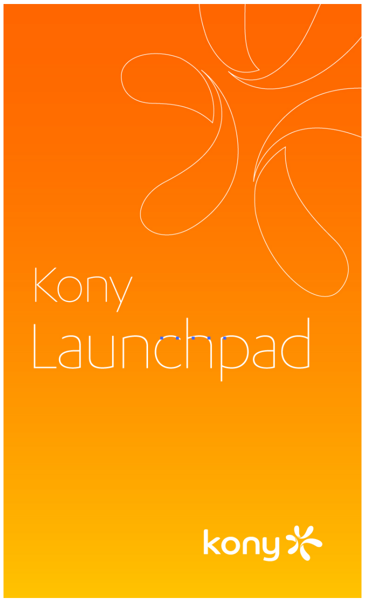
9.5.1.1 iOS



9.5.1.2 Android



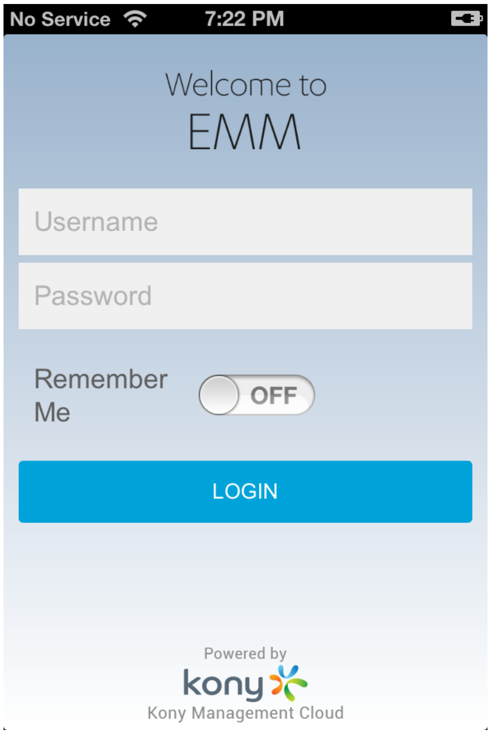
9.5.1.3 Windows Phone 8.X



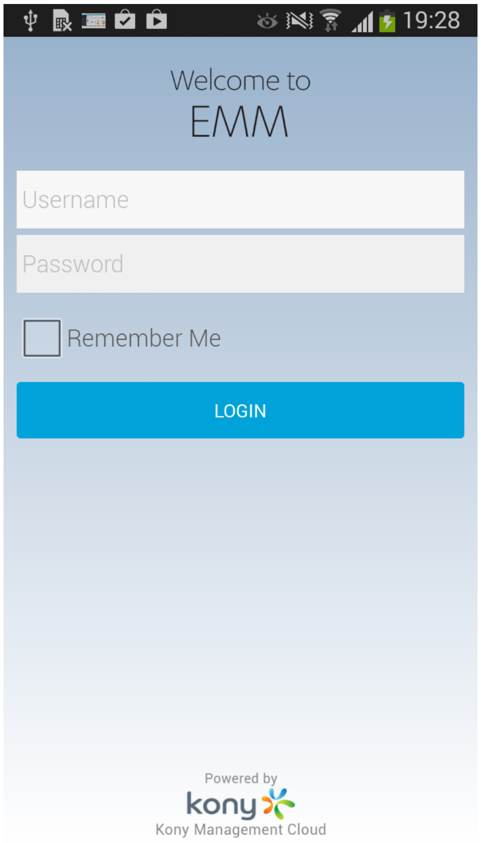
9.5.2 Log-in Screen

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.

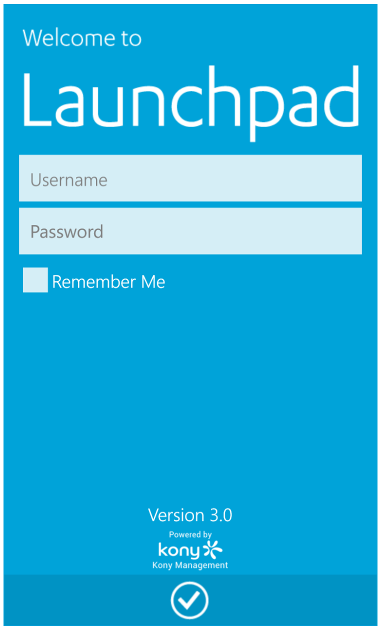
9.5.2.1 iOS


No Service
7:22 PM
Welcome to
EMM
Username
Password
Remember Me
OFF
LOGIN
Powered by
kony
Kony Management Cloud

9.5.2.2 Android



9.5.2.3 Windows Phone 8.X

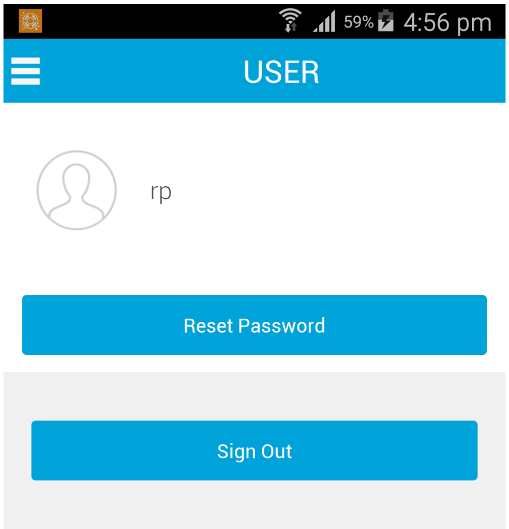


Kony EMM enterprise store has six tabs:

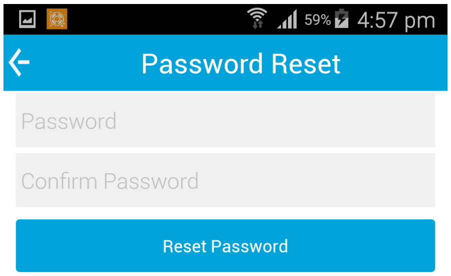
- User
- Store
- Device
- Content
- Messages
- Support

9.5.3 User

Displays the User details. You can sign out from the enterprise store from here.



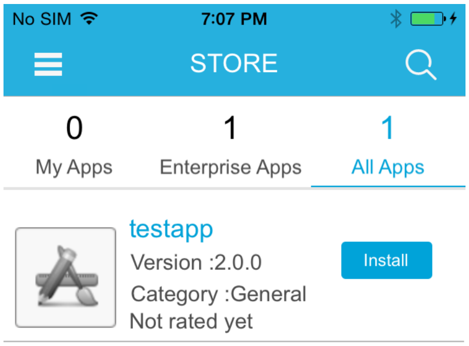
When you click the reset password button, reset page appears.



9.5.4 Store

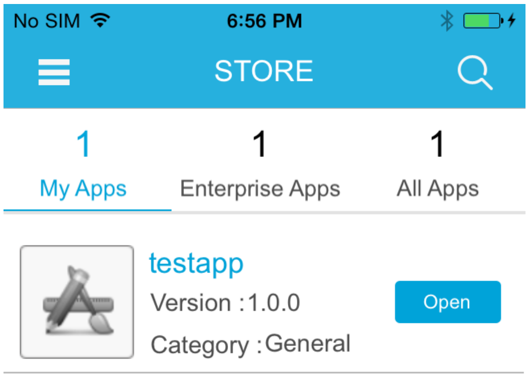
Once an app is published, the administrator pushes that app to the App Store. You can browse enterprise apps from the store, and select the required applications to download and install on your device. Applications that are targeted to a specific group or user are displayed only to them in the store.

Store is not available if the device is offline.



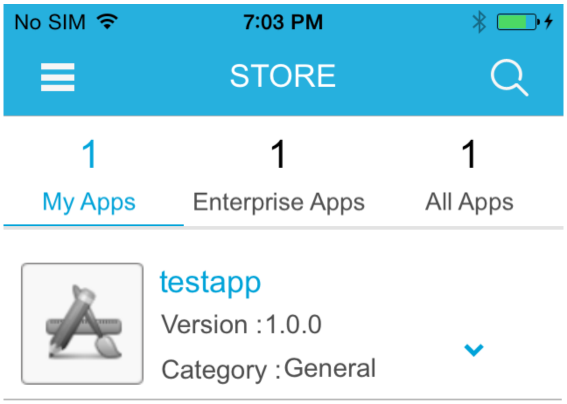
testapp
Version :2.0.0
Category :General
Not rated yet

In All Apps, all targeted apps are available, including wrap and sign, and sign-only apps. A user can choose to install the targetted app.



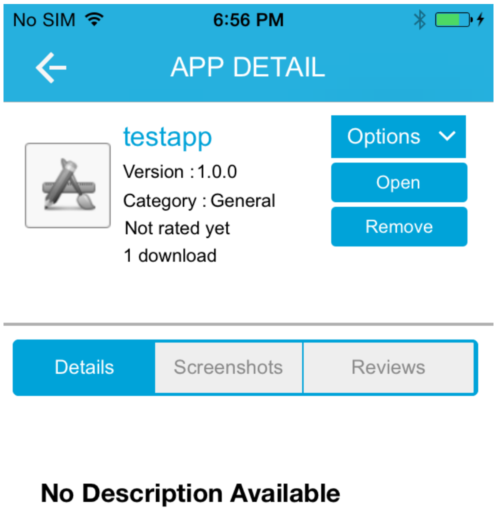
testapp
Version :1.0.0
Category :General

Once an app is installed, it appears in the My Apps page. The administrator can open the My Apps page to use the app.



testapp
Version :1.0.0
Category :General

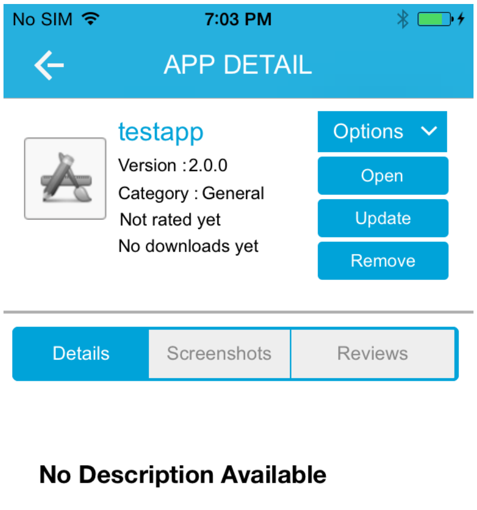
If there is an upgrade for the selected app, the more options **V** button appears. Click the more options button to see the **Open** and **Update** options.



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.



testapp
Version :2.0.0
Category : General
Not rated yet
No downloads yet

No Description Available

If there are updates to an app, the **Update** button appears under Options.

9.5.4.1 My Apps

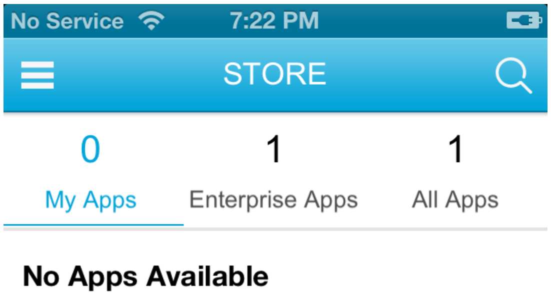
This tab displays all applications that are installed and can be installed on your iOS or Android device. An **Install** button displays for each application. If the application is already installed, then the **Launch** button appears.

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.

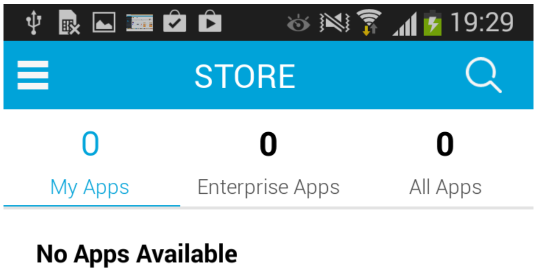
> *Important:* If a device experiences software upgrade issues and location services flip between On and Off, apps may launch. This condition has been seen in the Samsung Galaxy 54.

9.5.4.2 iOS



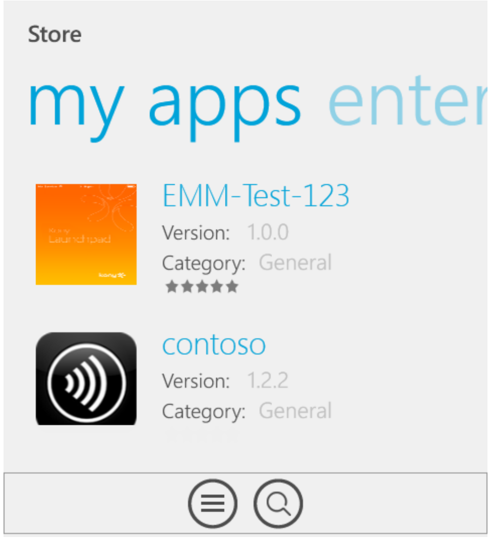
No Apps Available

9.5.4.3 Android



No Apps Available

9.5.4.4 Windows Phone 8X



Store

my apps enter

EMM-Test-123

Version: 1.0.0

Category: General

contoso

Version: 1.2.2

Category: General

9.5.5 Device

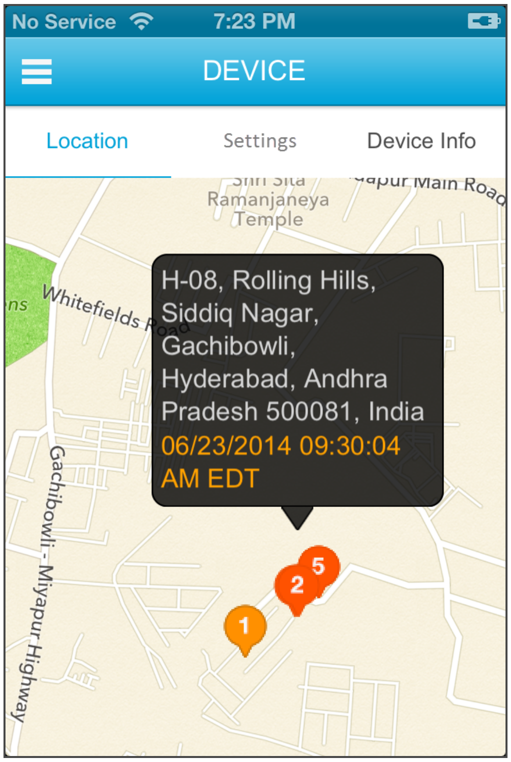
The **Device Management** tab includes three tabs.

- Location
- Settings (Not available for Windows Phone devices)
- Device Info

9.5.5.1 Location

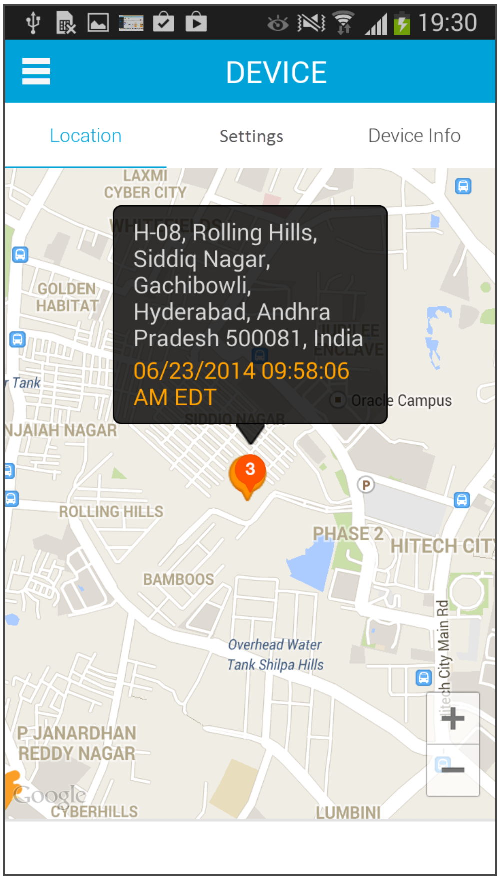
The Location tab displays the current location and the last five location details of the device.

iOS



H-08, Rolling Hills, Siddiq Nagar, Gachibowli, Hyderabad, Andhra Pradesh 500081, India
06/23/2014 09:30:04 AM EDT

Android



19:30

DEVICE

Location Settings Device Info

H-08, Rolling Hills, Siddiq Nagar, Gachibowli, Hyderabad, Andhra Pradesh 500081, India
06/23/2014 09:58:06 AM EDT

Note: In Android tablet, when user clicks the Location tab, intermittently, the system does not display current location details instead it displays time out alert. And once the device is restarted only then the current location is displayed. This is a limitation with Android platform.

Windows Phone 8.x

9.5.5.2 Settings

The settings tab is available for only iOS and Android devices. This feature is not available for Windows Phone devices. The **Settings** tab displays following details:

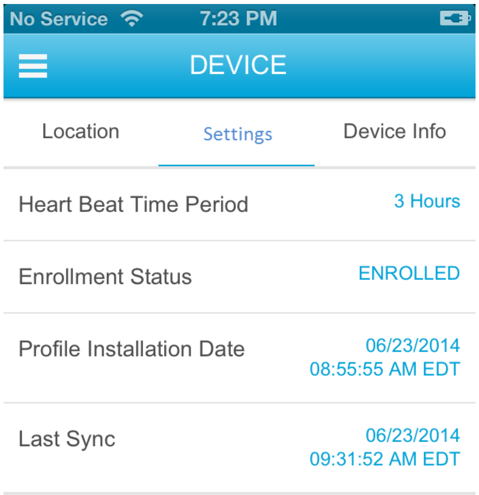
- **Heartbeat Time Period**: Time Period: with which the device communicates with the EMM server.
- **Carrier**: The current Telecom Service Provider.
- **Enrollment Status**: The device status can be Enrolled or not Enrolled with Kony EMM server.
- **Device OS Version**: Version of the current Operating System.
- **Profile Installation Date (Only for iOS)**: The date on which the profile was installed on the device.

- **Compliance Status (only for Android)** : It gives the info regarding the compliance status of the device.
- **Policy ID**: When a policy is pushed on a device. A unique Policy ID is generated to identify that policy.
- **Last Sync** : It displays the last sync information (date and time with time zone of the device).
- **Show Notification**: Show Notification button is used to navigates to notification screen. You receive all the notifications through Kony EMM server in Notification screen.

> *Important:* For iOS devices, EMM enterprise store does not get deleted automatically when the User removes control by deleting the profile. The User is required to delete the Agent if he wishes to enroll again.

> *Note:* Currently Landscape mode is not supported for EMM enterprise store.

iOS



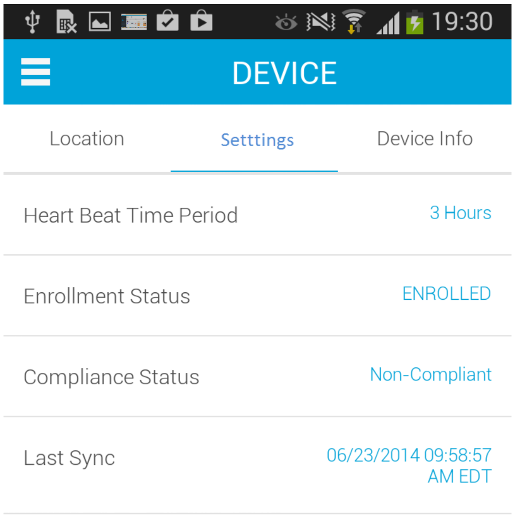
Heart Beat Time Period 3 Hours

Enrollment Status ENROLLED

Profile Installation Date 06/23/2014 08:55:55 AM EDT

Last Sync 06/23/2014 09:31:52 AM EDT

Android



Heart Beat Time Period 3 Hours

Enrollment Status ENROLLED

Compliance Status Non-Compliant

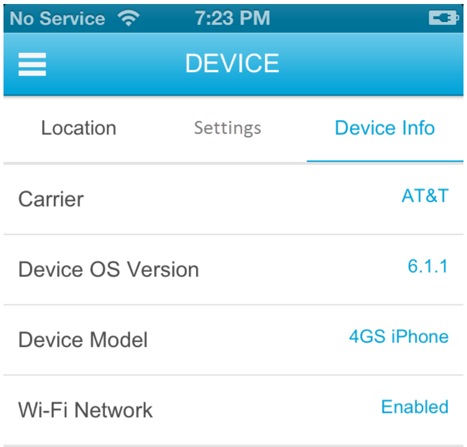
Last Sync 06/23/2014 09:58:57 AM EDT

9.5.5.3 Device Info

The **Device Info** page displays the complete information of the device. The page displays the following details:

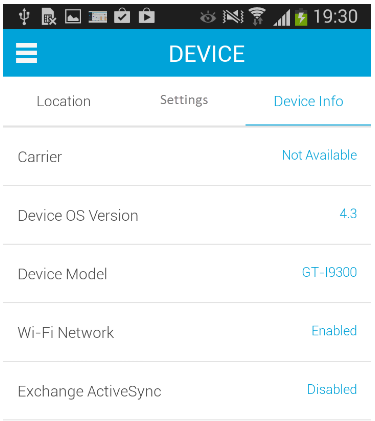
- Carrier (Service Provider with which the device currently works.)
- Device OS Version (Current device OS version)
- Device Model
- WiFi Network (it only defines if the WiFi is enabled or not)
- Exchange ActiveSync

iOS



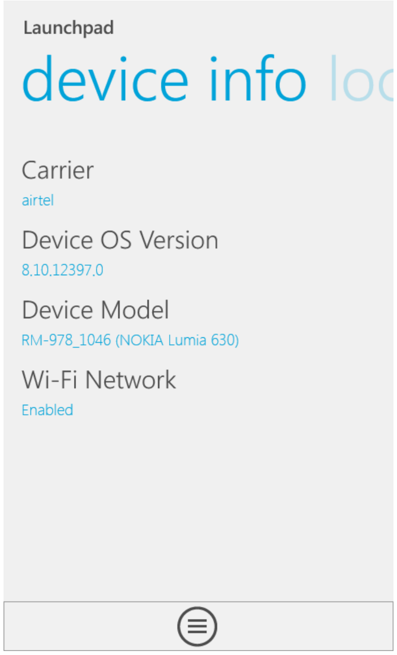
Carrier	AT&T
Device OS Version	6.1.1
Device Model	4GS iPhone
Wi-Fi Network	Enabled

Android



Carrier	Not Available
Device OS Version	4.3
Device Model	GT-I9300
Wi-Fi Network	Enabled
Exchange ActiveSync	Disabled

Windows Phone 8X



Launchpad

device info loc

Carrier
airtel

Device OS Version
8.10.12397.0

Device Model
RM-978_1046 (NOKIA Lumia 630)

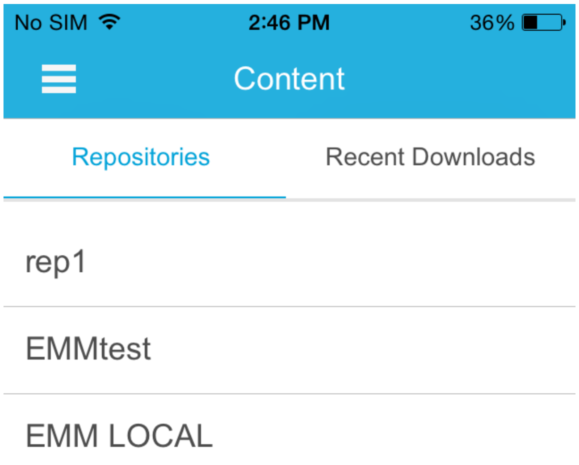
Wi-Fi Network
Enabled

9.5.6 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.



rep1

EMMtest

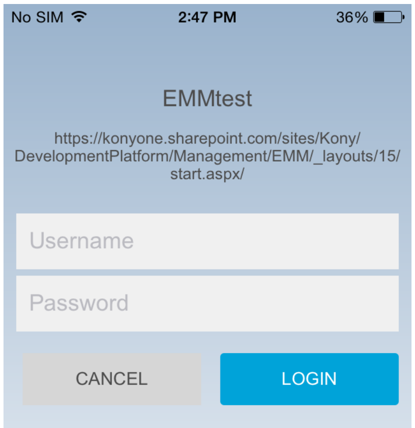
EMM LOCAL

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

9.5.7 SharePoint Repository

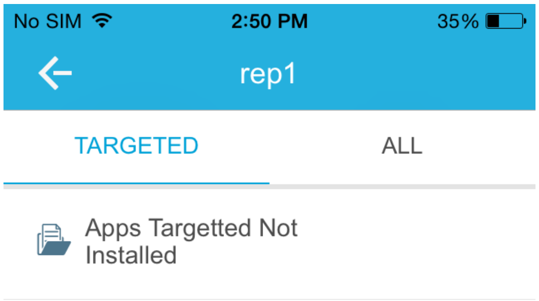
When you click a SharePoint repository the SharePoint login screen appears. To access your SharePoint, enter your SharePoint login credentials. Once you enter your credentials, the Content tab appears.



https://konyone.sharepoint.com/sites/Kony/DevelopmentPlatform/Management/EMM/_layouts/15/start.aspx/

The Content tab for SharePoint repositories displays two tabs.

- **Targeted** : Displays content that is targeted to the user or the group.



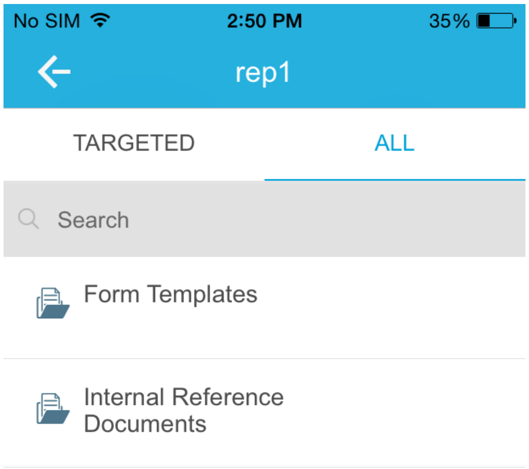
No SIM 2:50 PM 35%

rep1

TARGETED ALL

Apps Targetted Not Installed

- **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.



No SIM 2:50 PM 35%

rep1

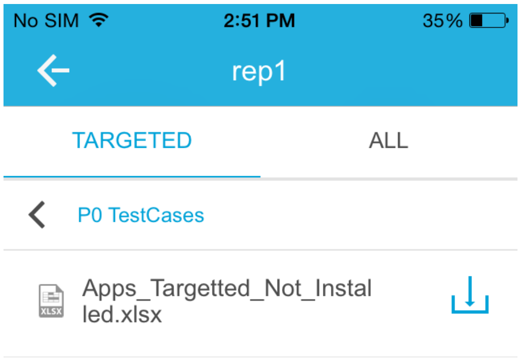
TARGETED ALL

Search

Form Templates

Internal Reference Documents

You can download any file that is available to you by tapping on the download button.



No SIM 2:51 PM 35%

rep1

TARGETED ALL

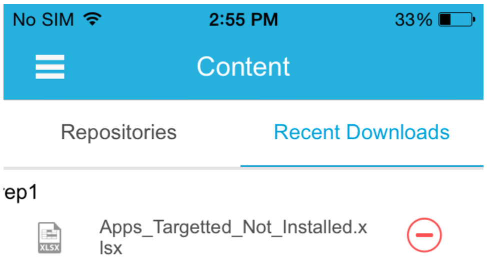
P0 TestCases

Apps_Targetted_Not_Installed.xlsx

When you download a file, an alert appears notifying you that you can now access the file offline on the device.

9.5.8 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.



9.5.9 Local Repository

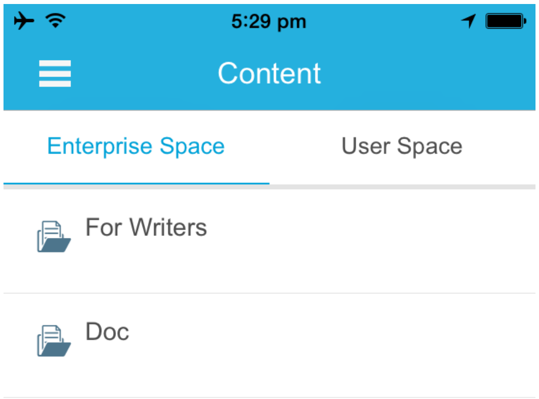
The content tab for a local repository displays two tabs:

Enterprise Space: Displays the content shared with a user by the enterprise and other users. Content is available only for iOS and Android devices.

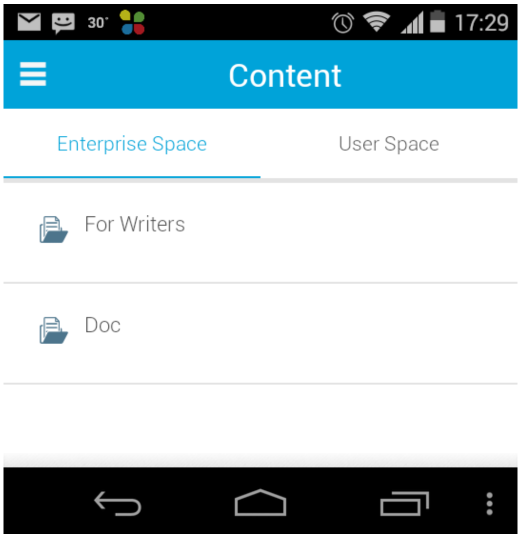
User Space: Displays content uploaded by a user to a self-service console.

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**.

9.5.9.1 iOS



9.5.9.2 Android

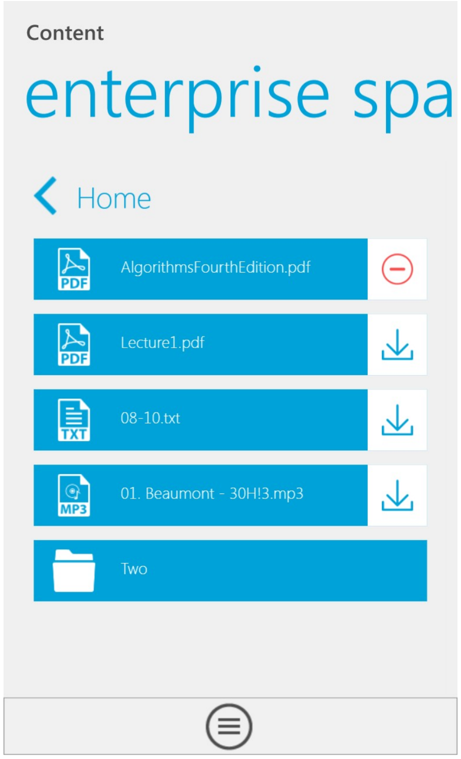


When a user downloads a document, on Android devices, the document is downloaded to the device. For iOS devices, the file is downloaded within the enterprise store and is available for a user even when the device is offline.

9.5.9.3 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 looses 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.

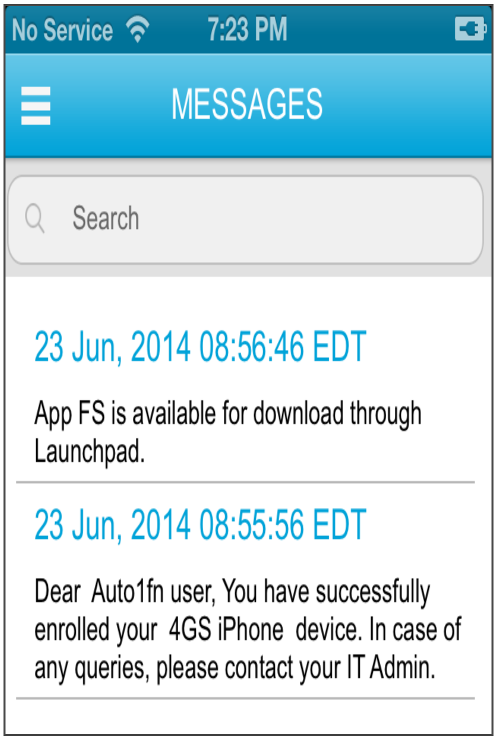


9.5.10 Messages

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.

9.5.10.1 iOS



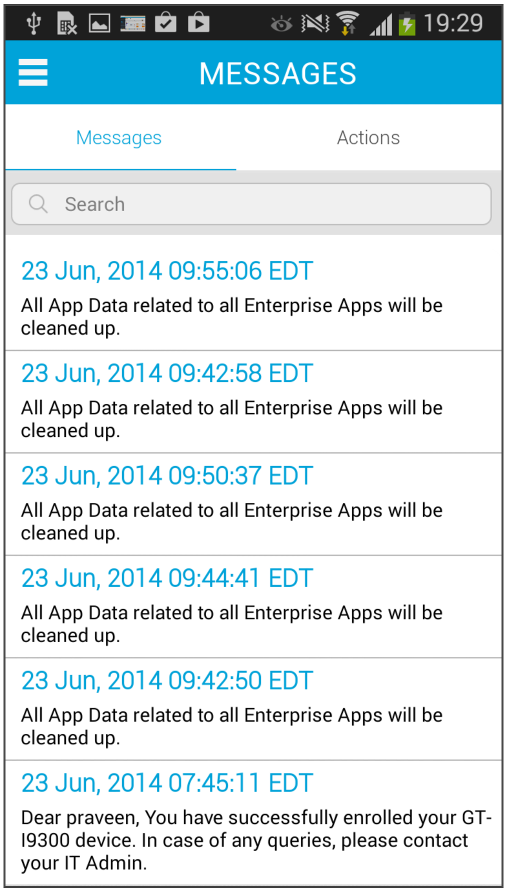
23 Jun, 2014 08:56:46 EDT

App FS is available for download through Launchpad.

23 Jun, 2014 08:55:56 EDT

Dear Auto1fn user, You have successfully enrolled your 4GS iPhone device. In case of any queries, please contact your IT Admin.

9.5.10.2 Android



23 Jun, 2014 09:55:06 EDT
All App Data related to all Enterprise Apps will be cleaned up.

23 Jun, 2014 09:42:58 EDT
All App Data related to all Enterprise Apps will be cleaned up.

23 Jun, 2014 09:50:37 EDT
All App Data related to all Enterprise Apps will be cleaned up.

23 Jun, 2014 09:44:41 EDT
All App Data related to all Enterprise Apps will be cleaned up.

23 Jun, 2014 09:42:50 EDT
All App Data related to all Enterprise Apps will be cleaned up.

23 Jun, 2014 07:45:11 EDT
Dear praveen, You have successfully enrolled your GT-I9300 device. In case of any queries, please contact your IT Admin.

On enterprise store for Android, the Messages section has two tabs:

- **Notifications -** All regular push messages are shown in Notifications tab.
- **Pending Actions -** Only pending actions are shown in the Pending Actions tab.

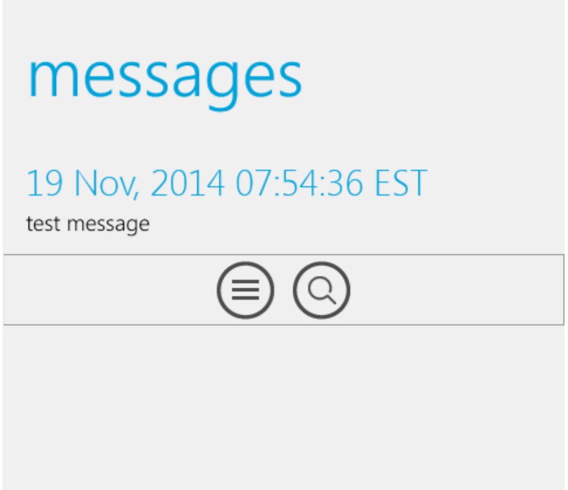
For Android, in order to apply policies, a user must perform some actions. These are captured in the pending actions list.

Following policies require user action to be completed:

- Password Policy
- Email Configuration with Touchdown

- Apps Policy (Required Apps)
- Device Encryption
- SAFE License

9.5.10.3 Windows Phone 8X



messages

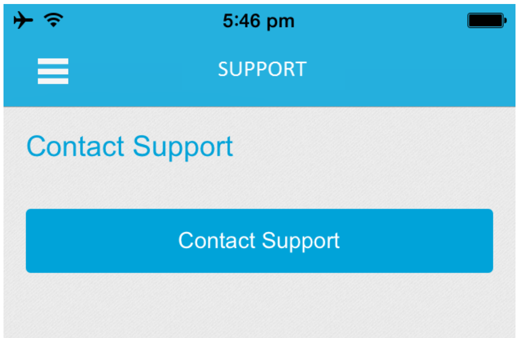
19 Nov, 2014 07:54:36 EST

test message

9.5.11 Support

Support page is available for iOS, Android, and Windows 8.1 devices.

Contact Support : To resolve any device related issue, you can contact Administrator through the Contact Support button.



9.5.12 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 enrolled, 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 to 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-enroll into EMM.

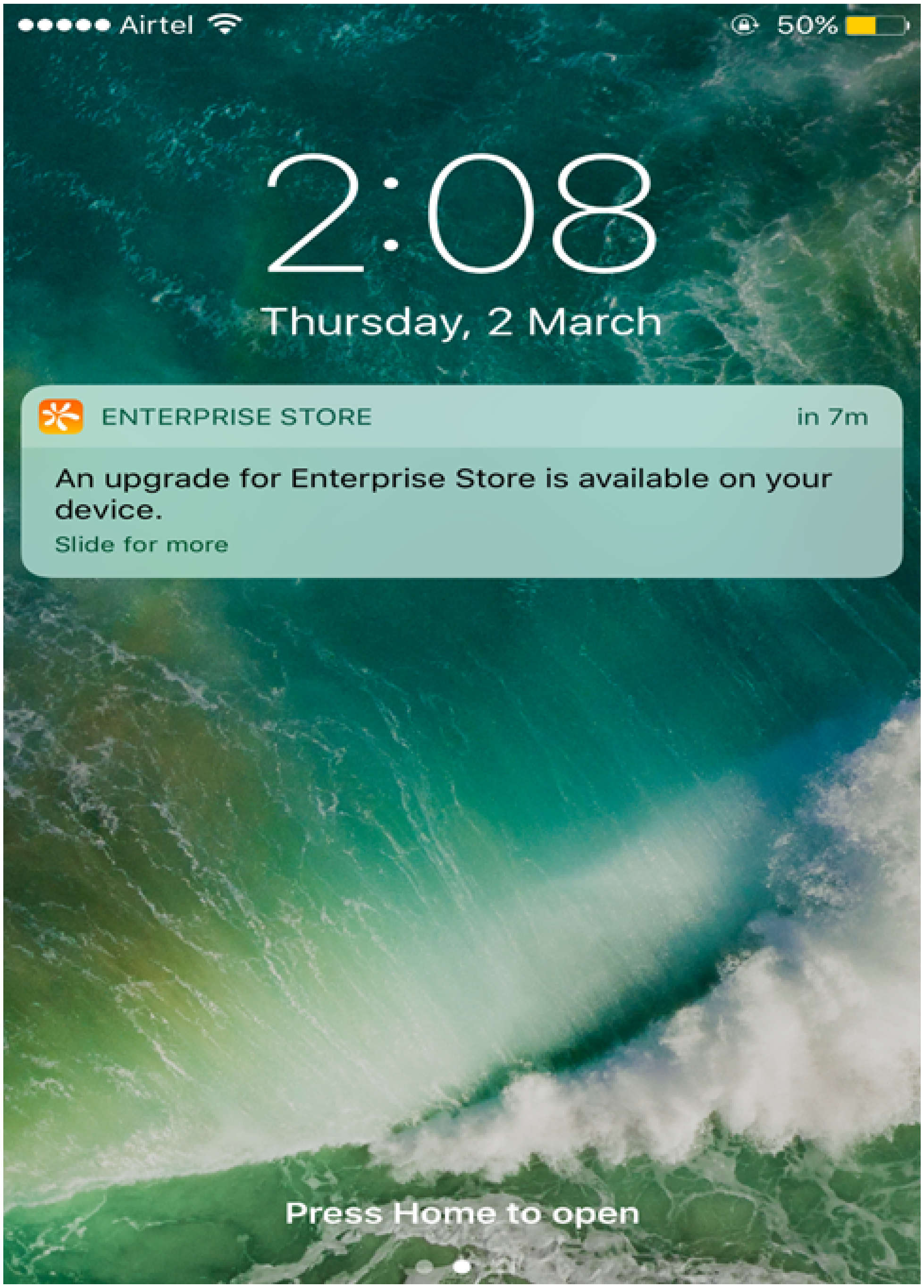
> ***Note:*** In case of Windows 8X devices, if enterprise store is deleted, but the device is still enrolled in EMM, enterprise store will be installed silently on next heartbeat.

9.5.13 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.

9.5.13.1 Upgrade Enterprise Store in iOS

When you have an update available for your enterprise store in iOS, you will receive a push message.

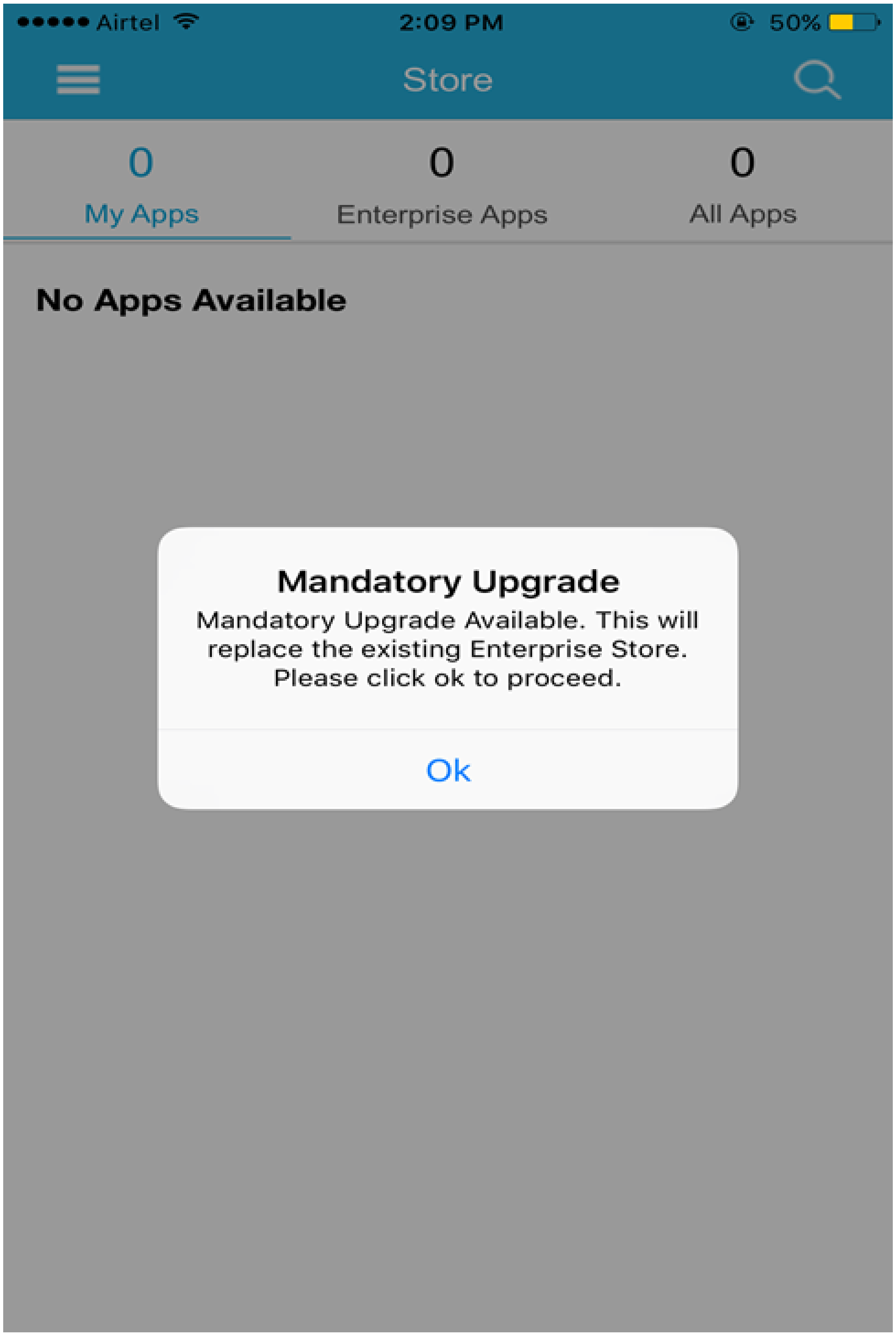


ENTERPRISE STORE in 7m

An upgrade for Enterprise Store is available on your device.

Slide for more

Once you log in to the device, a mandatory upgrade message appears.

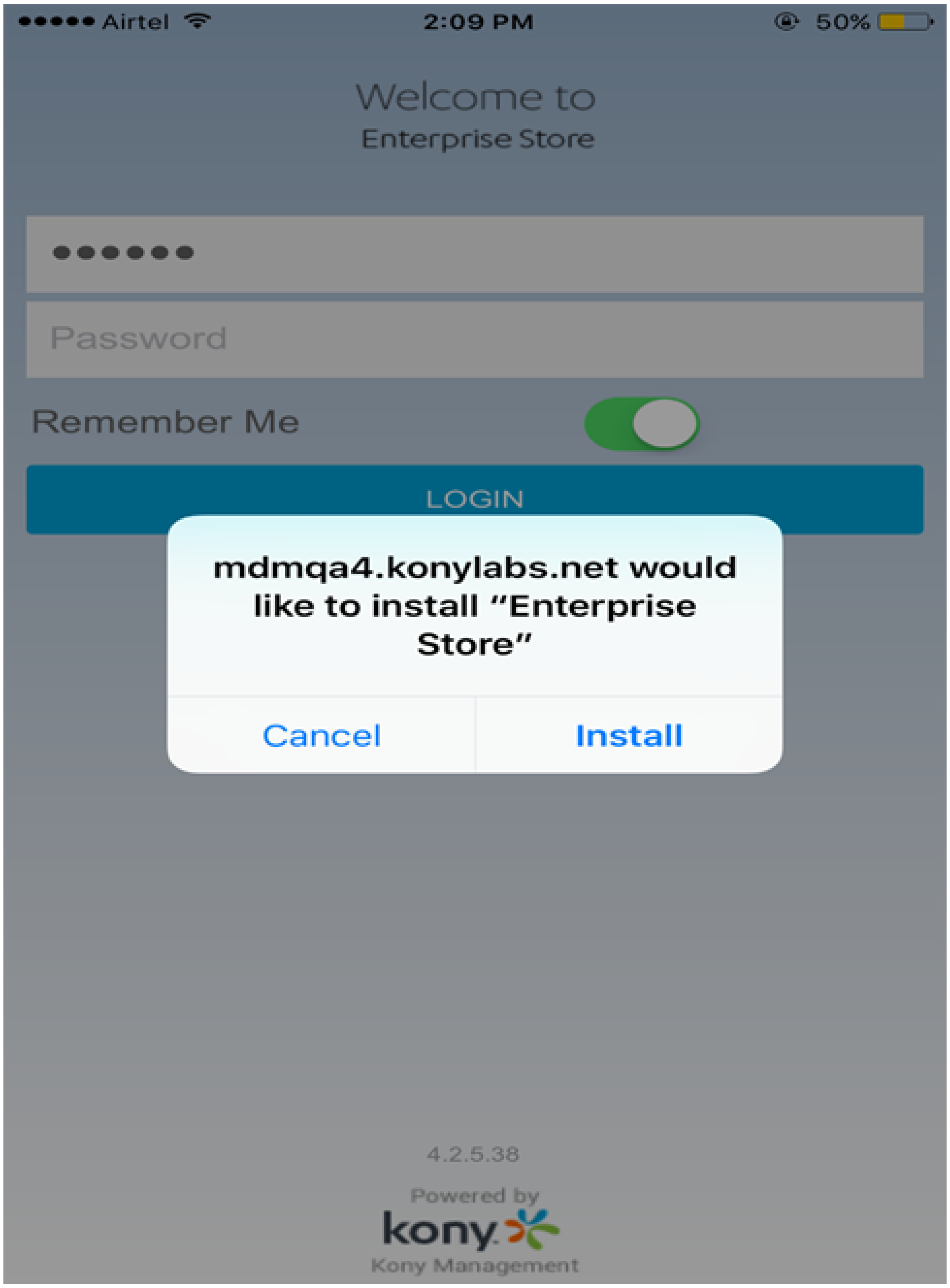


No Apps Available

Mandatory Upgrade

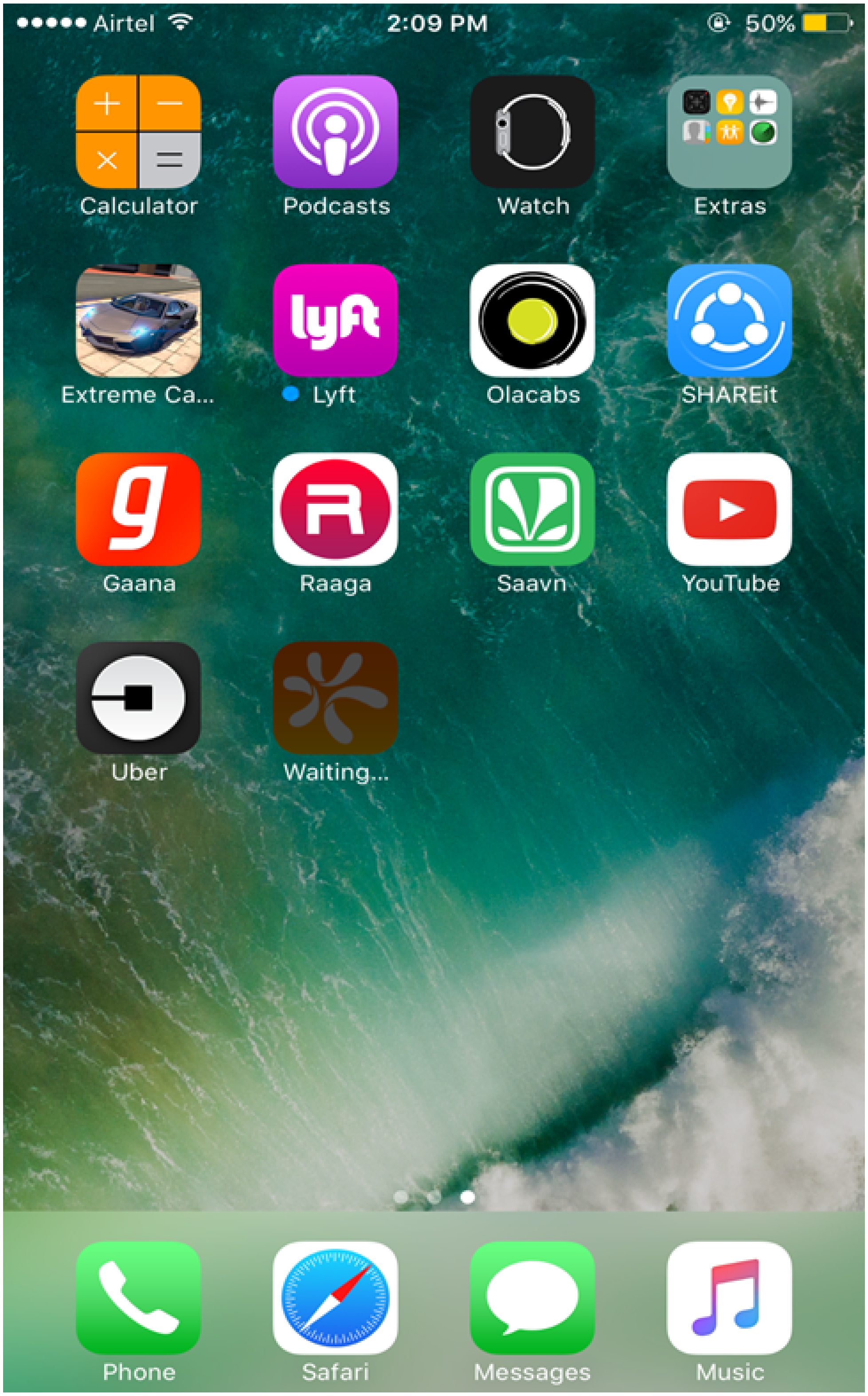
Mandatory Upgrade Available. This will replace the existing Enterprise Store. Please click ok to proceed.

Once you click **Ok**, an Install message appears.



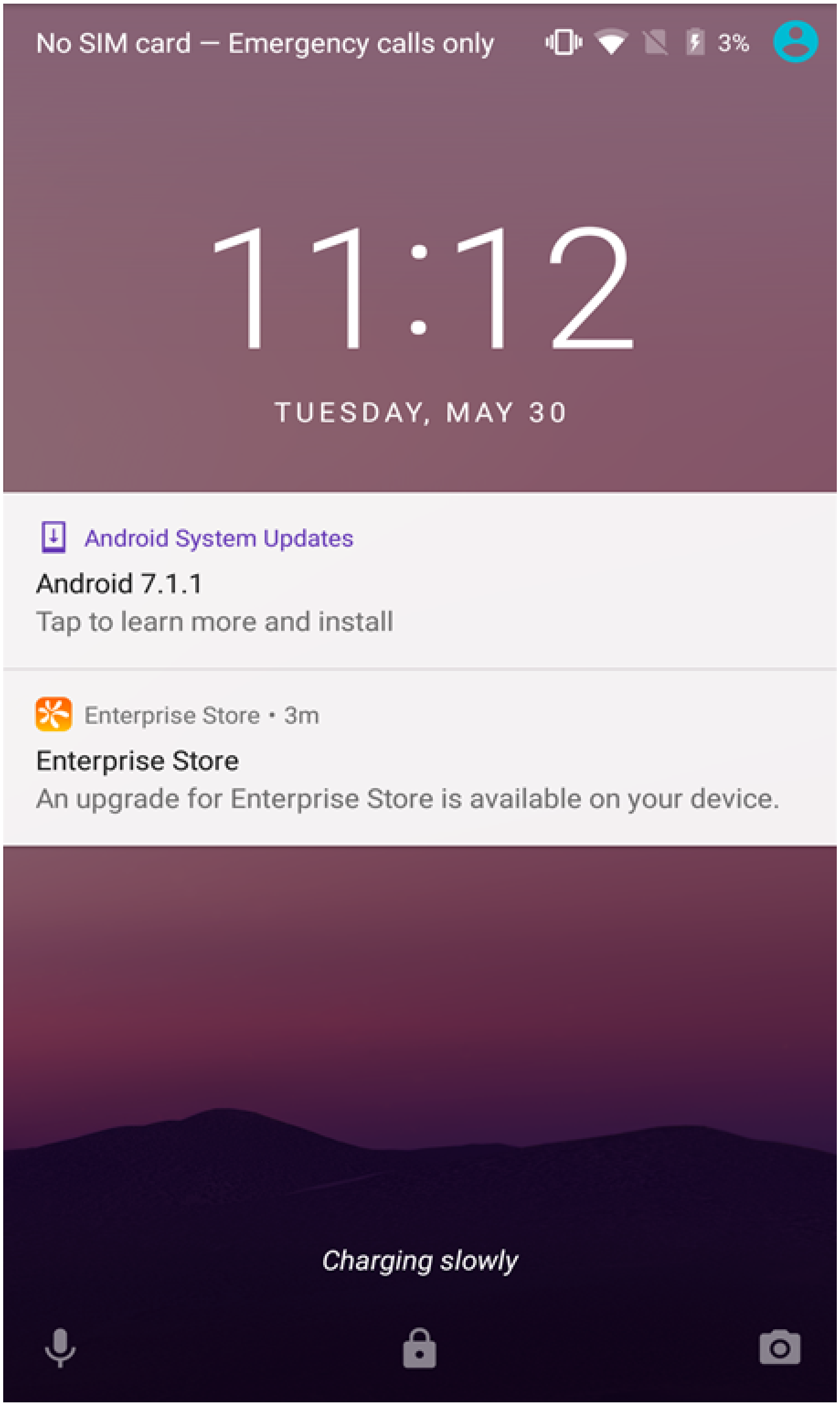
mdmqa4.konylabs.net would like to install "Enterprise Store"

Click **Install**. Screen goes back to the home page and the enterprise store is installed.


●●●●● Airtel
2:09 PM
50%
Calculator
Podcasts
Watch
Extras
Extreme Ca...
Lyft
Olacabs
SHAREit
Gaana
Raaga
Saavn
YouTube
Uber
Waiting...
Phone
Safari
Messages
Music

9.5.13.2 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.



No SIM card — Emergency calls only

3%

11:12

TUESDAY, MAY 30

Android System Updates

Android 7.1.1

Tap to learn more and install

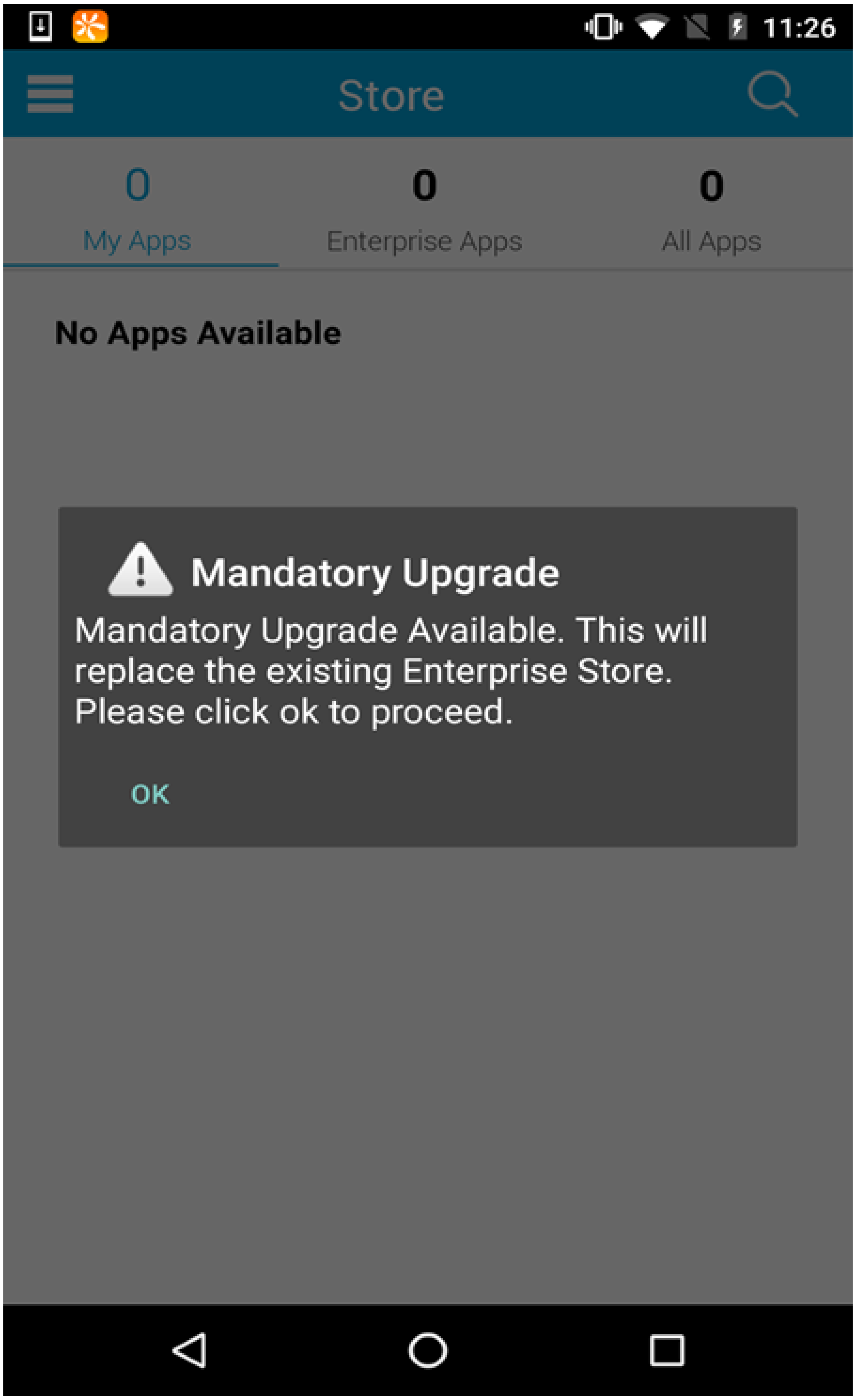
Enterprise Store • 3m

Enterprise Store

An upgrade for Enterprise Store is available on your device.

Charging slowly

Once you log in to the device, a mandatory upgrade message appears.

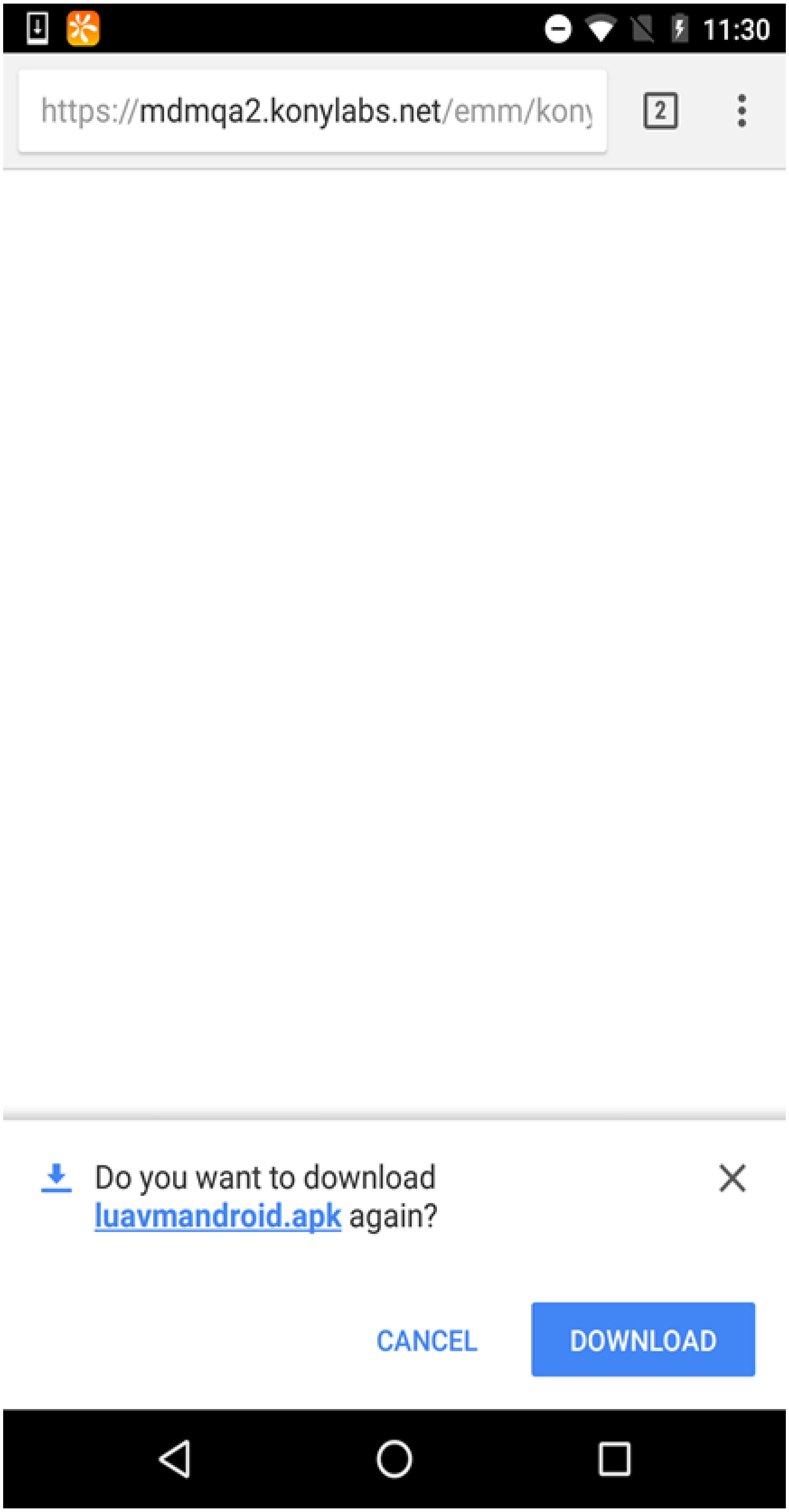


No Apps Available

Mandatory Upgrade

Mandatory Upgrade Available. This will replace the existing Enterprise Store. Please click ok to proceed.

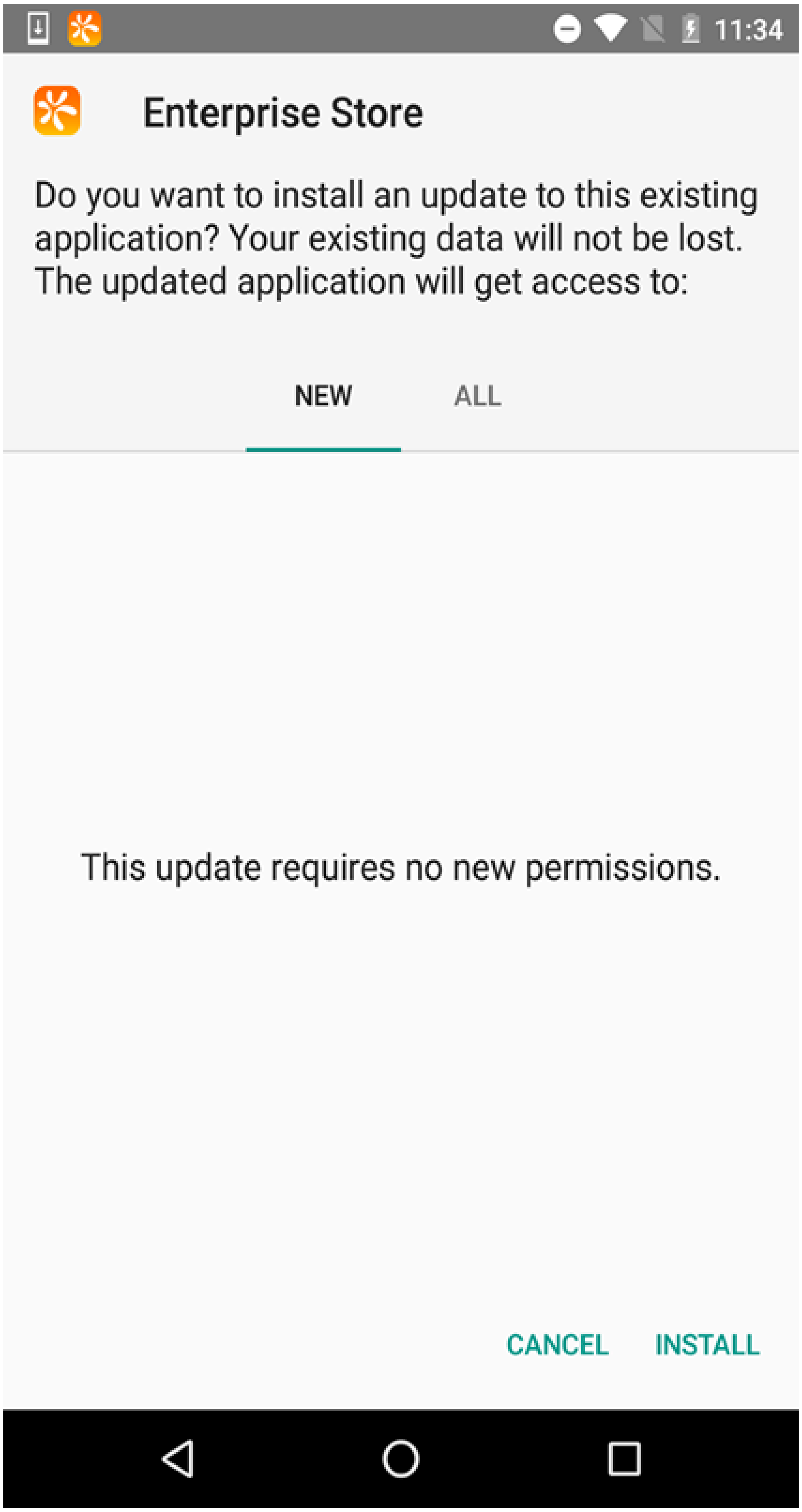
Once you click **Ok**, the page redirects to the download link of the enterprise store.



Do you want to download luavmandroid.apk again?

Click **Download**. The app downloads.

Open the downloaded apk file. An Install screen appears.



Enterprise Store

Do you want to install an update to this existing application? Your existing data will not be lost. The updated application will get access to:

This update requires no new permissions.

Click **Install**. Screen goes back to the home page and the enterprise store is installed.

9.5.13.3 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.

10. Device Management

Enterprise Mobility Management (EMM) software is primarily a policy and configuration management tool for mobile handheld devices. It helps enterprises to manage complex mobile computing and communications environment by supporting security, network services, and software and hardware management across multiple OS platforms.

This is especially significant as bring your own device (BYOD) initiatives is the focus of many enterprises. It can support corporate owned as well as personal devices, and supports a more complex and heterogeneous environment.

The primary purpose of MDM is to ensure that all the devices and device users are in compliance with the IT Policies set by company.

Devices must be enrolled to manage them efficiently. The management can allow some of their employees or all of them into this program. Once enrolled successfully, the IT Administrator has complete control over the devices.

Devices are grouped together into Device Sets based on a set of rules.

To keep the devices in check, device policies are created, and applied to device sets. A device may belong to several device sets and therefore can have several policies applicable to it. But only one policy should be applied to a device. To resolve this, each policy has a Priority associated with it. The policy with the highest priority among prescribed policies is applied.

The Administrator also defines Compliance Actions, if the policy rules are not complied. Based on the severity of the non-compliance, the Administrator can prescribe a set of actions, such as sending alerts to the Admin or a User, Blocking Email, Resetting Passcode and Locking Device, Enterprise Wipe and finally Complete Wipe.

The Admin can also view reports and dashboards on MDM activities.

10.1 Managing Devices

Managing devices includes:

- Device Set
- Device Policy
- Device
- Event Log

10.2 Device Set

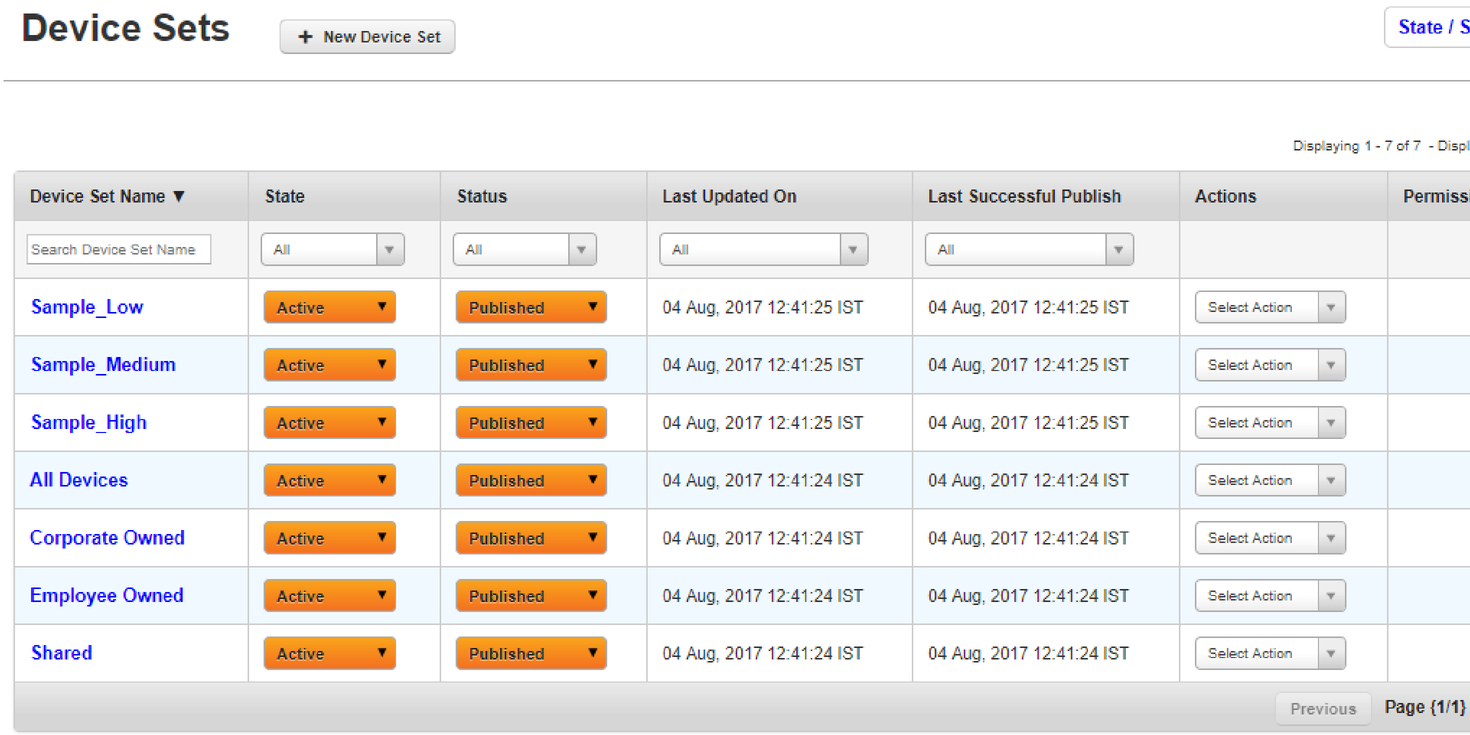
A Device Set is a collection of devices. The primary purpose to create a new Device Set is to group devices into a set based on business requirements and also to control all the enrolled and active devices as part of the set.

Limited Device Set: When a limited access administrator creates a device set, the device set is associated with permission sets assigned to the limited access administrator. Only devices that are within the purview of the applicable permission set can be part of the limited device set.

From the **Device Management** section, click the **Device Set** from the left panel. The Device Set page appears with a list of the device sets. The list view displays a list of all the device sets along with other details. You can search the device sets based on each column and also sort on each column.

Several device sets are available in the Device Sets page by default. Using these device sets, you can understand the different types of device sets. You can add devices to these devices sets and apply policies on these device sets.

Default device sets are associated with default groups and some default device policies. When a user is assigned to a group, devices enrolled by the user are associated with the corresponding device set and device policies.



Device Sets

Device Set Name ▼	State	Status	Last Updated On	Last Successful Publish	Actions	Permiss
Search Device Set Name	All ▼	All ▼	All ▼	All ▼		
Sample_Low	Active ▼	Published ▼	04 Aug, 2017 12:41:25 IST	04 Aug, 2017 12:41:25 IST	Select Action ▼	
Sample_Medium	Active ▼	Published ▼	04 Aug, 2017 12:41:25 IST	04 Aug, 2017 12:41:25 IST	Select Action ▼	
Sample_High	Active ▼	Published ▼	04 Aug, 2017 12:41:25 IST	04 Aug, 2017 12:41:25 IST	Select Action ▼	
All Devices	Active ▼	Published ▼	04 Aug, 2017 12:41:24 IST	04 Aug, 2017 12:41:24 IST	Select Action ▼	
Corporate Owned	Active ▼	Published ▼	04 Aug, 2017 12:41:24 IST	04 Aug, 2017 12:41:24 IST	Select Action ▼	
Employee Owned	Active ▼	Published ▼	04 Aug, 2017 12:41:24 IST	04 Aug, 2017 12:41:24 IST	Select Action ▼	
Shared	Active ▼	Published ▼	04 Aug, 2017 12:41:24 IST	04 Aug, 2017 12:41:24 IST	Select Action ▼	

The Device Set list view displays the following columns:

Columns	Description
Device Set Name	Displays the unique identification name of the Device Set. The Device Set can be sorted on the **Device Set Name** column.
State	Displays the current state of the Device Set.
Status	Displays the current status of the Device Set.
Last Updated On	Displays the date when the Device Set is last updated by the Administrator.
Last Successful Publish	Displays the date when the Device Set is last published by the Administrator.
Actions	Displays the actions possible on a Device Set.

Columns	Description
Permission Sets	Displays the Permission sets available for a device set. This column is shown to super administrators.

You can scroll the list view through **Previous** and the **Next** button.

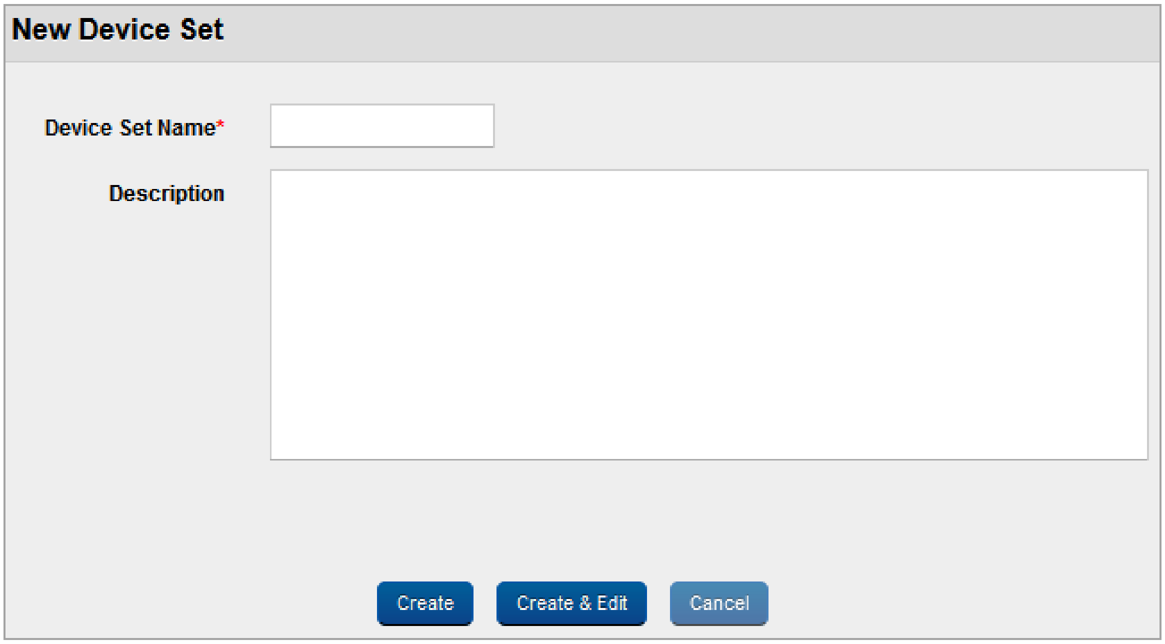
You can perform the following activities from this page:

- Adding a New Device Set
- Publishing a Device Set
- Assigning Policies to a Device set
- Policy Resolution
- Copying a Device Set
- Searching for Device Sets
- Updating Device Set Details
- Updating Published Device Sets
- Deleting a Device Set
- Unpublishing a Device Set

10.2.1 Adding a New Device Set

To create a new Device Set, follow these steps:

1. To open the **New Device Set** window, click the **+ Add Device Set** button next to the Device Set label at the top of the page.



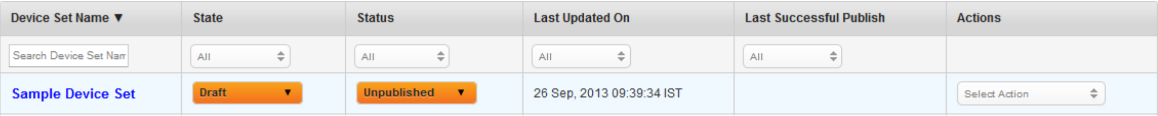
a. **Device Set Name**: Enter a logical name for the Device Set. When you create a Device Set, it is recommended that you give it a unique name that clearly describes its purpose. Once created, you cannot change the Device Set name.

b. **Description**: Enter a brief description of the Device Set. The description should accurately describe the features and functionality of your Device Set.

2. If you wish to update the newly created Device Set later, click the **Create** button. The Device Set is created and the Device Set appears in the list view.

3. If you wish to update the newly created Device Set immediately, click the **Create and Edit** button. The newly created Device Set opens in the Device Set Details page. You can define the properties and rules of the Device Set.

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



Device Set Name ▼	State	Status	Last Updated On	Last Successful Publish	Actions
Search Device Set Nam	All	All	All	All	
Sample Device Set	Draft	Unpublished	26 Sep, 2013 09:39:34 IST		Select Action

The newly created Device Set appears in the list view with State as **Draft** and Status as **Unpublished**.

Device set is able to send a message when it is in Draft state and the status is Unpublished. This allows the Admin to communicate with users about updates in progress, and on which date the device set is active.

10.2.1.1 Device Set Definition

To set the device set definition, follow these steps:

You need to set conditions that are applied to the Device Set. Device Set conditions are based on device parameters. Based on, selected parameter, the Device Attribute drop-down menu is updated. The following table displays existing device parameters with associated attributes.

Device Parameter	Device Attributes
Hardware Attributes	• Device Model • SIM ID • IMEI • Screen Size
User Attributes	• Device Name • Ownership Type • User Groups • User Name • User ID • Domain Name

Device Parameter	Device Attributes
Network Information	• Current Carrier • Phone Number • Home Carrier
Operating System	• OS Version • Platform
Security and Compliance	• Compliance State • Device Jailbroken or Rooted • Hardware Encryption Capability
Software Installed	• Name of Application
MDM Services	• Agent Version

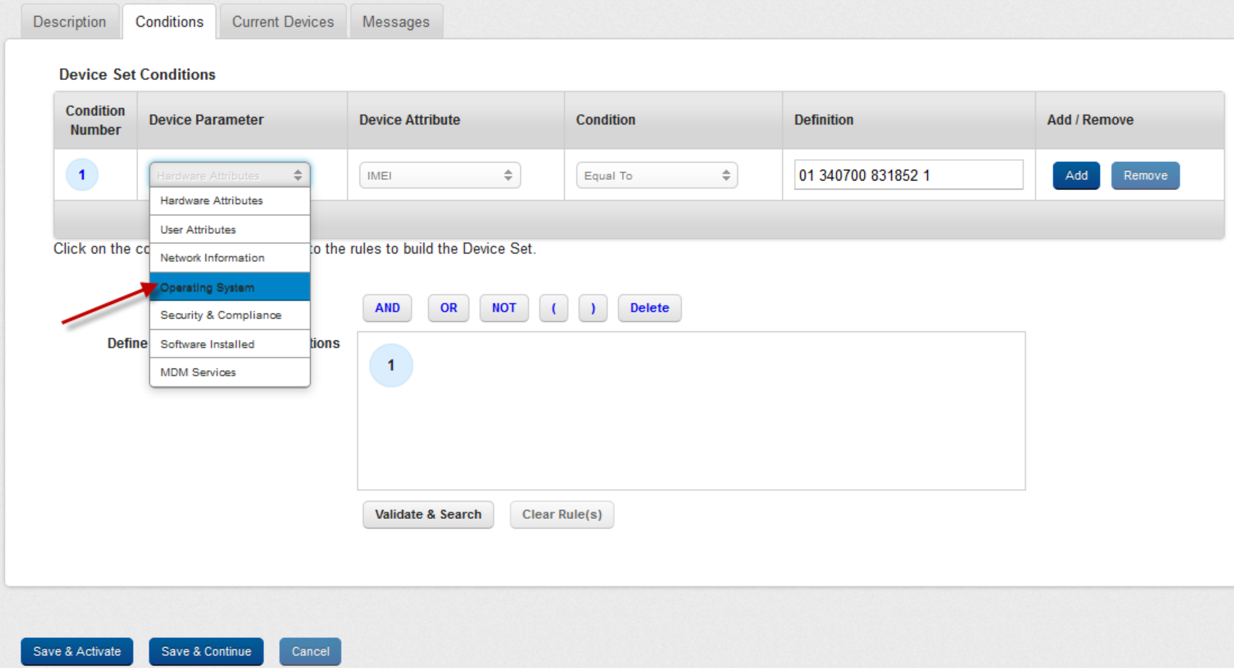
For device parameters, based on the device attribute, Condition column drop-down list changes. For example, while User Attributes parameter's Device Name attribute has all conditions available, Ownership attribute has only Equal To and Not Equal To conditions.

Conditions available are

- Begins With
- Contains
- Ends With
- Equal To
- In

- Does Not Contain
- Not Equal To

To apply Device Set conditions, follow these steps:



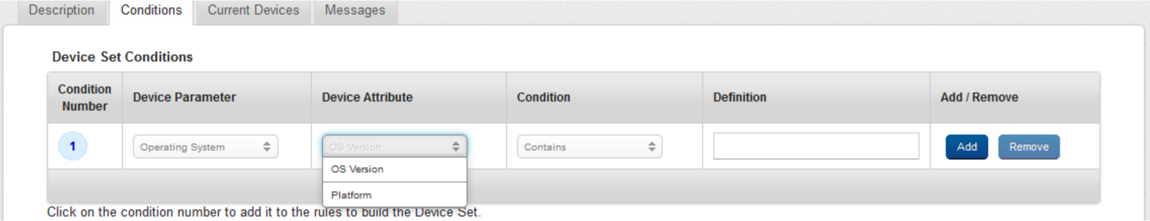
Device Set Conditions

Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Hardware Attributes	IMEI	Equal To	01 340700 831852 1	Add Remove

Click on the co to the rules to build the Device Set.

Define tions

1. **Device Parameter**: Select the device parameter from the drop-down list, for example, Operating System.

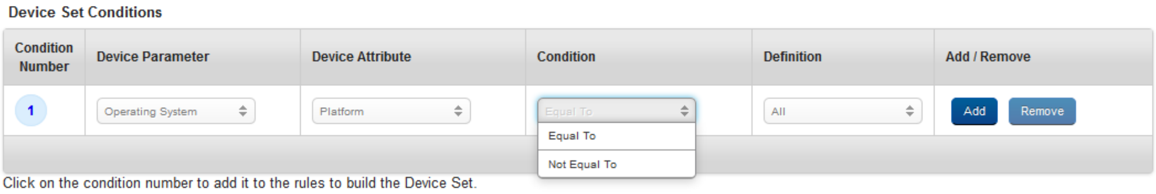


Device Set Conditions

Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Operating System	OS Version	Contains		Add Remove

Click on the condition number to add it to the rules to build the Device Set.

2. **Device Attributes**: As per selected Device parameter, Device Attributes changes, select the required attribute from the drop down list, for example, OS Version or Platform.

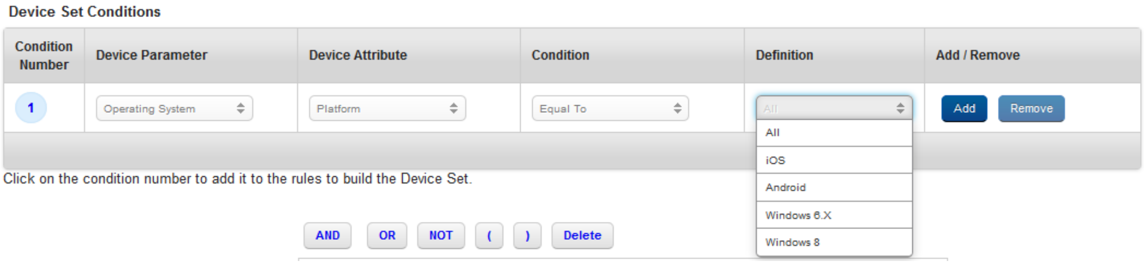


Device Set Conditions

Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Operating System	Platform	Equal To	All	Add Remove

Click on the condition number to add it to the rules to build the Device Set.

3. **Condition**: Select the condition from the drop -down list, for example, Equal to or Not Equal to



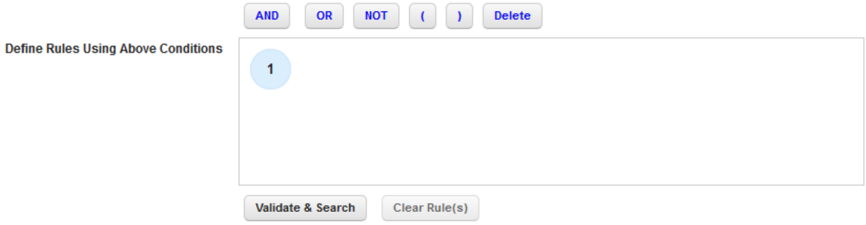
Device Set Conditions

Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Operating System	Platform	Equal To	All	Add Remove

Click on the condition number to add it to the rules to build the Device Set.

4. **Definition**: As per selected device attribute, Definitions are updated in the drop-down menu. Select the required Platform from the drop-down menu.

5. Click the **Condition Number**. The Condition Number appears in the **Defines Rules Using Above Conditions** text box. Expressions for the rules are created using boolean Algebra.



Define Rules Using Above Conditions: 1

6. Click the **Add** button to add another condition.

> ***Note:*** Do not use double negative operator in your expression when using Oracle database. Example, 1 AND 2 OR NOT NOT 3.

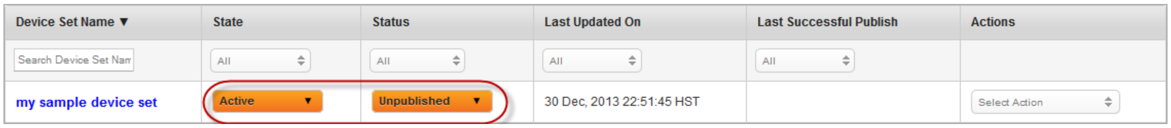
7. Click the **Validate and Search** button. The devices that map to the conditions prescribed are shortlisted and shown. Device Name, Device Owner, Ownership Type, IMEI, OS, Phone Number and Last Check-in details appears in the list view.

> ***Note:*** For limited device sets, this will contain devices under the applicable purview.

8. Click the **Save and Activate** button.

   The devices are assigned to the Device Set. Click the Current Devices tab to view assigned devices to the Device Set.

> ***Note:*** While using conditions such as Contains and Does not Contains for OS version, the OS name is also considered. You can use the term Android and get some devices. For definitive comparators such as equal to and not equal to, the field must be filled exactly, such as Android 4.2.2 otherwise no results are displayed.



Device Set Name ▼	State	Status	Last Updated On	Last Successful Publish	Actions
Search Device Set Nam	All	All	All	All	
my sample device set	Active ▼	Unpublished ▼	30 Dec, 2013 22:51:45 HST		Select Action

The updated Device Set appears in the list view. The device state is changed to Active and Status remains as Unpublished.

You can change the state and status of the device set from the list view and also from the device set details page. You can change the State and Status of the device set from the list view through options available under State and Status columns. In order to make a device set live, you must publish it.

> ***Important:*** If a published device set has a reference to an AD group, and the Group is deleted on AD, then the device is automatically unpublished and returned to Draft state.

10.2.2 Publishing a Device Set

Based on existing business rules, device sets are published. Once a newly created device set is created, it is displayed in list view. By default, the newly created device set is in Draft mode and the status is set to unpublished.

As a prerequisite, to make changes in state and status of a Device Set, you should own that Device Set.

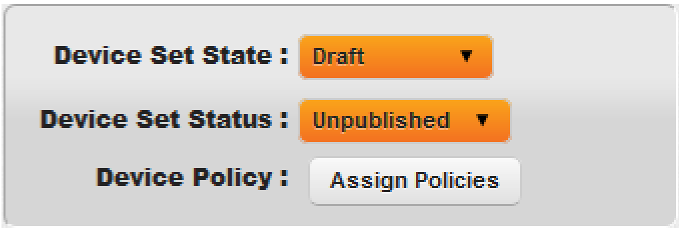
10.2.2.1 Device Set State

State indicates the specific action state set to the device. It indicates the type of action that is done or needs to be done to the device set.Until the Device Set definition is completed and the Admin submits the same for publication, the state remains as a draft. Once activated, the Device Set can be published by the Administrator with appropriate permissions.

10.2.2.2 Device Set Status

Status indicates the readiness of the device set to be used. Device set Status can be either Unpublished or Published. When a new device set is created, the Status is set to Unpublished. Once activated, Administrator can publish the device set with appropriate permissions.

To publish a Device Set, follow these steps:



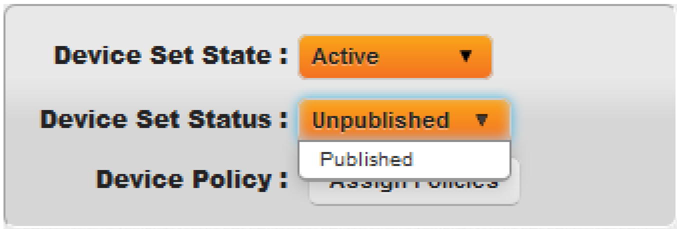
Device Set State : Draft

Device Set Status : Unpublished

Device Policy : Assign Policies

By default, a newly created Device Set appears in **Draft** State and Status is set to Unpublished.To activate a device set, you first need to define the device set definition.

The following procedure explains how to publish a device set from the device set details page.

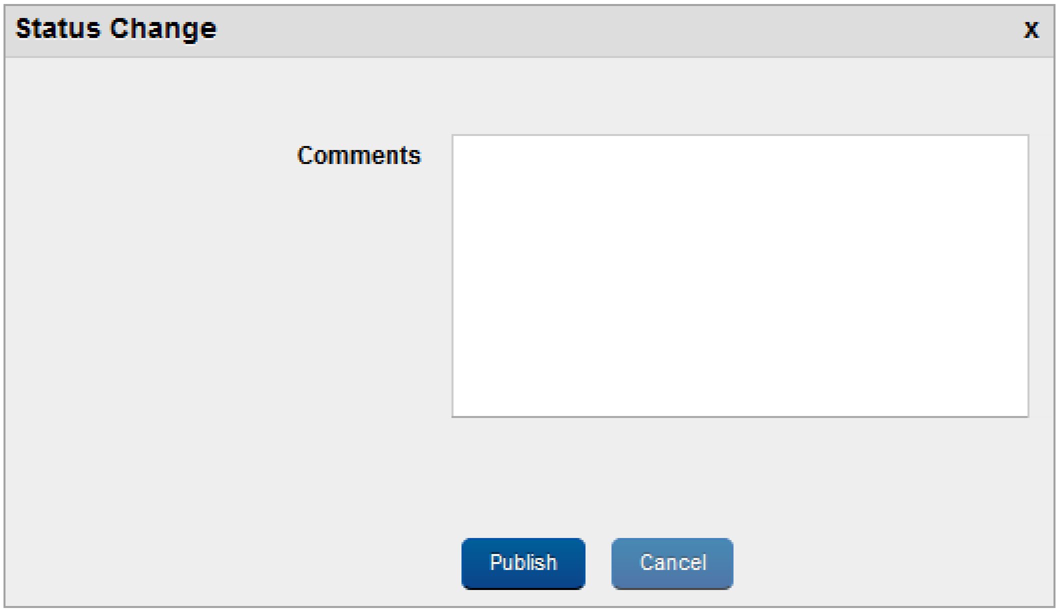


Device Set State : Active

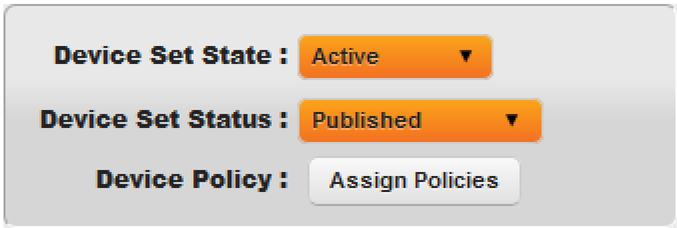
Device Set Status : Unpublished

Device Policy : Assign Policies

1. To publish the Device Set, select the Device Set Status as **Published** from the drop-down menu.



2. **Status Change** window appears.
3. Enter a valid reason justifying publication of the device set. Click the **Publish** button. In the confirmation (Status Change window) message that appears, click OK to continue.



Device Set State : Active ▼
Device Set Status : Published ▼

The Status changes to Published.

10.2.3 Assigning Policies to a Device Set

Administrators apply policies on device sets to ensure that all the devices adhere to the organization's IT policies. To apply a policy, the Device Set should be approved and published. The Admin must choose policies of each type to apply on device sets.

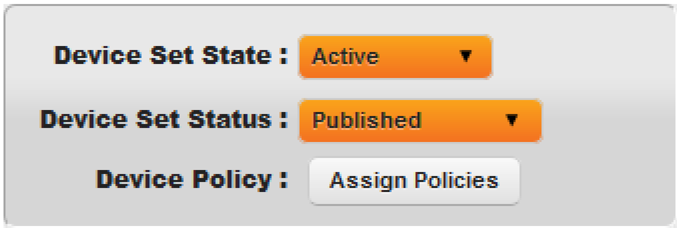
Along with the Policy, the Admin may specify a Geo-fence or a Time Fence, if applicable from the list of Geo and Time Fences available.The Admin has the choice of either applying a Geo-fence or a Time fence or not. The Admin should not choose Geo-fences or Time fences that overlap. If no Geo-fence or Time fence is specified, then multiple policies cannot be prescribed for a device set. Once the policies of each type are assigned to the Device Set, Administrator validates them.

All the Devices as part of a Device Set are enforced with the policies that are pushed on the Device Set. If the device is part of more than one Device Set, then priority of policies determine which policy should be applied to the device.

The newly chosen policies are applied on the Device Set.

To apply policies to a device set follow these steps:

1. Select the required Device set from the list view. The **Device Set Details** page appears.

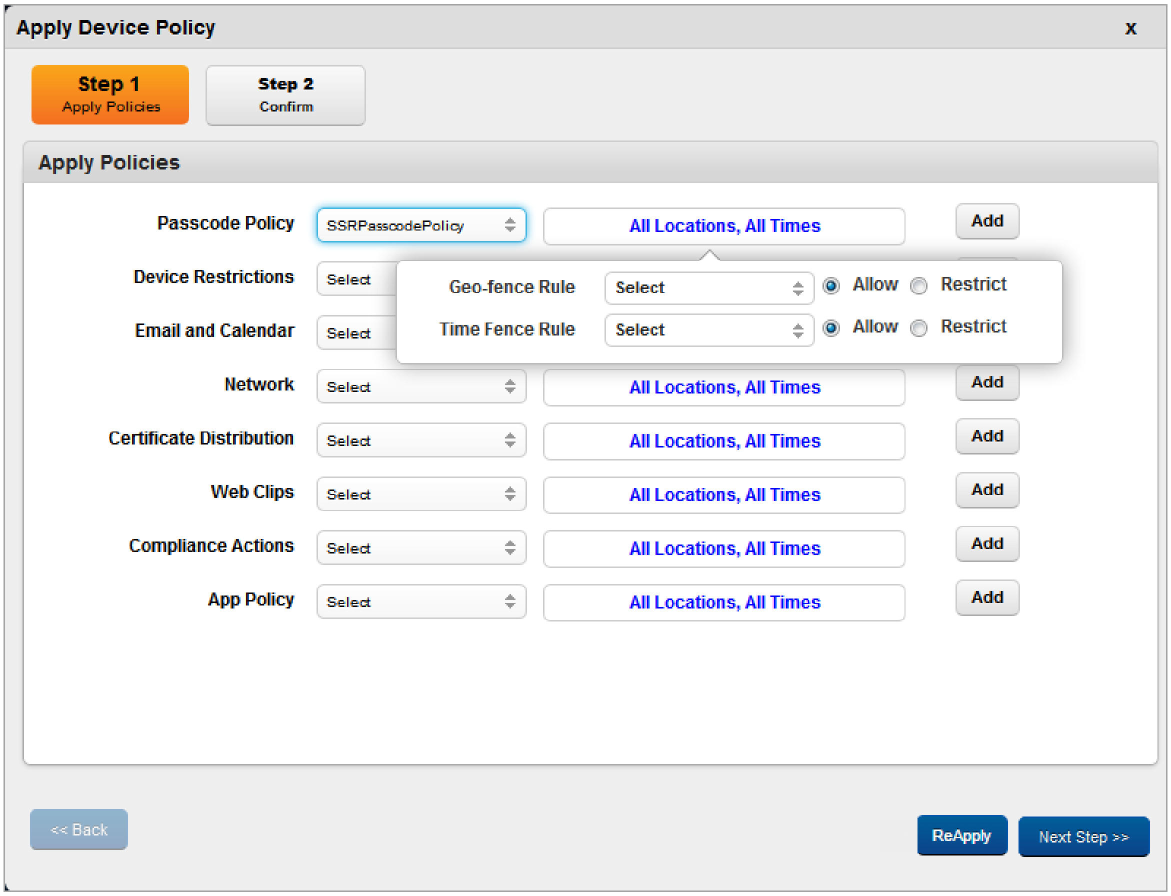


Device Set State : Active ▼

Device Set Status : Published ▼

Device Policy :

2. Click the **Assign Policies** button to open **Apply Device Policy** window.



Passcode Policy	SSRPasscodePolicy	All Locations, All Times	Add
Device Restrictions	Select		
Email and Calendar	Select		
Network	Select	All Locations, All Times	Add
Certificate Distribution	Select	All Locations, All Times	Add
Web Clips	Select	All Locations, All Times	Add
Compliance Actions	Select	All Locations, All Times	Add
App Policy	Select	All Locations, All Times	Add

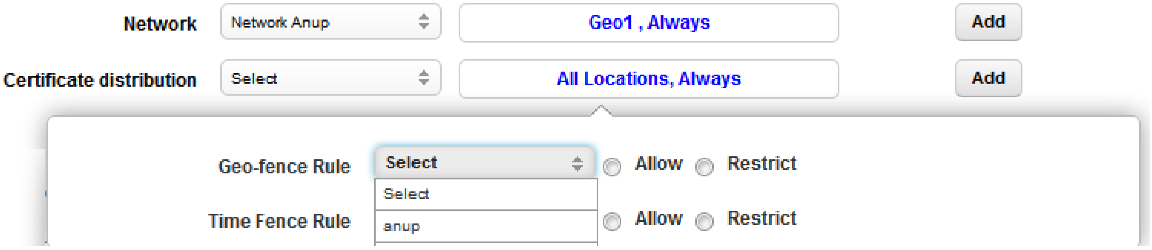
Geo-fence Rule	Select	● Allow	○ Restrict
Time Fence Rule	Select	● Allow	○ Restrict

The **Apply Device Policy** window appears.

> *Important:* If you want to assign a policy again on a device set, click **ReApply**.

3. **Step One - Apply Policies**: Each policy is associated with a drop-down menu. Select the appropriate options from the drop- down list for Policies.

4. To set the Geo-fence Rule and the Time Fence rule, place the cursor in **All Locations, All Times** pane.



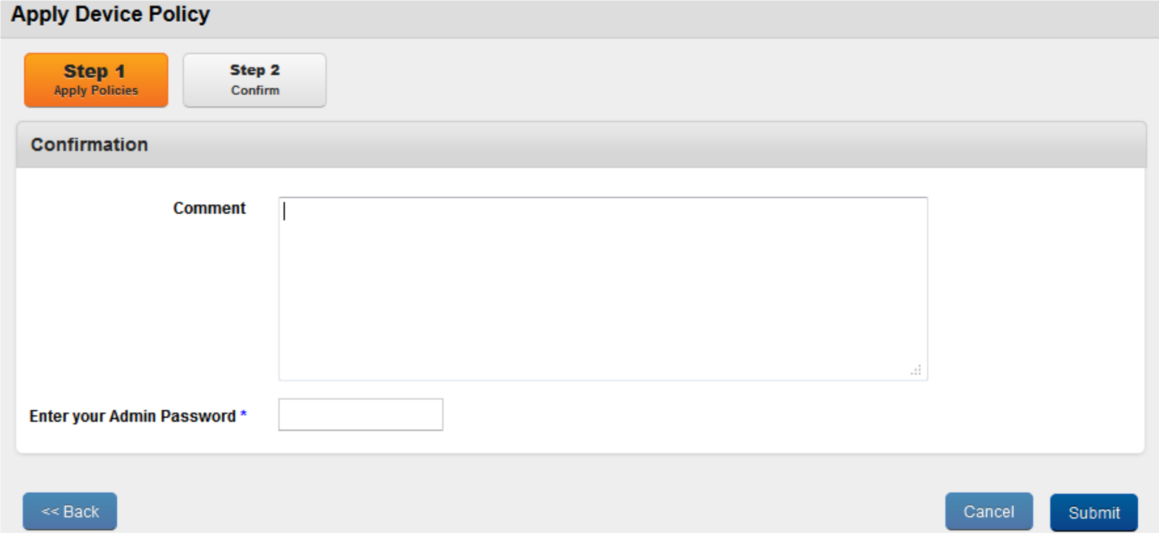
A pop-up with options for Geo-fence Rule and Time Fence Rules appears.

5. **Geofence Rule**: Select the location from the drop-down menu and select the option as Allow or Restrict.

6. **Time Fence Rule**: Select the Time Fence rule from the drop-down menu and select the option as Allow or Restrict.

   The selected options are updated in the pane.

7. Click the **Next Step** button to open the **Step 2** window.



Confirmation window appears.

8. **Step 2 - Confirm**: Enter a valid comment in the **Comments** box to justify applying policy to the Device Set.

9. Click the **Submit** button to submit the details. In the confirmation (**Apply Policy window**) message that appears, click **OK** to continue.

   The System displays the confirmation message about successful application of policies to the device set. Click **OK** to return to the page.

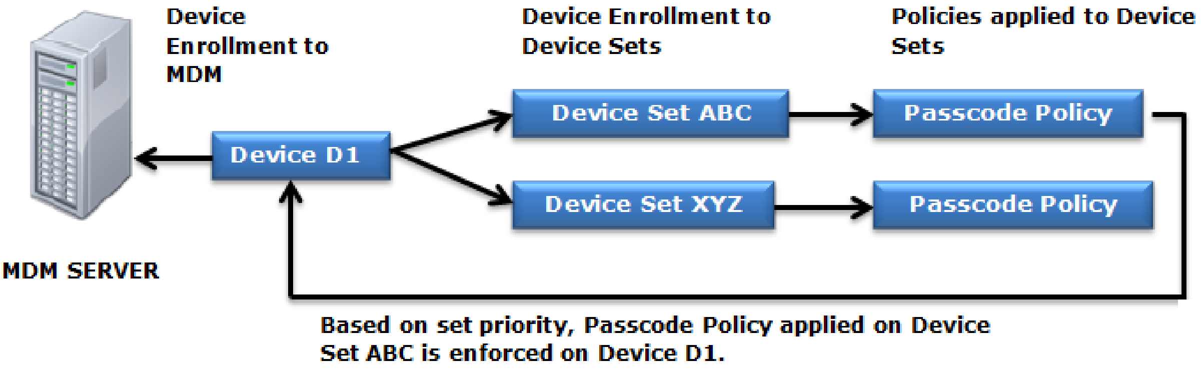
   Click the **Cancel** button to close the window.

   Policies cannot be assigned to unpublished device sets.

   > *Important:* If you want to assign the policy again on the device set, click **ReApply**.

10.2.4 Policy Resolution

All the devices as part of the Device Set are enforced with the policies that are pushed on to the Device set. If the device is part of more than one Device Set, then according to priority of policies, a policy is applied.


Device Enrollment to MDM
Device Enrollment to Device Sets
Policies applied to Device Sets
Device Set ABC
Passcode Policy
Device D1
Device Set XYZ
Passcode Policy
MDM SERVER
Based on set priority, Passcode Policy applied on Device Set ABC is enforced on Device D1.

Device Set Name	Member Devices	Applied Policies
ABC	**D1**, D2, D3, D4	**Passcode Policy**, Network Policy, Device Restriction Policy

Device Set Name	Member Devices	Applied Policies
XYZ	**D1**, D5, D7, D8	**Passcode Policy**, App Policy, Compliance Action Policy

This following example describes the resolution of the policies.

Device Set **ABC** comprises four devices, D1, D2, D3, and D4. Device Set **XYZ** comprises four devices D1, D5, D6 and D8.

Policies applied on Device Set ABC: **Passcode Policy**, **Network Policy** and **Device Restrictions Policy**. **The priority for the Passcode Policy is set to 1**.

Policies applied on Device Set XYZ: **Passcode Policy**, **App Policy** and **Compliance Action Policy**. **The priority for the Passcode Policy is set to 3**.

In the above scenario, **Device D1** is a common member of both the device sets; therefore overall five policies are applied on Device D1.

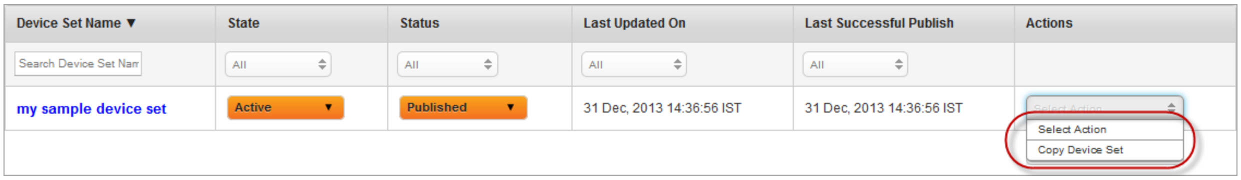
Applied Policies on D1: Passcode Policy, Network Policy, Device Restrictions Policy, App Policy and Compliance Action Policy

Passcode Policy is applied on both the device sets, so based on set priority **Passcode Policy** applied on **Device Set ABC** is enforced on **Device D1**.

10.2.5 Copying a Device Set

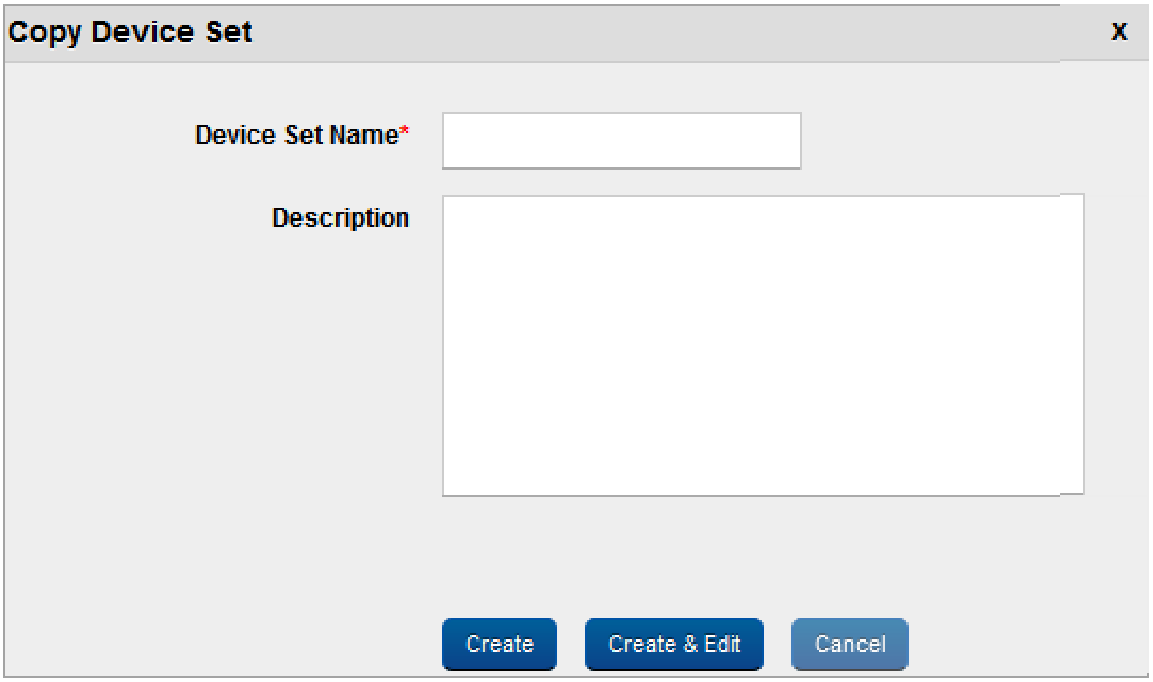
If you wish to build a new Device Set with similar conditions applied to an existing Device Set, you can copy an existing Device Set to create a new Device Set. The copied Device Set comprises all the configurations provided in the parent Device Set. You need to rename the copied Device Set and provide a logical description. Once created, you can update the copied Device Set.

To copy a Device Set, follow these steps:



Device Set Name ▼	State	Status	Last Updated On	Last Successful Publish	Actions
Search Device Set Nam	All	All	All	All	
my sample device set	Active ▼	Published ▼	31 Dec, 2013 14:36:56 IST	31 Dec, 2013 14:36:56 IST	Select Action Copy Device Set

1. To open the Copy Device Set option, click the **Copy Device Set** option under the Actions column.



Copy Device Set window appears.

2. Enter the following details:

   a. **Device Set Name**: Enter a unique and appropriate Device set name.

   b. **Description**: Enter an appropriate description of the device set.

3. Click the **Create** button.

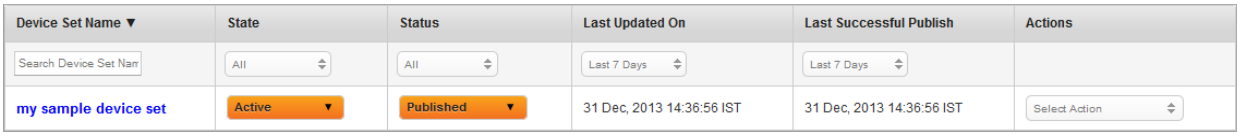
   The copied Device Set appears in the list view. The copied device set state is in draft mode and status is set to unpublished. .

4. If you wish to update the newly created Device Set immediately, click the **Create and Edit** button. The newly created Device set opens into **Device Set Details** page. You can set the definition of the device set.

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

10.2.6 Searching for Device Sets

You can search a desired Device Set 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 Device Set, follow these steps:



Device Set Name ▼	State	Status	Last Updated On	Last Successful Publish	Actions
Search Device Set Nam	All	All	Last 7 Days	Last 7 Days	
my sample device set	Active ▼	Published ▼	31 Dec, 2013 14:36:56 IST	31 Dec, 2013 14:36:56 IST	Select Action

1. Enter or select details for the following search filters:

   a. **Device Set Name**: Enter partial or a complete Device Set name in the **Search Device Set Name** text field.

   b. **State**:Select the desired option from the drop-down list, for example, Draft or Active.

   c. **Status**: Select the desired option from the drop-down list, for example, Published or Unpublished.

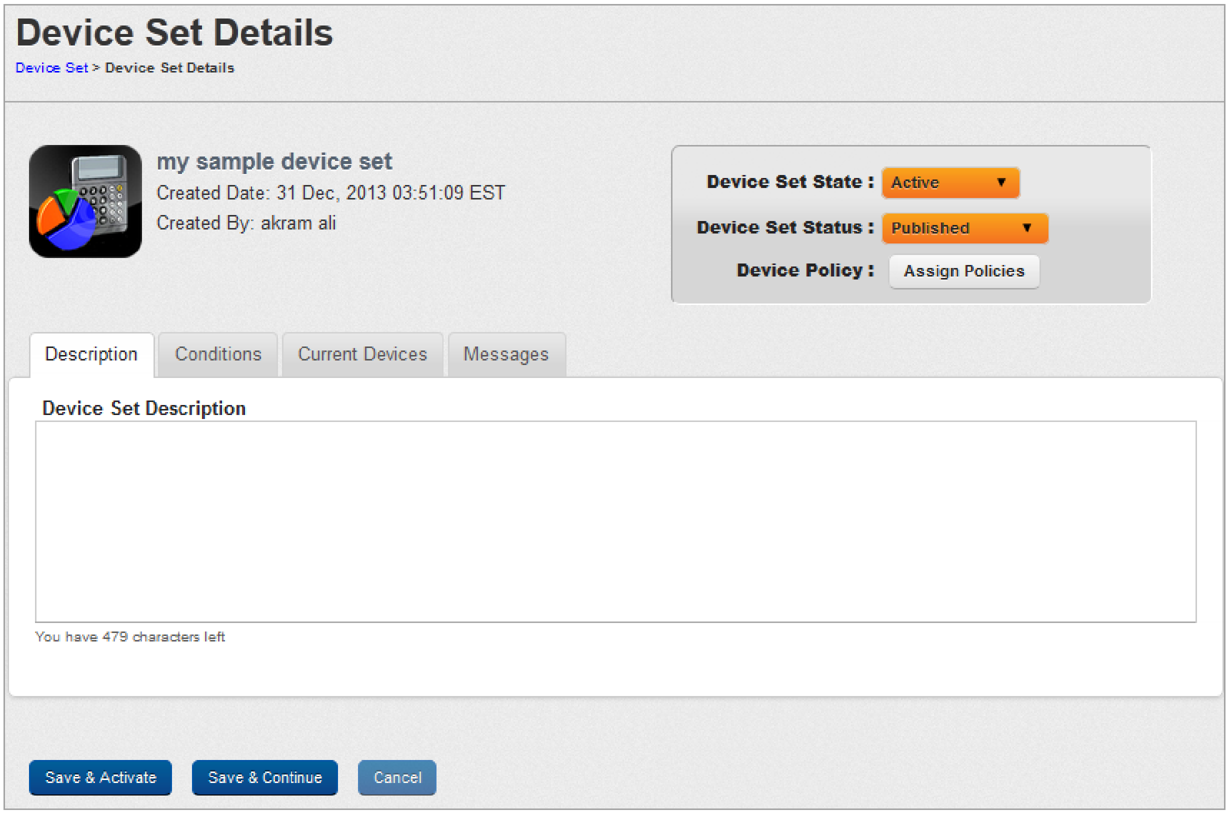
   d. **Last Updated On**: Select the period when device set was last updated, for example, Today or Yesterday.

   e. **Last Successful Publish**: Select the period when the device set was last published successfully.

2. According to your search filters criteria, the list view is updated with respective device set details. By default, the list view displays ten device sets 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.

10.2.7 Updating Device Set Details

The primary purpose to update an active and published device set is to fulfill the requirement of existing business rules. You may need to redefine the definition of a device set based on applied business rules.



Device Set Details

Device Set > Device Set Details

my sample device set
Created Date: 31 Dec, 2013 03:51:09 EST
Created By: akram ali

Device Set State : Active
Device Set Status : Published
Device Policy : Assign Policies

Device Set Description

You have 479 characters left

The Device Set Details Page includes the following screen elements:

Screen Element Properties	Description
Page Title	This is available on extreme right corner on top of the screen, for example, Device Set Details.
Navigation Link	This link navigates you to main page, for example, click Device Set>Device Set Details link to navigate to Device Set main page.

Screen Element Properties	Description
Device Set Name	Displays the device set name next to the icon.
Device Set Status	You change the device set status through this button.
Device Set State	You change the device set state through this button.
Device Policy	You assign the device policies through this button.
Created Date	Displays the date and the time when the device set was created.
Created By	Displays name of the Administrator who created the device set..

Click the required Device Set in the list view, which you need to publish. By default Description tab is set to active. The tabs on the page are as follows:

- Description
- Conditions
- Current Devices
- Messages

To update description of the device set, follow these steps:

10.2.7.1 Description Tab

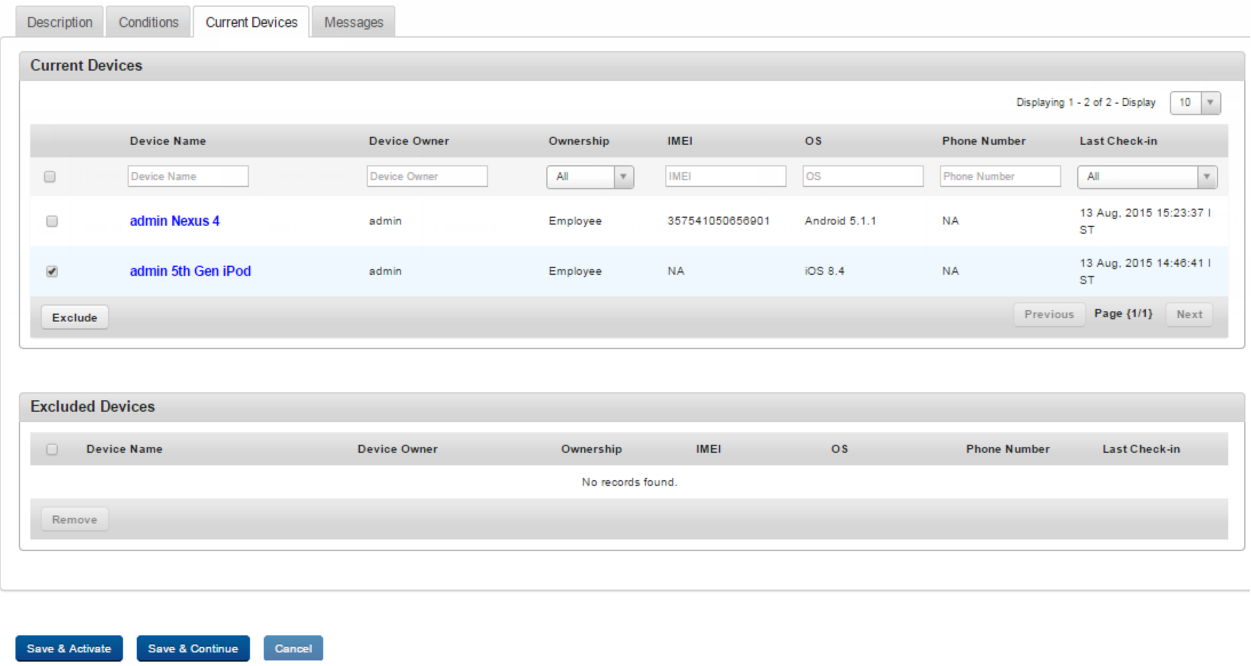
Enter the appropriate description for the Device Set or if required, update the existing content.

10.2.7.2 Conditions

To update the device set conditions, refer Adding a New Device Set

10.2.7.3 Current Devices

The Current devices tab displays the list of current devices and excluded devices in the device set.



Current Devices

Displaying 1 - 2 of 2 - Display 10

	Device Name	Device Owner	Ownership	IMEI	OS	Phone Number	Last Check-in
□	Device Name	Device Owner	All	IMEI	OS	Phone Number	All
□	admin Nexus 4	admin	Employee	357541050656901	Android 5.1.1	NA	13 Aug, 2015 15:23:37 IST
☑	admin 5th Gen iPod	admin	Employee	NA	iOS 8.4	NA	13 Aug, 2015 14:46:41 IST

Excluded Devices

□	Device Name	Device Owner	Ownership	IMEI	OS	Phone Number	Last Check-in

No records found.

Current Devices

The current devices section displays the number of devices assigned to a Device Set. The list view displays Device Name, Device Owner, Ownership, IMEI, OS, Phone Number, and Last Check-in details. These are the devices that are currently a part of the device set. As device sets are dynamic, this list changes as device properties change.

> ***Note:*** Current devices list for a limited access device set will display the same device list to all administrators (super and limited).

Excluded Devices

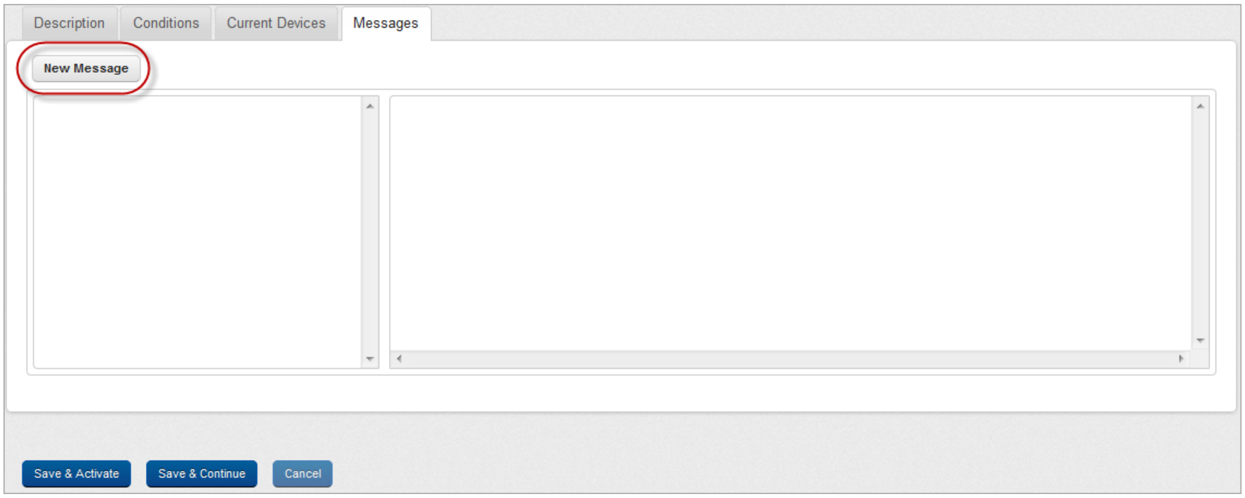
The excluded devices section displays details of devices assigned to a device set but excluded from the device set policy compliance. The list view displays Device Name, Device Owner, Ownership, IMEI, OS, Phone Number, and Last Check-in details.

Click any device in the list view to view details about a device in the Device List page.

10.2.7.4 Messages

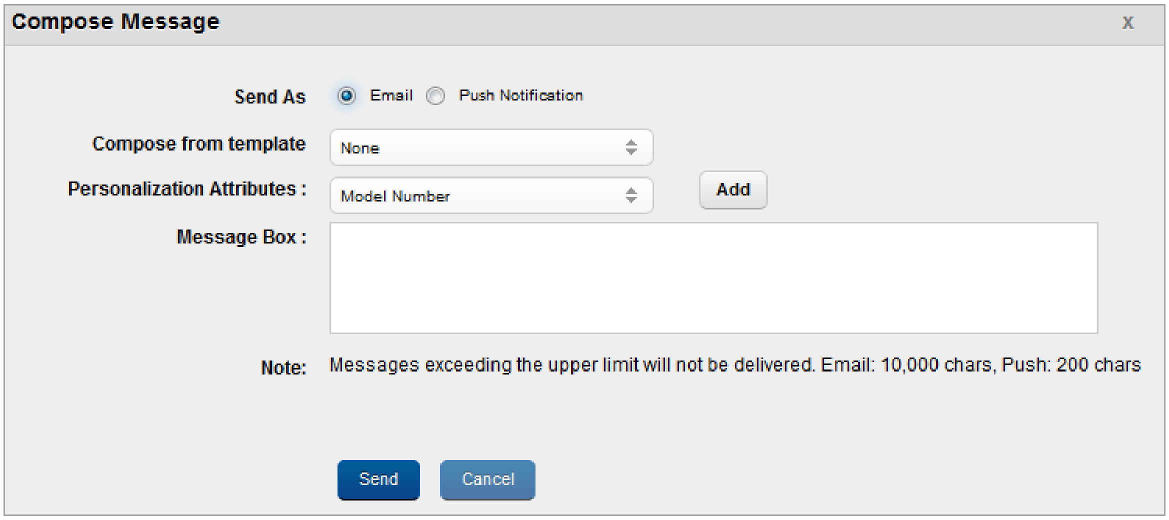
The section on notifications handles all the messages from the EMM Server. You can send new messages as well as view enrollment messages, alerts and other push messages from the EMM server.

You can compose messages from the template. You can create Message Templates under Device Settings> Message Template.



To compose a new message, follow these steps:

1. Click the New Message button.



Send As ● Email ○ Push Notification

Compose from template: None

Personalization Attributes : Model Number

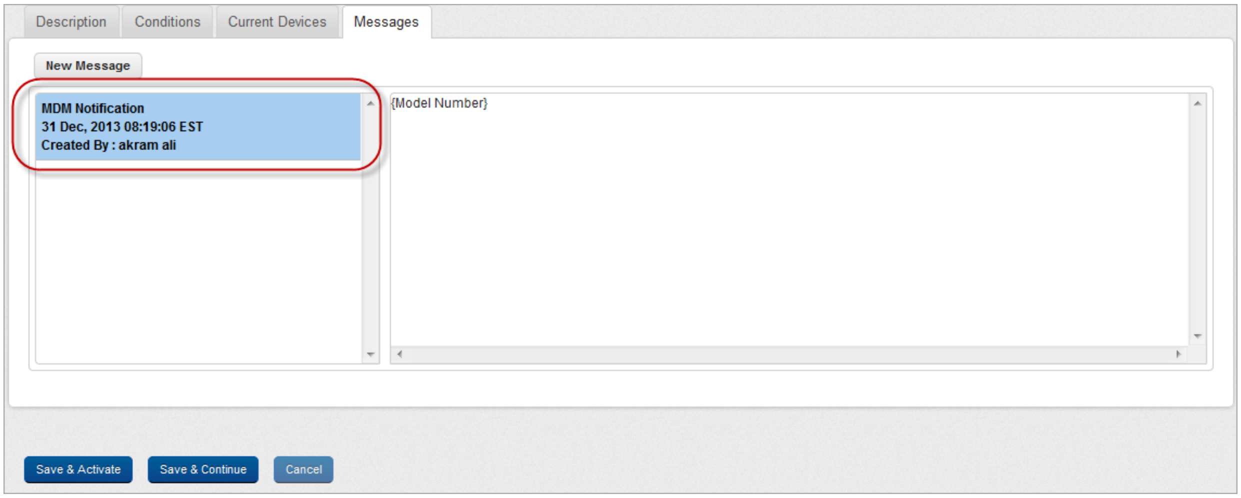
Message Box :

Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

Compose Message window appears.

2. Enter and select details for the following fields:
   a. **Send As**: By default, this option is set to Email. You can modify it to Push Notification.
   b. **Compose from Template**: If required, select the required option from the drop-down list.
   c. **Personalization Attributes**: If required, select the required option from the drop-down list.
   d. **Message Box**: As per selected options, content appears in the Message Box.

3. Click the **Send** button. In the confirmation (Send Message Success) message that appears, click OK to continue.



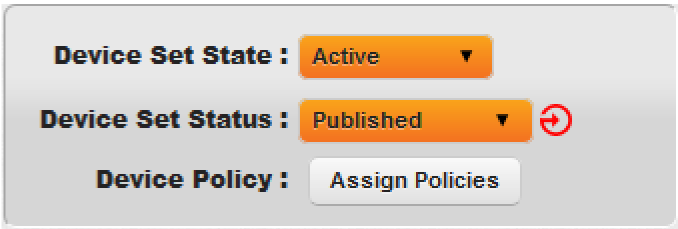
MDM Notification
31 Dec, 2013 08:19:06 EST
Created By : akram ali

{Model Number}

The sent message appears in the left panel.

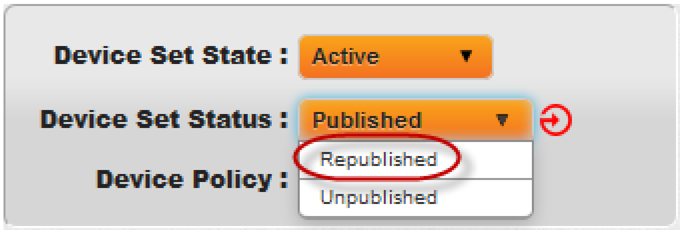
10.2.8 Updating Published Device Sets

If there are any changes to the device set definition, you may require updating the published device set. To validate the carried out updates, you need to republish the device set.


Device Set State : Active
Device Set Status : Published
Device Policy : Assign Policies

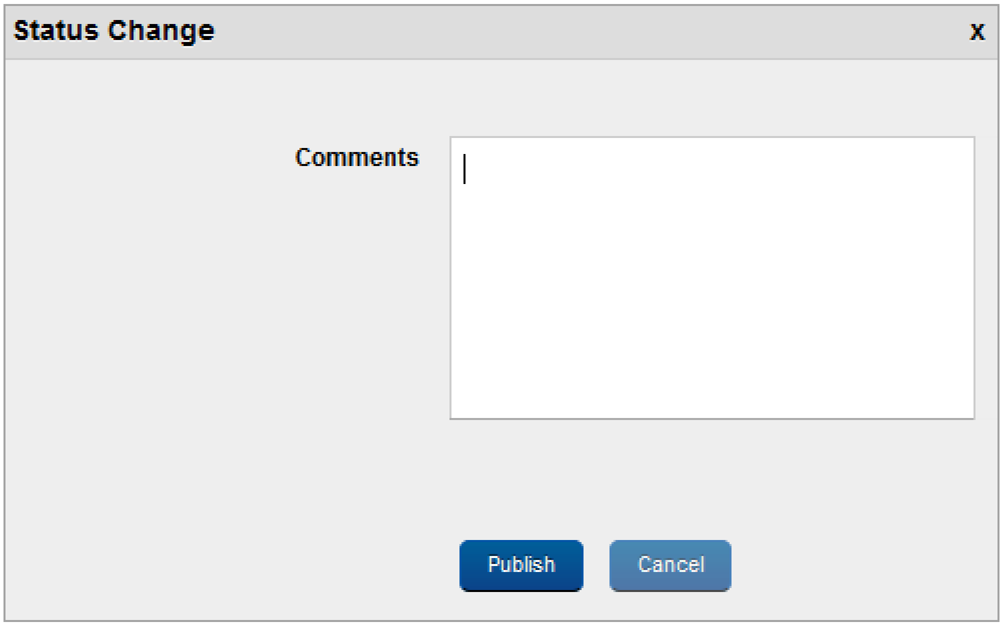
A stale state icon next to the corresponding device set status is used to indicate that changes have been made to the definition of the Device set.

To republish the Device Set, follow these steps:


Device Set State : Active
Device Set Status : Published

Device Policy :

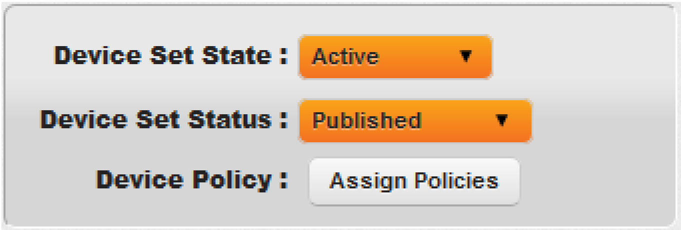
1. To publish the Device Set, select the Device Set Status as Republished from the drop-down list.



Status Change window appears.

2. Enter a valid reason for state change in the **Comments** text box.

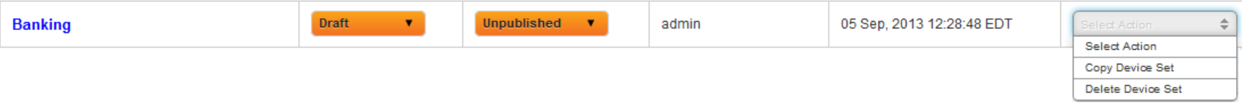
3. Click the **Publish** button to submit the status change details. In the confirmation message (Status Change) that appears, Click OK to proceed.


Device Set State : Active
Device Set Status : Published
Device Policy : Assign Policies

The Status changes to Published.

10.2.9 Deleting a Device Set

You can delete only Unpublished Device Sets. Once a Device Set is deleted, it is removed from the Device Set list.



Banking	Draft ▼	Unpublished ▼	admin	05 Sep, 2013 12:28:48 EDT	Select Action

To delete a device set, follow these steps:

1. Click the **Delete Device Set** option under the **Actions** column.

   Warning message appears.

2. The warning (Delete Device Set) message asks, if user wishes to delete the device set. Click Yes to continue.

   Confirmation message appears.

3. In the confirmation message that appears, click OK to continue.

   The Device is no longer displayed in the list view.

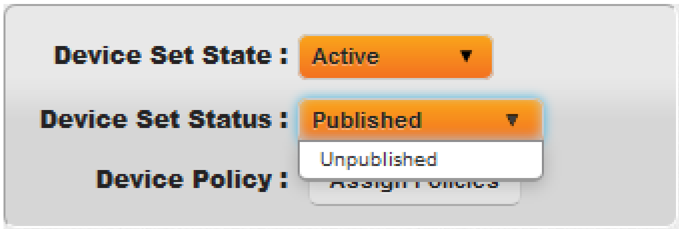
10.2.10 Unpublishing a Device Set

Unpublishing a Device Set signifies that:

- All the devices pertaining to the Device Set are removed automatically.
- All the existing policies applied to the Device Set are removed and you cannot assign new policies to the unpublished device set.

> *Important:* Immediately after status changes to unpublished, the assigned policies and devices are seen as per heart beat duration set under device settings. After the heart beat duration is over, all policies and devices are removed from the device set. For a limited device set associated with multiple permission sets, if any of the permission sets is deleted, the device set status will change to unpublished and the device set state will change to draft.

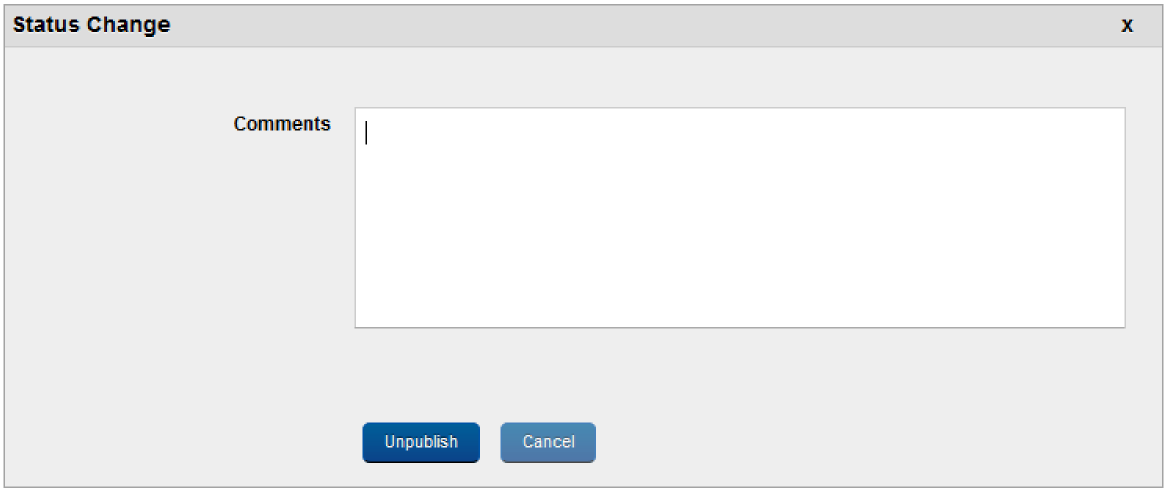
To unpublished a Device Set, follow these steps:



1. To unpublish a Device Set, select the Status as Unpublished from the drop-down menu.

   Warning message appears.

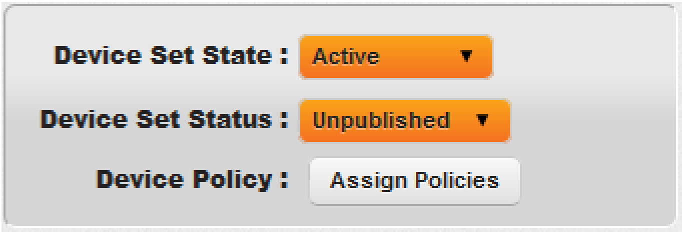
2. The warning (Delete Device Set) message warns that unpublishing the device set may leave devices without a device set and therefore policies. The warning (Unpublish Device Set) message asks, if user wishes to unpublish the device set. Click Yes to continue.

   Status Change window appears.

3. Enter a valid comment justifying device status change to Unpublished.

4. Click the **Unpublish** button. In the confirmation message that appears, click OK to continue.



Device Set State : Active ▼

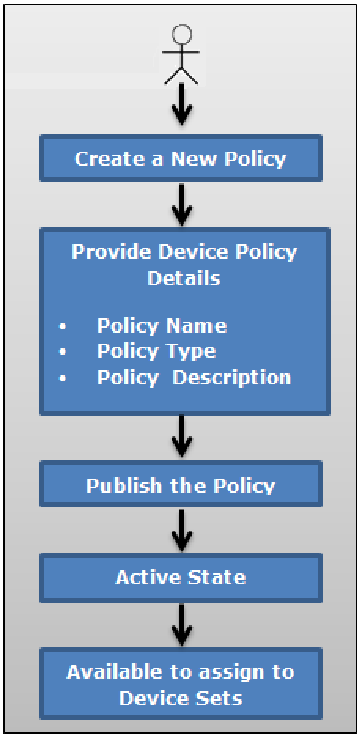
Device Set Status : Unpublished ▼

Device Policy :

The device Status changes to Unpublished.

10.3 Device Policy

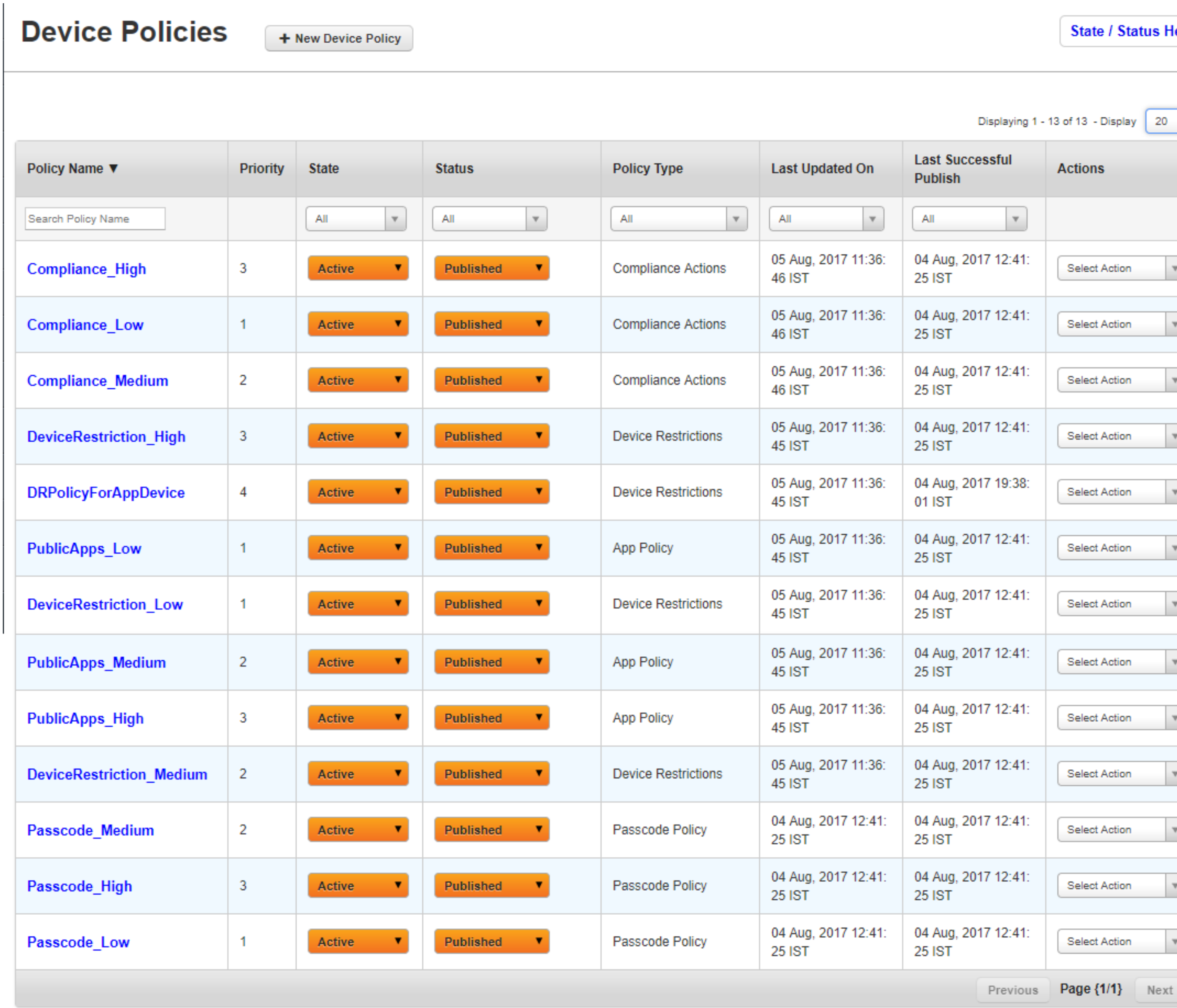
The primary purpose of a device policy is to control the end user device with respect to the business rules defined by the Administrator. Device policies are applied to a device set as per supported platforms.



From the **Device Management** section, click the **Device Policy** from the left panel. The Device Policy page appears with a list of the device policies. The list view displays a list of all the policies along with other details. You can search the device policies based on each column and also sort on each column.

In the Device Policies page, several default policies are available. Using these policies, you can understand various types of device policies that you can create. You can apply these policies on various groups, or users, or device sets.

Default device policies are associated with default device sets and to default group types. When a user is assigned to a group, devices enrolled by the user are associated with the corresponding device set and device policies.



Device Policies

Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
Compliance_High	3	Active	Published	Compliance Actions	05 Aug, 2017 11:36: 46 IST	04 Aug, 2017 12:41: 25 IST	Select Action
Compliance_Low	1	Active	Published	Compliance Actions	05 Aug, 2017 11:36: 46 IST	04 Aug, 2017 12:41: 25 IST	Select Action
Compliance_Medium	2	Active	Published	Compliance Actions	05 Aug, 2017 11:36: 46 IST	04 Aug, 2017 12:41: 25 IST	Select Action
DeviceRestriction_High	3	Active	Published	Device Restrictions	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
DRPolicyForAppDevice	4	Active	Published	Device Restrictions	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 19:38: 01 IST	Select Action
PublicApps_Low	1	Active	Published	App Policy	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
DeviceRestriction_Low	1	Active	Published	Device Restrictions	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
PublicApps_Medium	2	Active	Published	App Policy	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
PublicApps_High	3	Active	Published	App Policy	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
DeviceRestriction_Medium	2	Active	Published	Device Restrictions	05 Aug, 2017 11:36: 45 IST	04 Aug, 2017 12:41: 25 IST	Select Action
Passcode_Medium	2	Active	Published	Passcode Policy	04 Aug, 2017 12:41: 25 IST	04 Aug, 2017 12:41: 25 IST	Select Action
Passcode_High	3	Active	Published	Passcode Policy	04 Aug, 2017 12:41: 25 IST	04 Aug, 2017 12:41: 25 IST	Select Action
Passcode_Low	1	Active	Published	Passcode Policy	04 Aug, 2017 12:41: 25 IST	04 Aug, 2017 12:41: 25 IST	Select Action

The Device Policy list view displays the following columns:

Columns	Description
Policy Name	Displays the unique identification name of the device policy. The Device Policy details can be sorted on the **Policy Name** column.

Columns	Description
Priority	Displays the set priority value of a policy, for example 1.
State	Displays the current state of the device policy, for example, Draft or Active.
Status	Displays the current status of the device policy, for example, Published or Unpublished.
Policy Type	Displays the type of policy, for example, Passcode.
Last Updated on	Displays the date when the Device Policy is last updated by the Administrator.
Last Successful Publish	Displays the date when the Device Policy is last published by the Administrator.
Actions	Displays the current action done with the device policy, for example, Copy device policy.

You can scroll the grid view through **Previous** and the **Next** button.

You can perform the following activities from this page:

- Creating a New Policy
- Publishing a Device Policy
- Copying a Policy
- Changing Priority of a Policy
- Searching for Policies
- Updating Policy Details
- Updating Published Device Policy Details

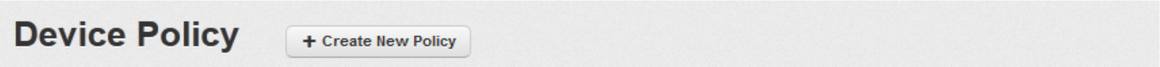
- Deleting a Policy
- Unpublishing a Policy

10.3.1 Creating a New Policy

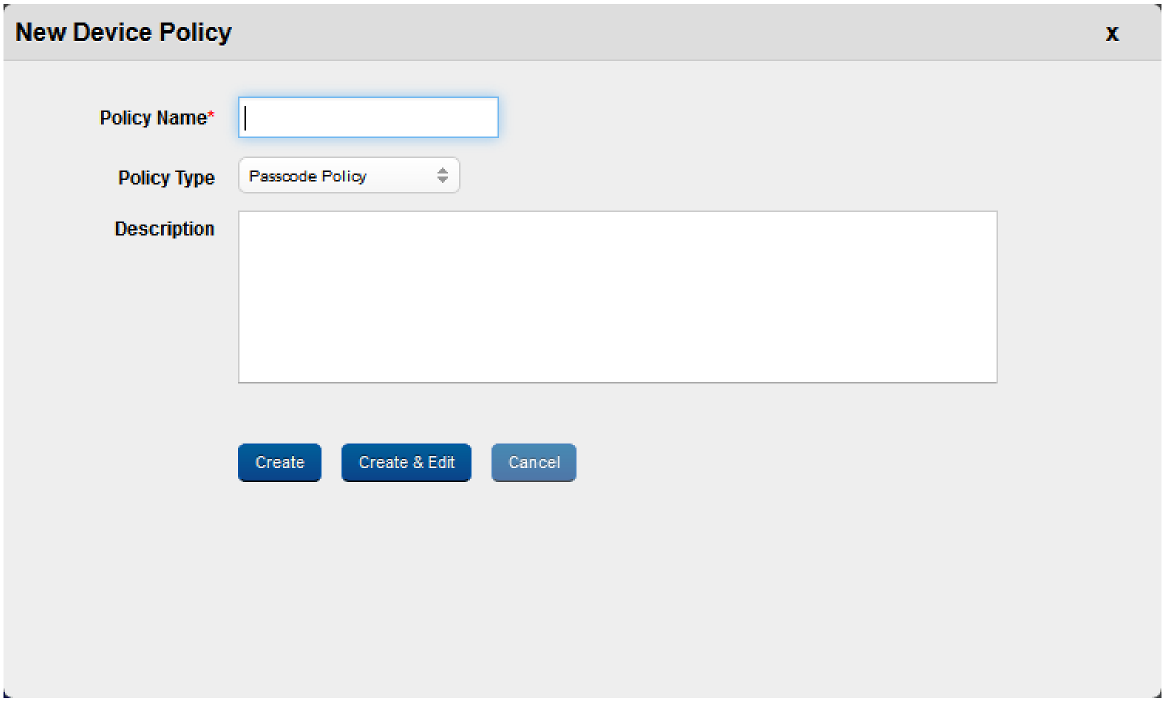
To create a new policy, you need to specify a unique name, type of the policy and an appropriate description for the same.

To create a new Device Policy, follow these steps:

1. To open the **New Device Policy** window, click the **+ Create New Policy** button next to the Device Policy label at the top of the page.

   New **Device Policy window** appears. Enter details for the following fields:

   
   New Device Policy

   Policy Name*

   Policy Type: Passcode Policy

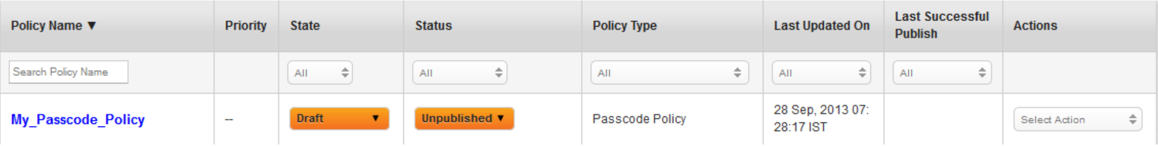
   Description

2. **Policy Name**: Enter a logical name for the device policy.When you create a device policy, it is recommended that you give it a unique name that clearly describes its purpose. If you enter the already existing policy name, system displays the error message.

3. **Policy Type**: Select the required policy type from the drop-down list. By default it is set to Passcode Policy. The policy types are Passcode Policy, Device Restrictions, Email and Calendar, Network, Certificate Distribution, Webclips, App Policy and Compliance Actions. Each device policy comprises rules for all the supported operating systems.

4. **Description**: Enter a precise description for the device policy. The description should accurately describe the features and functionality of your device policy.

5. If you wish to update newly created device policy later, click the **Create** button. The Device Policy is created and the device policy appears in the list view.



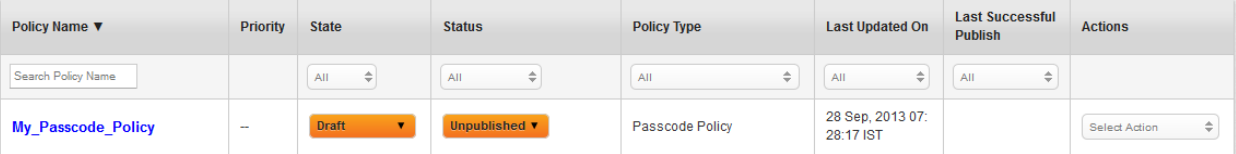
Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
My_Passcode_Policy	--	Draft ▼	Unpublished ▼	Passcode Policy	28 Sep, 2013 07:28:17 IST		Select Action

6. If you wish to update newly created device policy immediately, click the **Create and Edit** button. The newly created Device policy opens into Device Policy Details page. You can define the properties and rules of the Device Policy.
Click the **Cancel** button to close the window.

10.3.2 Publishing a Device Policy

Based on existing business rules, policies are published and then applied to appropriate device sets.

Once a new device policy is created, it is displayed in list view



Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
My_Passcode_Policy	--	Draft ▼	Unpublished ▼	Passcode Policy	28 Sep, 2013 07:28:17 IST		Select Action

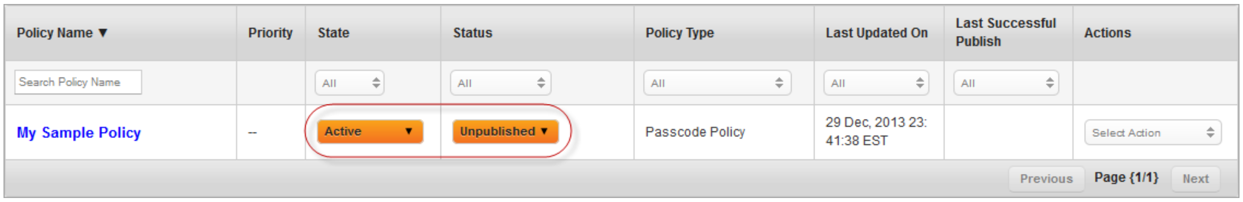
By default, the newly created policy is in Draft mode and the Status is set to Unpublished. As a prerequisite, to make changes in State and Status of a device policy, you should own that device policy.

Device Policy State

State indicates the specific action state set to the device policy. It indicates the type of action that is done or needs to be done to the Device Policy. By default a device policy appears as a draft in list view. Until the Device Policy definition is completed and you submit the same to be active, the state remains as a draft. You review the draft mode and after confirming the details, change the State as Active. Once the State is converted to Active, you can publish the device policy.

Device Policy Status

Status indicates the readiness of the Policy to be used. Policy Status can be Unpublished or Published. When a new device policy is created, the Status is set to Unpublished. Once activated, you can publish the device policy with appropriate permissions.



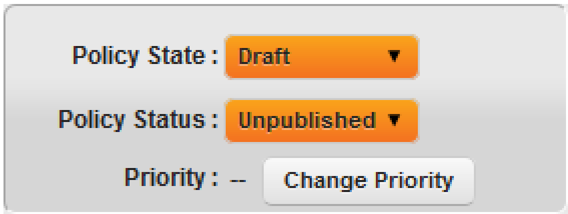
Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
My Sample Policy	--	Active ▼	Unpublished ▼	Passcode Policy	29 Dec, 2013 23:41:38 EST		Select Action

You can change the state and status of the device policy from the list view and also from the device policy details page. You can change the State and Status of the device policy from the list view through options available under State and Status columns.

> ***Note:*** If you face any issues with Internet Explorer 9, See Annexure.

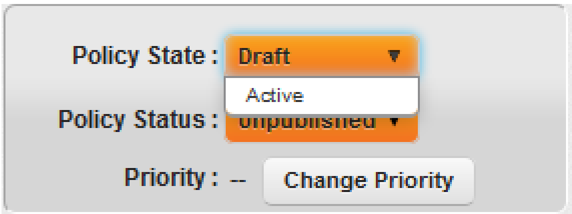
The following procedure explains how to publish a device policy from the device policy details page.

To publish a Device Policy, follow these steps:

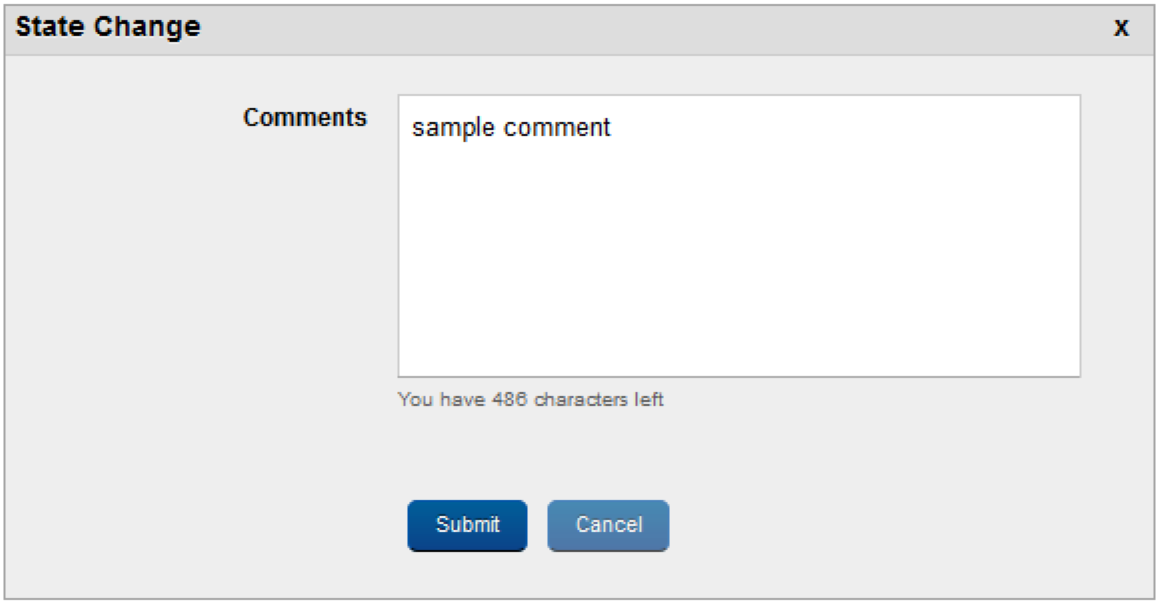


By default, a newly created Device Policy appears in Draft mode.

1. Select the State as Active from the drop-down menu.



The State Change window appears.



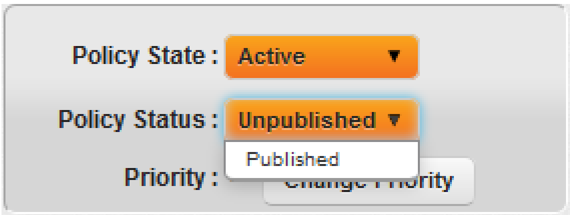
Comments: sample comment

You have 486 characters left

2. Enter a valid comment justifying State Change in the **Comments** box.

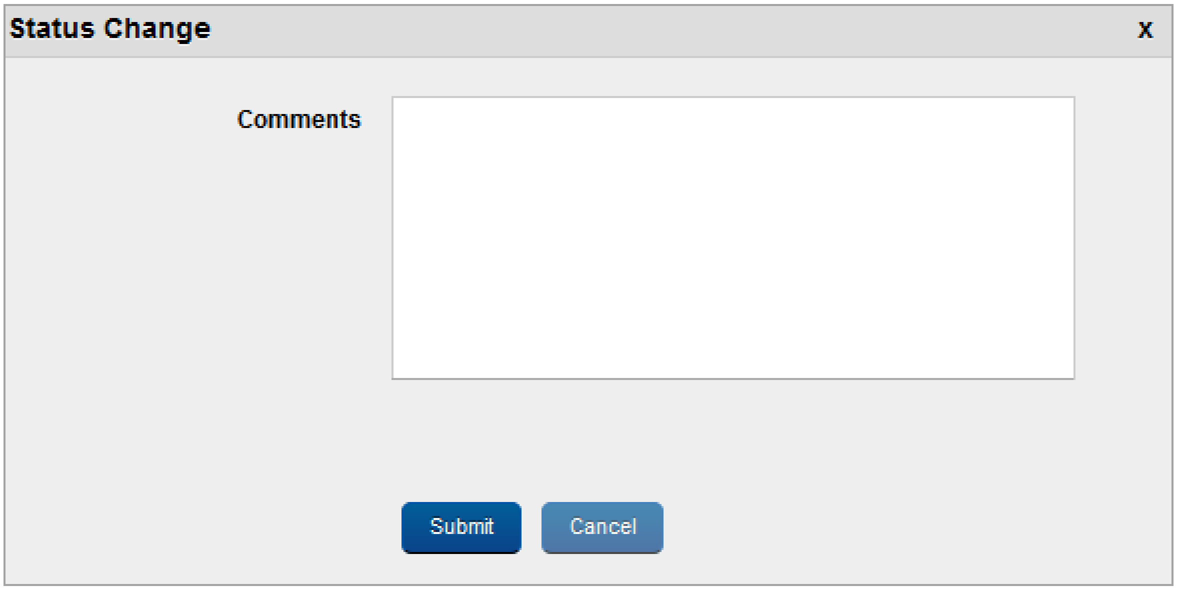
3. Click the **Submit** button to submit the Status change details. In the Confirmation message that appears, click OK to continue.

The State changes to Active.

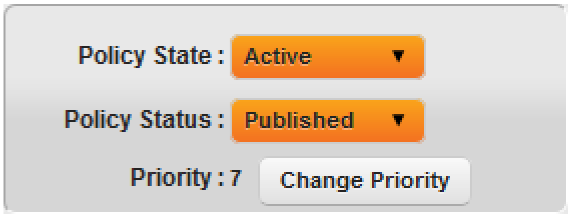


4. To publish the Device Policy, select the Device Policy Status as Published from the drop-down menu.

   Status Change window appears.



5. Enter a valid reason in the **Comments** box justifying publication of the device policy. Click the **Submit** button. In the Confirmation message that appears, click OK to continue.

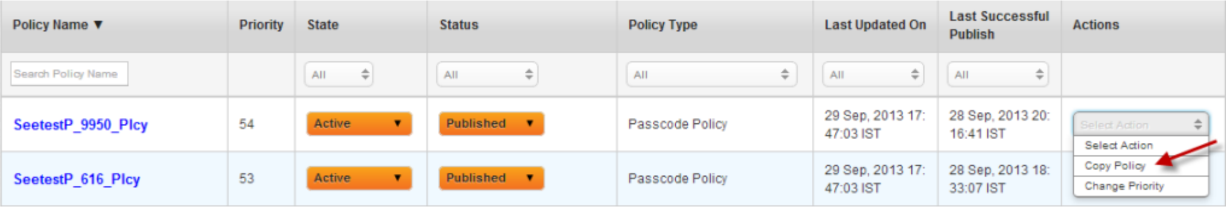


The Policy Status changes to Published.

10.3.3 Copying a Policy

If you wish to build a new device policy with similar conditions applied to an existing device policy, you can copy an existing device policy to create a new device policy.The copied policy comprises all the configurations provided in the parent policy. You can update the copied policy to generate a new policy definition.You also need to rename the copied policy as policy names are unique.

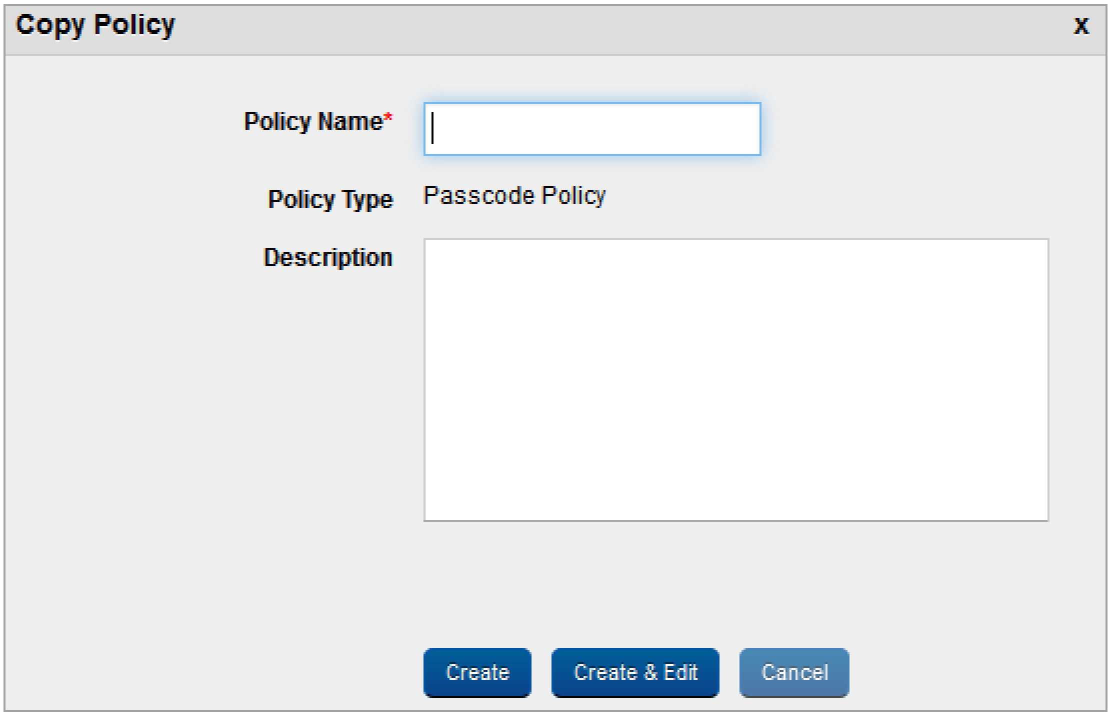
To copy a policy, follow these steps:



Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
SeetestP_9950_Plcy	54	Active ▼	Published ▼	Passcode Policy	29 Sep, 2013 17:47:03 IST	28 Sep, 2013 20:16:41 IST	Select Action Select Action Copy Policy Change Priority
SeetestP_616_Plcy	53	Active ▼	Published ▼	Passcode Policy	29 Sep, 2013 17:47:03 IST	28 Sep, 2013 18:33:07 IST	

1. Select the **Copy Policy** option from the drop-down menu under **Actions** column.

   Copy Policy Window appears. Enter details for the following fields:



2. **Policy Name**: Enter a unique name for the policy.

3. **Description**: Enter a brief and appropriate description for the policy.

4. Click the **Create** button.

   The created policy appears in the list view.

5. Click the **Create and Edit** button to do immediate changes in the policy.

   The newly copied policy is in draft mode and status is set to unpublished.To change the priority of the policy, you need to publish it.

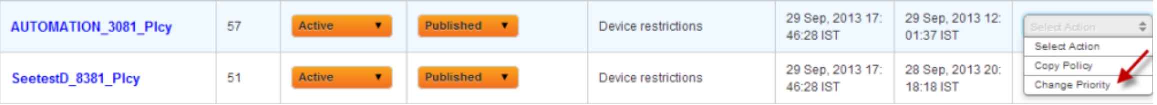
10.3.4 Changing Priority of a Policy

Only one policy can be applied to a device at any point of time. As devices may belong to multiple device sets, there is possibility of several policies are applied to the same device. To resolve this conflict, every policy has a unique Priority value. You must save a policy with a Priority value.Policies with lower Priority value are more important and override policies with higher Priority value, for example, 1>2>3 ...

By default a newly created Policy is given the least priority. You need to change the policy priority to reflect its requirements. No two policies can have the same priority.You can change the priority only of a published policy.

You can change the priority of the policy from the two locations:

- From the List view under Actions column.



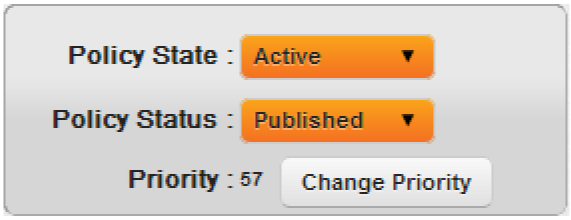
AUTOMATION_3081_Plcy	57	Active ▼	Published ▼	Device restrictions	29 Sep, 2013 17:46:28 IST	29 Sep, 2013 12:01:37 IST	Select Action
SeetestD_8381_Plcy	51	Active ▼	Published ▼	Device restrictions	29 Sep, 2013 17:46:28 IST	28 Sep, 2013 20:18:18 IST	

- From the Policy Details page through the Change Priority button.

The following procedure explains how to change the priority of a device policy from the device policy details page.

To change a policy priority, follow these steps:

1. Click the required policy in the list view to open Policy Details page.

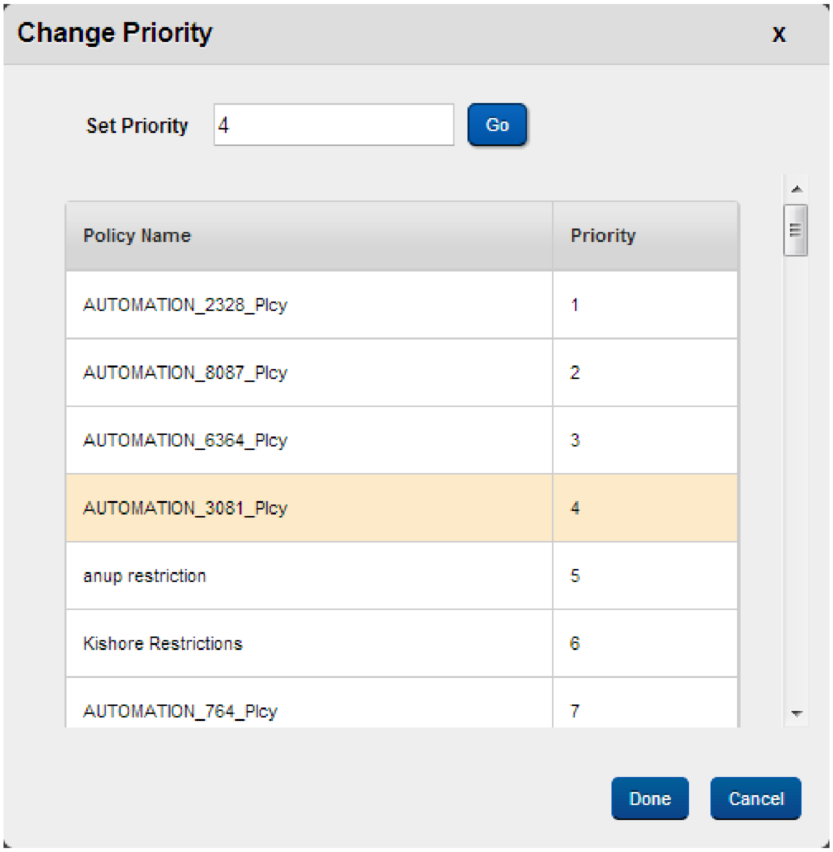


Policy State : Active ▼

Policy Status : Published ▼

Priority : 57

2. Click the **Change Priority** button.



Change Priority

Set Priority: 4

Policy Name	Priority
AUTOMATION_2328_Plcy	1
AUTOMATION_8087_Plcy	2
AUTOMATION_6364_Plcy	3
AUTOMATION_3081_Plcy	4
anup restriction	5
Kishore Restrictions	6
AUTOMATION_764_Plcy	7

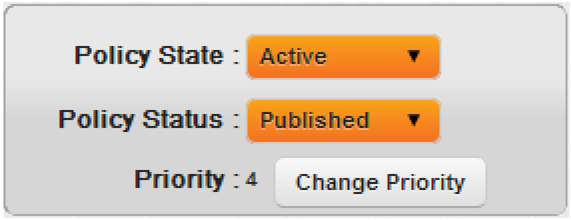
Change Priority Window appears. In current example the system generated priority is set to 57.

3. Enter details for the following fields:

   a. **Set Priority**: Enter a value in **Set Priority** Text field. Click the **Go** button.

      The set priority is highlighted with different color in the list view.

4. Click the **Done** button to submit the priority value. In the Confirmation message that appears, click OK to continue.



Policy State : Active ▼

Policy Status : Published ▼

Priority : 4

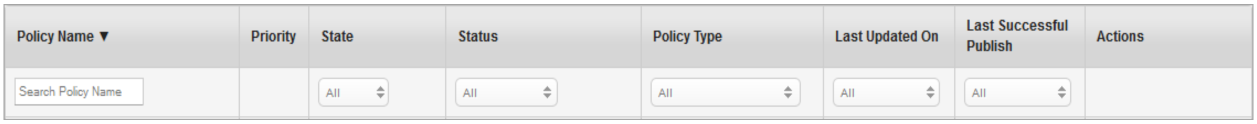
As per set priority, the priority value is set to 4.

5. The changed policy value is reflected in policy details page next to Priority label.

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

10.3.5 Searching for Policies

You can search a desired device 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. To search a device policy, follow these steps:



Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	

1. Enter or select details for the following search filters:
   - **Policy Name**: Enter partial or a complete device policy name in the **Search Policy Name** text field.
   - **Policy Type**: Select the desired policy type from the drop-down list.
   - **Last Updated on**: Select the period when device policy was last updated.
   - **Last Successful Publish**: Select the period when the device policy was last published successfully.

2. According to your search filters criteria, the list view is updated with respective policy details.

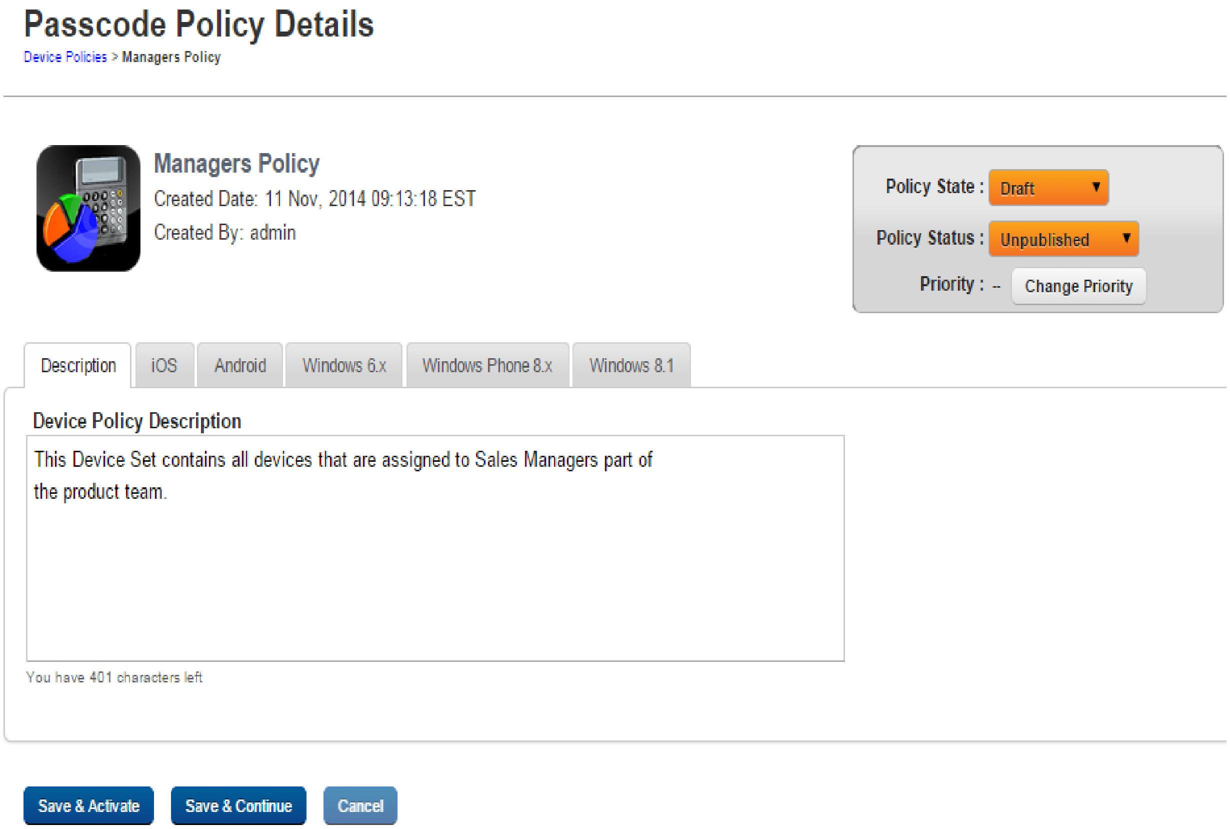
   By default, the list view displays ten policies according to Display settings, which you can modify through the **Display** drop-down list.You can also scroll the list view through **Previous** and the **Next** button.

10.3.6 Updating Policy Details

Based on business rules, an active and published device policy can be applied to a device set. You may also require updating the settings for any or all the supported platforms through device policy details page.

Click the required device policy in list view, which you need to publish. The Device Policy Details page appears with four tabs. By default, Description tab is set to active. Other four tabs pertains to all the supported platforms.

If a limited administrator tries to modify a policy (Edit, Set as Approved/Draft, Publish/Unpublish, and Change Priority) and if the policy is applied to a device set that is not in the administrator's purview, an error alert displays that the administrator does not have permission to modify the policy.



Passcode Policy Details

Device Policies > Managers Policy

Managers Policy

Created Date: 11 Nov, 2014 09:13:18 EST

Created By: admin

Policy State : Draft

Policy Status : Unpublished

Priority : --

Device Policy Description

This Device Set contains all devices that are assigned to Sales Managers part of the product team.

You have 401 characters left

The Device Policy Details Page includes the following screen elements:

Screen Element Properties	Description
Page Title	This is available on extreme right corner on top of the screen, for example, Device Policy Details.
Navigation Link	This link navigates you to main page, for example, click Device Policy>Device Policy Details link to navigate to Device Policy main page.
Priority	This label displays the priority of the policy.
Change Priority	You change priority of the policy through this button.
Policy Status button	You change the policy status through this button.

Screen Element Properties	Description
Policy State button	You change the policy state through this button.
Policy Name	Displays the policy name next to icon.
Created Date	Displays the date and the time when the policy was created.
Created By	Displays name of the Administrator who created the policy.

By default Description, tab is set to active. The other four tabs pertain to each platform supported by the device policy.

To update a device policy, follow these steps:

1. Description: Enter the appropriate description for the device policy or if required, update the existing content
2. Other four tabs pertain to respective platforms, iOS, Android, Window 6.x and Windows 8. According to the selected policy type, tabs for the supported platforms are displayed. If required you may need to update the default settings for specific platforms.

You can specify details for the various policies in Policy Types:

- Passcode Policy
- Device Restrictions Policy
- Email and Calendar Policy
- Network Policy
- Certificate Distribution Policy
- Webclips policy

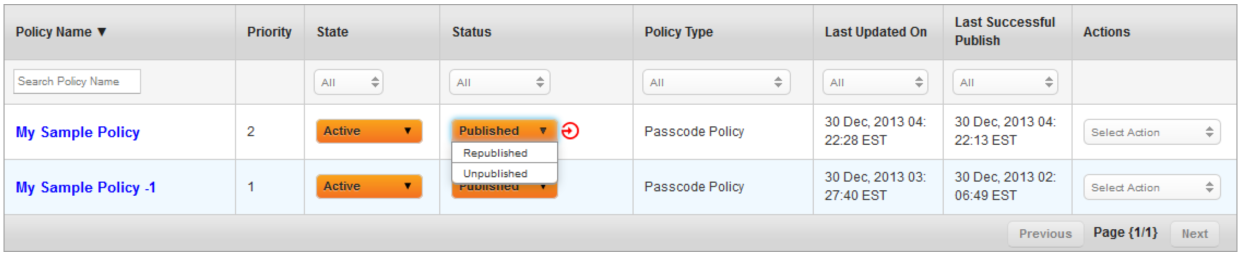
- Public App Policy
- Compliance Actions Policy

10.3.7 Updating Published Device Policy Details

If there are changes to the device policy definition, you may require to update the published device policy. After updating a published policy, 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 device policy.

A stale state icon next to the corresponding device policy status is used to indicate that changes have been made to the definition of the device policy. Once all the active policies are updated and republished, the updates are pushed to all the active devices. For iOS, the updated Profile is pushed. For Android, the new update is conveyed to the Device Agent.

The state must be changed to active and published again for the changes to take effect. You can update the published device policies from the list view and also from the device policy details page.

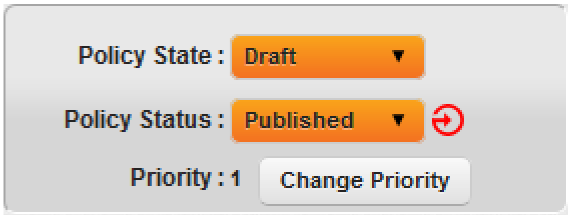


Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	All	All	All	All	
My Sample Policy	2	Active ▼	Published ▼ Republished Unpublished	Passcode Policy	30 Dec, 2013 04:22:28 EST	30 Dec, 2013 04:22:13 EST	Select Action
My Sample Policy -1	1	Active ▼	Published ▼	Passcode Policy	30 Dec, 2013 03:27:40 EST	30 Dec, 2013 02:06:49 EST	Select Action

In List view, you need to select the Republished option under Status column.

The following procedure explains how to update a published device policy from the device policy details page.

To republish a Device Policy, follow these steps:

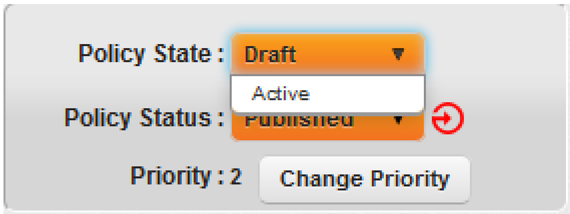


Policy State : Draft

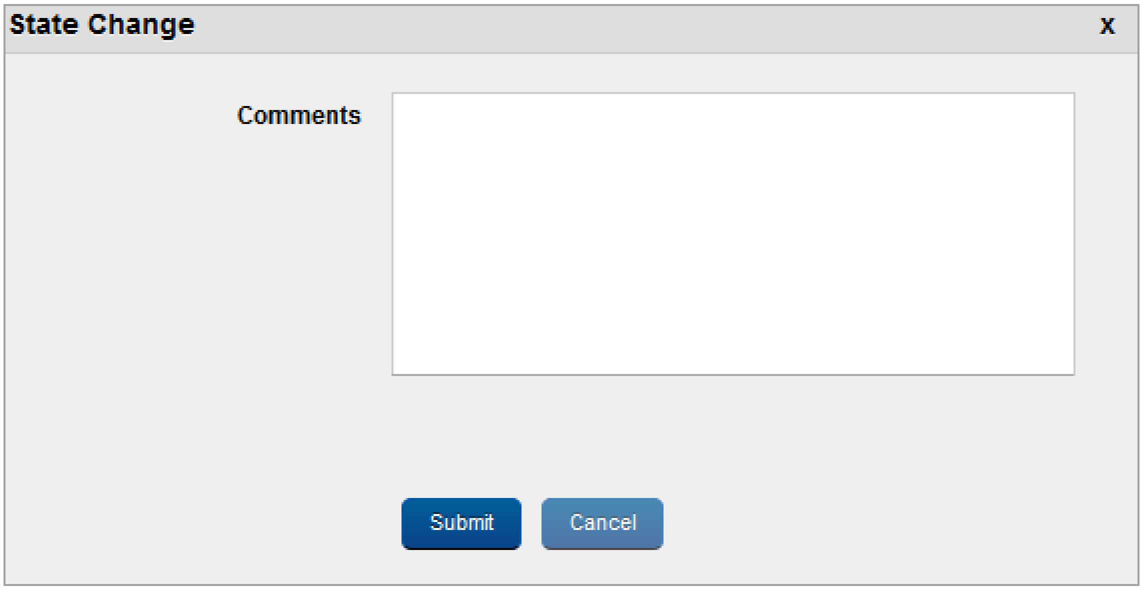
Policy Status : Published

Priority : 1

Currently the device state is changed to Draft state.



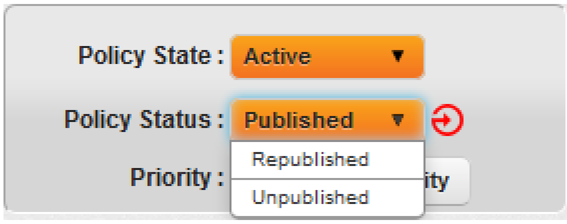
1. Select the device state as Active from the dropdown list.



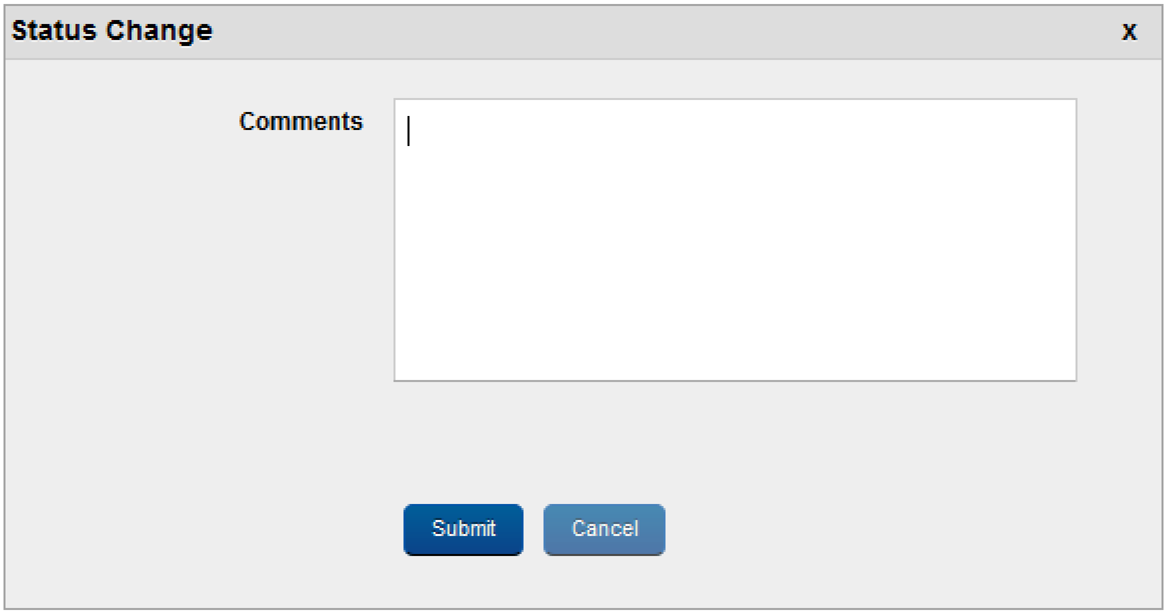
State Change window appears.

2. Enter a valid reason for state change in the **Comments** text box.

3. In the confirmation (State Change) message that appears, click OK to continue. The policy state changes to active.



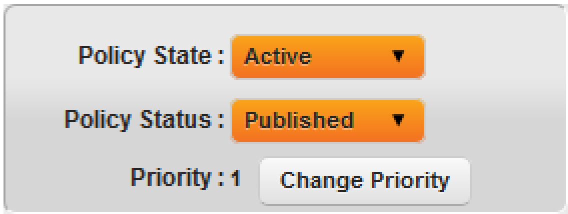
4. Select the policy Status as **Republished** from the drop-down menu.



Status Change Window appears.

5. Enter a valid reason for status change in the **Comments** text box.

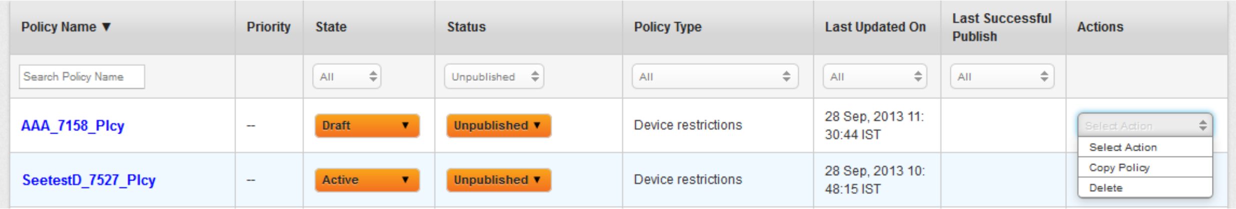
6. Click the **Submit** button to submit the status change details. In the confirmation (Status Change) message that appears, click OK to continue.


Policy State : Active
Policy Status : Published
Priority : 1

The Status changes to Published.

10.3.8 Deleting a Policy

You can delete only Unpublished Device policies. Once a device policy is deleted, it is removed from the Device Policy list.



Policy Name ▼	Priority	State	Status	Policy Type	Last Updated On	Last Successful Publish	Actions
Search Policy Name		All	Unpublished	All	All	All	
AAA_7158_Plcy	--	Draft ▼	Unpublished ▼	Device restrictions	28 Sep, 2013 11:30:44 IST		Select Action
SeetestD_7527_Plcy	--	Active ▼	Unpublished ▼	Device restrictions	28 Sep, 2013 10:48:15 IST		

To delete a device policy, follow these steps:

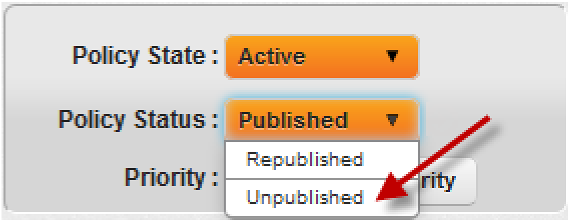
1. To delete the required Device Policy, click the **Delete** option under the **Actions** column.
2. In the confirmation message that appears, click Yes to continue.
3. The system displays the Delete Policy confirmation message. Click OK to continue.

   The Policy is no longer displayed in the list view.

10.3.9 Unpublishing a Policy

Unpublishing a Device Policy signifies that Policy is deactivated and its rules are no longer applicable to any device. Prior to unpublishing a device policy, it must be ensured that it is not applied to any device set.

To unpublish a Device Policy, follow these steps:



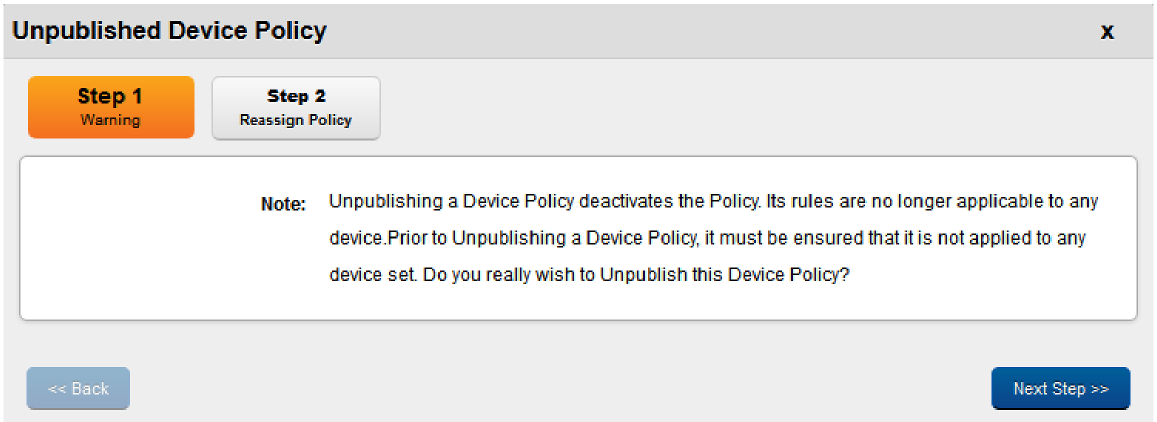
Policy State : Active ▼

Policy Status : Published ▼

Priority :

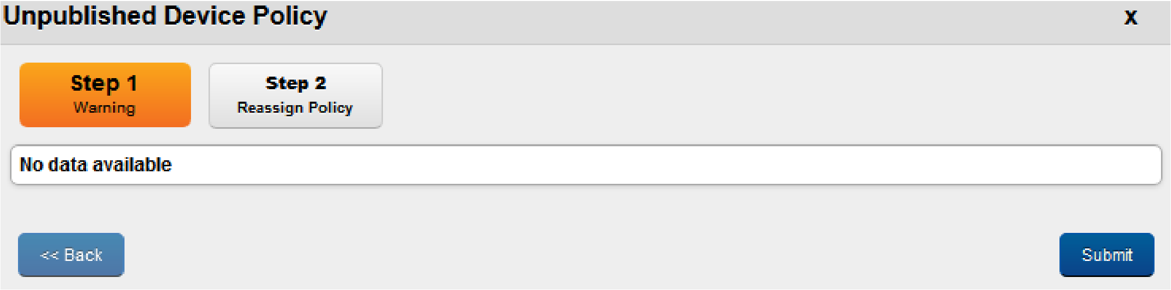
1. To unpublish a Device Policy, select the Status as Unpublished from the drop-down menu.

   Unpublished Device Policy window appears with a warning message.


Unpublished Device Policy

Note: Unpublishing a Device Policy deactivates the Policy. Its rules are no longer applicable to any device.Prior to Unpublishing a Device Policy, it must be ensured that it is not applied to any device set. Do you really wish to Unpublish this Device Policy?

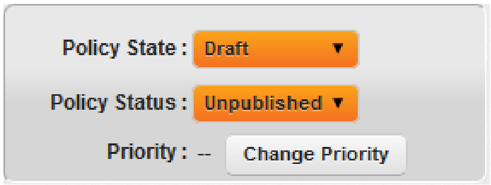
2. If the policy is not applied to any device set, click the **Next Step** button.


Unpublished Device Policy

No data available

Step Two - Reassign Policy window appears.

3. Click the Submit button. In the confirmation message (Unpublish Policy) that appears, click **OK** to continue.


Policy State : Draft

Policy Status : Unpublished

Priority : --

The Policy Status changes to Unpublished.

10.4 Policy Types

This section details about EMM supported policy types, settings for each of the policies.

10.4.1 Introduction

For Android, EMM policies are defined in two categories as follows:

- Stock Android Policies
- SAFE Policies

The following table provides information on policies applicable on different platforms.

MDM Policies	iOS	Android	Windows Phone 8.x	Windows Phone 8	Windows 8.1
Passcode Policy	Yes	Yes	Yes	Yes	Yes
Device Restrictions	Yes	Yes	Yes	Yes	Yes
Email and Calendar	Yes	Yes	Yes	Yes	No
Network	Yes	Yes	Yes	No	No
Certificate Distribution	Yes	Yes	Yes	No	No
Web Clips	Yes	No	No	No	No
Compliance Actions	Yes	Yes	No (Not required)	No	No
Public Apps	Yes	Yes	Yes	No	No

MDM Policies	iOS	Android	Windows Phone 8.x	Windows Phone 8	Windows 8.1
Others	Yes	No	No	No	No

10.4.1.1 Stock Android Policies

Stock Android policies are available by default in EMM. The Stock Android policies can be created for all device sets, and can be applied to Android devices.

10.4.1.2 SAFE Policies

Samsung For Enterprise (SAFE) is an inbuilt software feature provided by Samsung for devices it manufactures. Samsung devices enabled with SAFE are targeted to meet specific enterprise level management and security benchmarks.

Users can access these features on SAFE devices:

- Enhanced support for Microsoft Exchange ActiveSync
- VPN connectivity
- On-device encryption using the 256-bit Advanced Encryption Standard
- Mobile Device Management (MDM) component

SAFE is an extension of the device capabilities that are handled the same way as in Kony EMM.

In case of SAFE even if control is removed, SAFE licenses and polices remain active on the device. The user must also delete enterprise store to remove SAFE license on the device. Even after the Enterprise Store is deleted, some settings will remain on the device, such as:

- SAFE exchange email policy
- APN Settings
- VPN settings
- Certificates

Once a SAFE license is accepted on a device, the license cannot be revoked from the server:

- To remove a SAFE larcenist user must delete enterprise store.
- To remove SAFE policies, a device must be enterprise wiped.
- For any residual actions that were performed on a device through Device Details, enterprise store needs to be removed.

10.4.1.3 SAFE Compliant Devices

EMM supports SAFE devices from Android OS V 4.2+ (SAFE Version 4.0 and later)

The following devices are supported with SAFE:

- Galaxy Note 3
- Galaxy Note 4
- Galaxy S4
- Galaxy Note 10.1 2014 Edition
- Galaxy Note 8
- Galaxy Tab 3 10.1
- Galaxy Note 2
- Galaxy S3
- Galaxy Note 10.1

For an updated list of devices supported with SAFE, refer to the Samsung site.

10.4.1.4 SAFE License

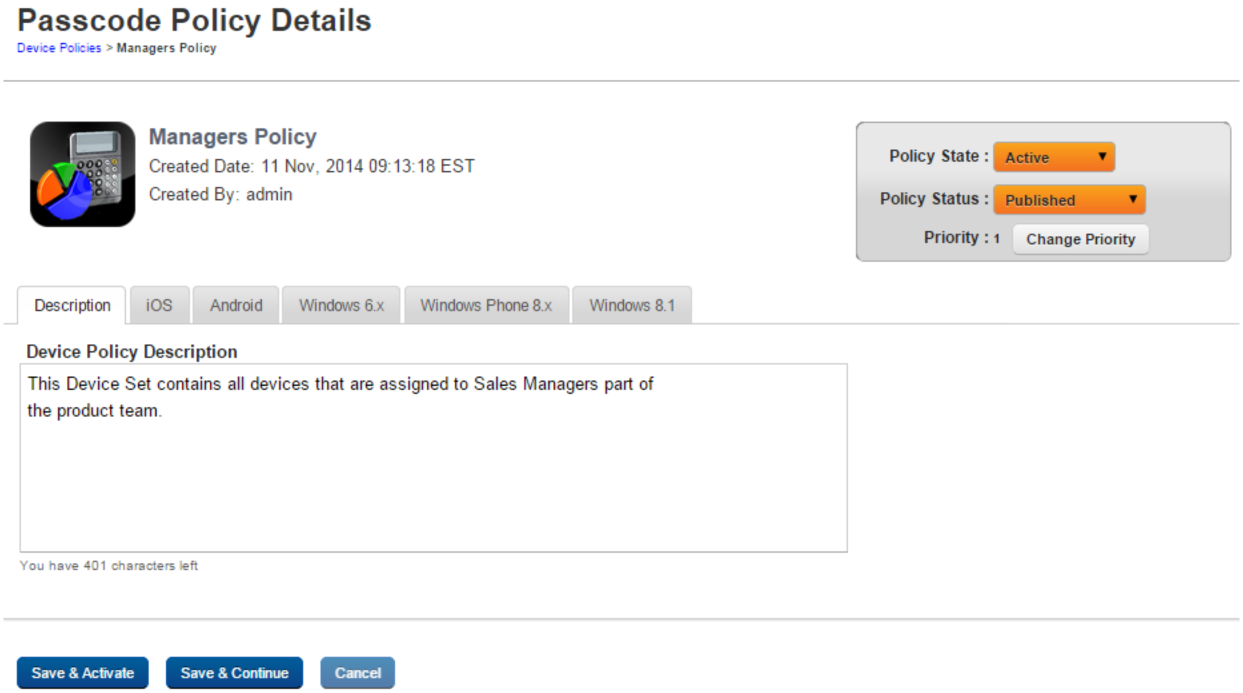
A license activates SAFE on a device. SAFE license activation occurs when a SAFE device with MDM Version >=4.0 or later is enrolled.

In order to implement SAFE (for Samsung Android 4.2) in EMM, the following necessary configurations need to be done in the EMM console. You can specify details for the following policy types:

- Passcode Policy
- Device Restrictions Policy
- Email and Calendar Policy
- Network Policy
- Certificate Distribution Policy
- Webclips Policy
- Public App Policy
- Compliance Actions Policy
- Others Policy

10.4.2 Passcode Policy

The primary purpose of the Passcode policy is to authenticate users and ensure data safety. Based on business rules, the Passcode policy is defined for all the supporting platforms.



Passcode Policy Details

Device Policies > Managers Policy

Managers Policy

Created Date: 11 Nov, 2014 09:13:18 EST

Created By: admin

Policy State : Active

Policy Status : Published

Priority : 1

Device Policy Description

This Device Set contains all devices that are assigned to Sales Managers part of the product team.

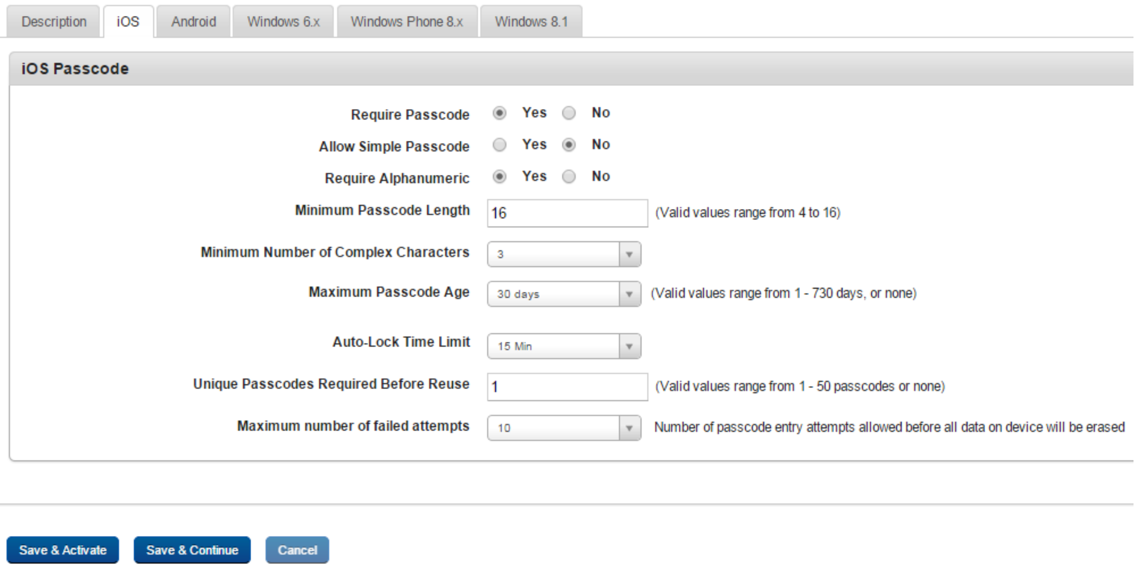
You have 401 characters left

You can set passcode priorities for the following operating systems.

- Set Passcode Policy for iOS
- Set Passcode Policy for Android
- Set Passcode Policy for Windows 6.x
- Set Passcode Policy for Windows Phone 8.x
- Set Passcode Policy for Windows 8.1

10.4.2.1 Set Passcode Policy for iOS

1. To set passcode policy for iOS, fill the following fields:



iOS Passcode

Require Passcode ● Yes ○ No

Allow Simple Passcode ○ Yes ● No

Require Alphanumeric ● Yes ○ No

Minimum Passcode Length 16 (Valid values range from 4 to 16)

Minimum Number of Complex Characters 3

Maximum Passcode Age 30 days (Valid values range from 1 - 730 days, or none)

Auto-Lock Time Limit 15 Min

Unique Passcodes Required Before Reuse 1 (Valid values range from 1 - 50 passcodes or none)

Maximum number of failed attempts 10 Number of passcode entry attempts allowed before all data on device will be erased

a. **Require Passcode**: By default, this option is set to No. You can modify it to Yes. If this option is set to No, then no device passcode is required.

   If you select Yes, the remaining fields become active. You can enter details and select the options for the following fields.

b. **Allow Simple Passcode**: By default, this option is set to Yes. You can modify it to No. If you select No, then **Minimum Number of Complex Characters** field is activated.

   Select the required number of complex characters from the drop-down list.

c. **Require Alphanumeric**: By default, this option is set to No. You can modify it to Yes.

   This setting requires that a password contain numeric and non-numeric characters.

d. **Minimum Passcode Length**: Set the passcode length. The passcode length can be between four to 16 characters.

e. **Minimum Number of Complex Characters**: Set the minimum number of complex characters limit. You can set the limit upto 3.

f. **Maximum Passcode Age**: Select the maximum passcode age from the drop-down list. The default value is 30 days, which you can modify up to 730 days.

g. **Auto-lock Time Limit**: Select the appropriate auto-lock time limit from the drop-down list.

   This field specifies the period (in minutes) for which an auto-lock time limit is enforced.

h. **Unique Passcodes Required before Reuse**: This security setting defines the number of times a passcode can be reused. Select the required value from the drop-down list.

i. **Maximum number of failed attempts:** Select the limit for invalid password attempts from the drop-down list.

   If the limit is crossed, the OS automatically does a factory reset of the device. As this is not communicated to the EMM server, the status remains as enrolled. The device cannot be enrolled with any other user unless the status is changed manually by issuing a wipe command to the device. The same user can re-enroll the device.

2. Click the **Save and Continue** button to save the data and stay on the same page to update other details immediately.

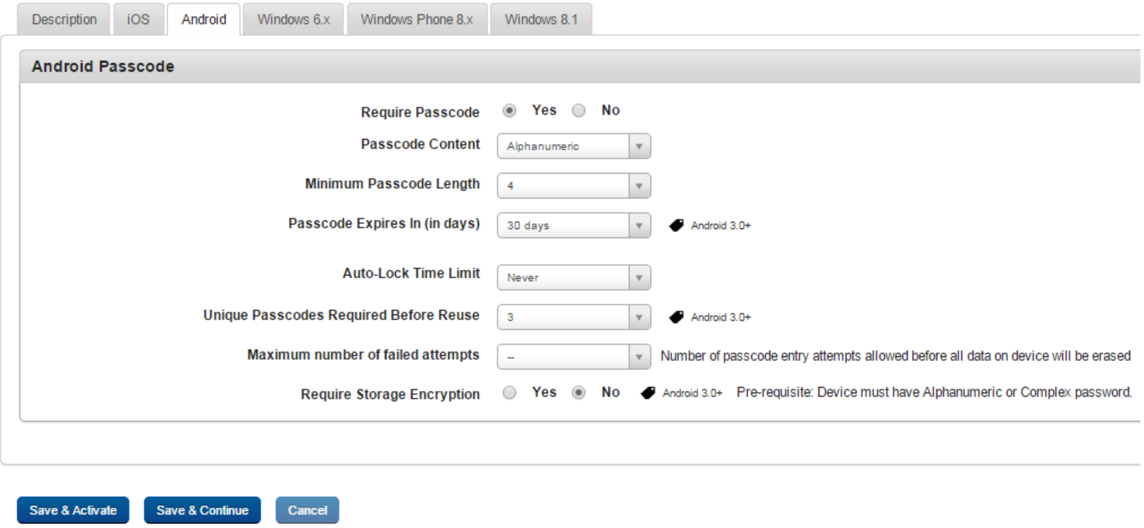
3. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

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

   > ***Important:*** For iOS devices, the passcode policy is in sync with the carrier time. If the device is not synced with NTP, someone could tamper with the device's date and time. This would affect the passcode enforcement as there could be a difference between device time and carrier time.

10.4.2.2 Set Passcode Policy for Android

1. To set passcode policy for Android, complete these fields:



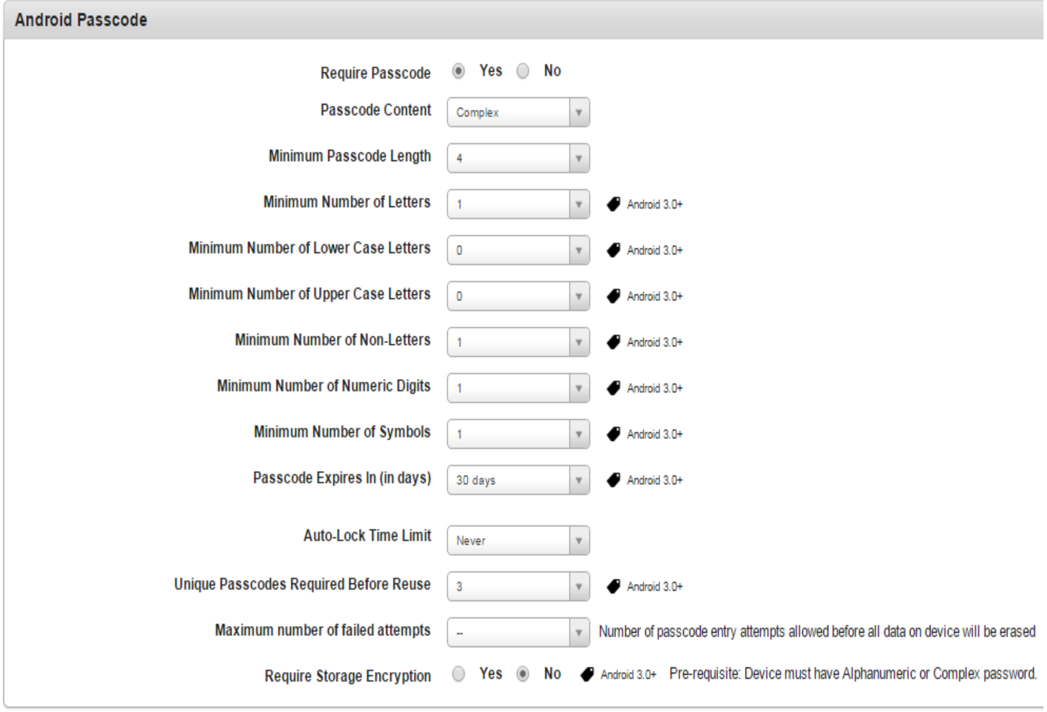
Android Passcode

Require Passcode	● Yes ○ No
Passcode Content	Alphanumeric
Minimum Passcode Length	4
Passcode Expires In (in days)	30 days · Android 3.0+
Auto-Lock Time Limit	Never
Unique Passcodes Required Before Reuse	3 · Android 3.0+
Maximum number of failed attempts	-- · Number of passcode entry attempts allowed before all data on device will be erased
Require Storage Encryption	○ Yes ● No · Android 3.0+ · Pre-requisite: Device must have Alphanumeric or Complex password.

   a. **Require Passcode**: By default, this option is set to Yes. You can modify it to No.

   b. **Passcode Content**: Based on the selected option from the dropdown list, required entry fields are displayed. If you select the option as numeric, alphanumeric, or alphabetic then **Minimum Passcode length** field is displayed. Select the required minimum passcode length from the drop-down list.

      If you select the option as **Complex** from the dropdown list, following fields supporting complex passcode appears. Select appropriate options:



Android Passcode

Require Passcode	● Yes ○ No	
Passcode Content	Complex	
Minimum Passcode Length	4	
Minimum Number of Letters	1	Android 3.0+
Minimum Number of Lower Case Letters	0	Android 3.0+
Minimum Number of Upper Case Letters	0	Android 3.0+
Minimum Number of Non-Letters	1	Android 3.0+
Minimum Number of Numeric Digits	1	Android 3.0+
Minimum Number of Symbols	1	Android 3.0+
Passcode Expires In (in days)	30 days	Android 3.0+
Auto-Lock Time Limit	Never	
Unique Passcodes Required Before Reuse	3	Android 3.0+
Maximum number of failed attempts	--	Number of passcode entry attempts allowed before all data on device will be erased
Require Storage Encryption	○ Yes ● No	Android 3.0+ Pre-requisite: Device must have Alphanumeric or Complex password.

i. Minimum Passcode Length: Select the minimum passcode length to define a complex passcode from the drop-down list.

ii. Minimum Number of Letters: Select the minimum number of letters to define a complex passcode from the drop-down list.

iii. Minimum Number of Lowercase Letters: Select the minimum number of lowercase letters to define a complex passcode from the drop-down list.

iv. Minimum Number of Uppercase Letters: Select the minimum number of uppercase letters to define a complex passcode from the drop-down list.

v. Minimum Number of Non-Letters: Select the minimum number of non- letters to define a complex passcode from the drop-down list.

vi. Minimum Number of Numeric Digits: Select the minimum number of numeric digits to define a complex passcode from the drop-down list.

vii. Minimum Number of Symbols: Select the minimum number of symbols to define a complex passcode from the drop-down list.

viii. Passcode Expires In (in Days): Select the number of days to define maximum passcode age from the drop-down list.

ix. Auto-lock Time Limit: Select the time limit (in minutes) to define maximum passcode age from the dropdown list. This field specifies the period (in minutes) for which an auto-lock time limit is enforced.

x. Unique Passcode required Before Reuse: This security setting defines the number of times a password can be reused. Select the required value from the drop-down list.

xi. Maximum number of failed attempts: Select the limit for invalid password attempts from the drop-down list.

xii. Require Storage Encryption: By default, this option is set to No. You can modify it to Yes. Storage encryption is the conversion of data into a coded form to secure data.

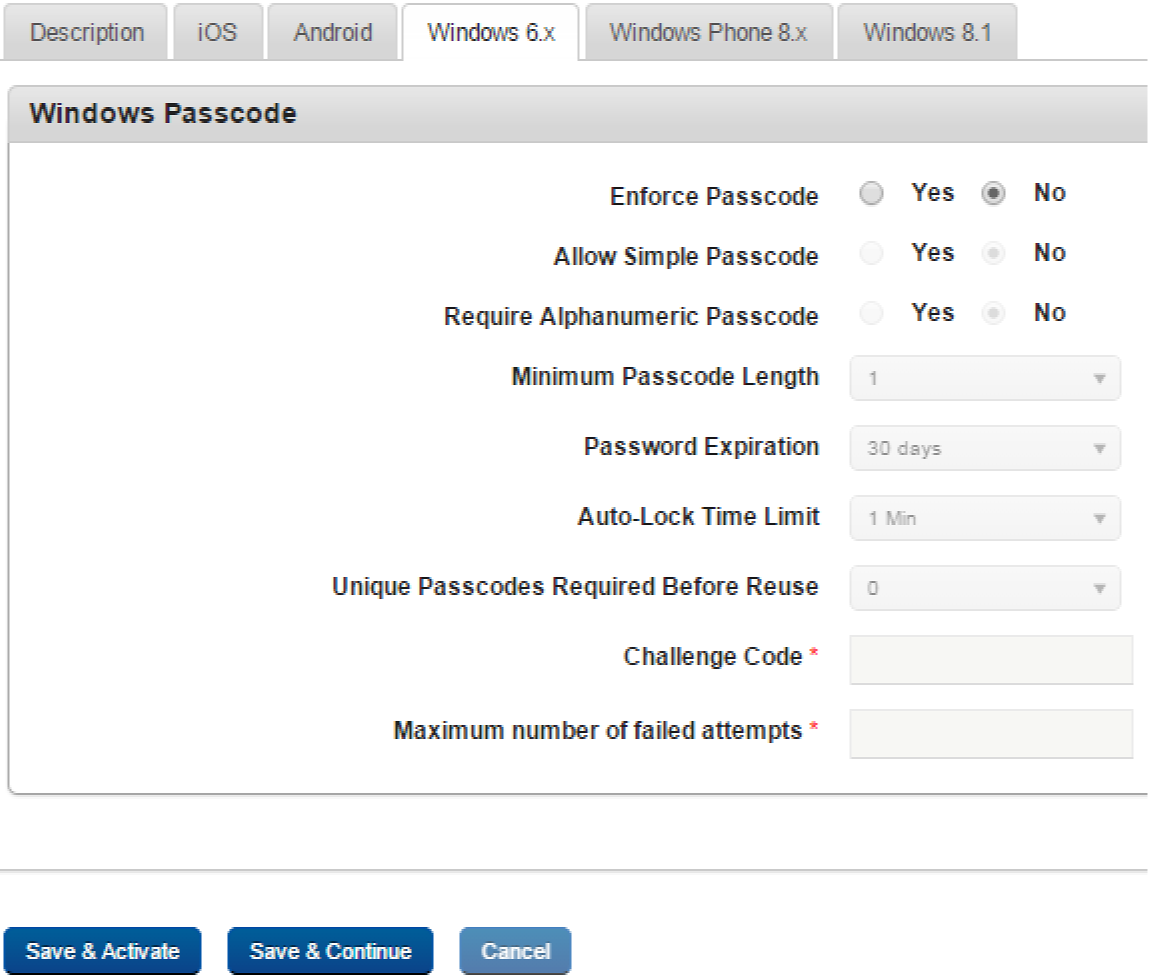
2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

> ***Important:*** The Sony Ericsson ST15i AOS 4.0.4 and the HTC Sense (Android 4.0.3 Platform only) cannot handle complex passcode settings.
> If a user tries to set a complex passcode policy on the Sony Ericsson ST15i AOS 4.0.4, a "Settings has stopped" message will be displayed.
> If a user tries to set a complex passcode policy on the HTC Sense, the device will only display a numeric keypad.

10.4.2.3 Set Passcode Policy for Windows 6.x

1. To set passcode policy for Windows 6.x, follow these steps:



Windows Passcode

Enforce Passcode	○ Yes ● No
Allow Simple Passcode	○ Yes ● No
Require Alphanumeric Passcode	○ Yes ● No
Minimum Passcode Length	1
Password Expiration	30 days
Auto-Lock Time Limit	1 Min
Unique Passcodes Required Before Reuse	0
Challenge Code *	
Maximum number of failed attempts *	

a. **Enforce Passcode**: By default, this option is set to No. You can modify it to Yes. If you select the option as Yes, all the remaining fields become active, and you can enter details and select the options.

b. **Allow Simple Passcode**: By default, this option is set to No. You can modify it to Yes.

c. **Require Alphanumeric Passcode**: By default, this option is set to No. You can modify it to Yes.

d. **Minimum Passcode Length**: Select the minimum number from the drop-down list. By default, it is set to six.

e. **Password Expiration**: Select the number of days for passcode life time from the drop-down menu. By default, it is set to 30 days.

f. **Auto Lock Time Limit:** Select the auto-lock time limit from the drop-down menu. By default, it is set to 1 minute.

   After the time passes, the account becomes locked.

g. **Unique Passcode Required Before Reuse**: Select the limit for Passcode reuse from the drop-down menu.

h. **Challenge Code:** Enter the unique Challenge Code to access the application after failed log in attempts in the text field. This security setting ensures that after a certain number of failed flocking attempts, system prompts the user to enter the Challenge code to access the application. If the user fails to enter the challenge code, then application is locked.

i. **Maximum Number of Failed Attempts**: Enter the limit for password attempts. If the limit is crossed, the OS automatically does a factory reset of the device. As this is not communicated to the EMM server, the status remains as enrolled. The device cannot be enrolled with any other user unless the status is changed manually by issuing a wipe command to the device. The same user can re-enroll the device.

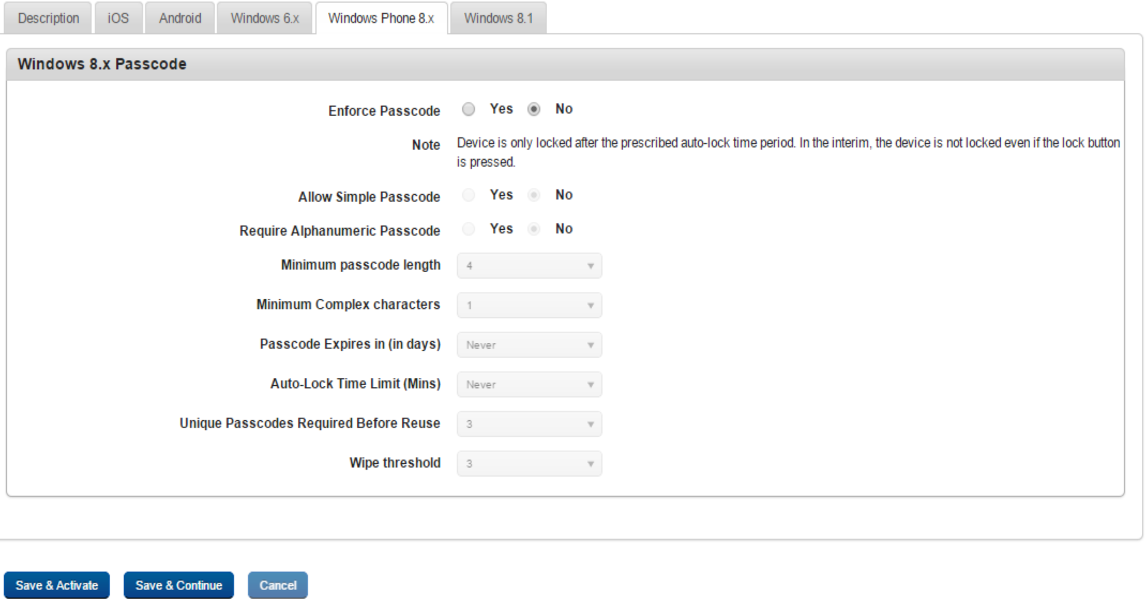
2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.2.4 Set Passcode Policy for Windows Phone 8.x

1. To set passcode policy for Windows 8, follow these steps:



Windows 8.x Passcode

Enforce Passcode ○ Yes ● No

Note Device is only locked after the prescribed auto-lock time period. In the interim, the device is not locked even if the lock button is pressed.

Allow Simple Passcode ○ Yes ○ No

Require Alphanumeric Passcode ○ Yes ○ No

Minimum passcode length 4

Minimum Complex characters 1

Passcode Expires in (in days) Never

Auto-Lock Time Limit (Mins) Never

Unique Passcodes Required Before Reuse 3

Wipe threshold 3

a. **Enforce Passcode**: By default, this option is set to No. You can modify it to Yes. If you select the option as Yes, all the remaining fields become active, and you can enter details and select the options.

b. **Allow Simple Passcode**: By default, this option is set to No. You can modify it to Yes.

c. Require Alphanumeric Passcode: By default, this option is set to No. You can modify it to Yes.

d. **Minimum Passcode Length**: Select the minimum passcode length from the drop-down list.

e. **Password Expiration in Days**: Enter the number of days after that passcode expires.

f. **Maximum Auto Lock Time Limit (mins)**: Enter the maximum auto-lock time limit in the text field.

g. **Unique Passcode Required Before Reuse**: Enter the number of times a passcode can be reused.

h. **Wipe Threshold**: Enter the limit for invalid password attempts in the text field.

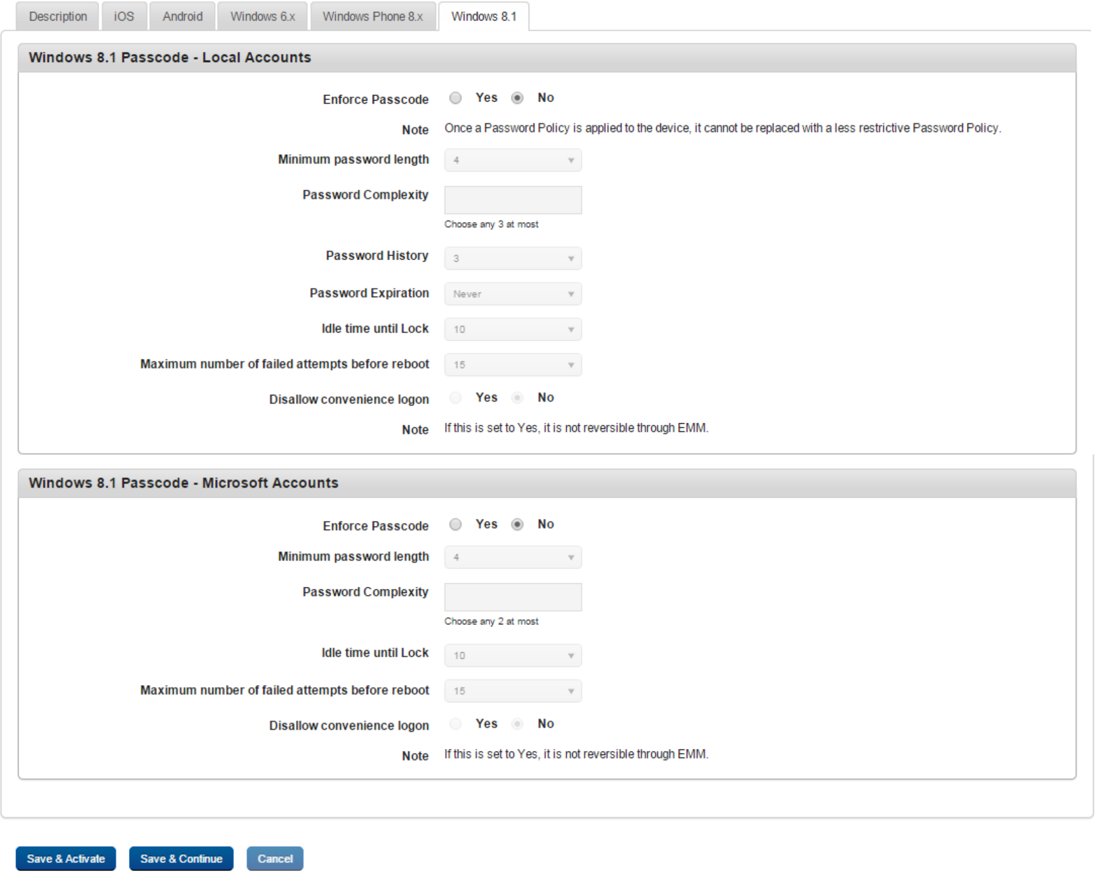
   If the limit is crossed, the OS automatically does a factory reset of the device. As this is not communicated to the EMM server, the status remains as enrolled. The device cannot be enrolled with any other user unless the status is changed manually by issuing a wipe command to the device. The same user can re-enroll the device.

2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.2.5 Set Passcode Policy for Windows 8.1

1. To set the passcode policy for Windows 8.1, follow these steps:



Windows 8.1 Passcode - Local Accounts

Enforce Passcode ○ Yes ● No

Note Once a Password Policy is applied to the device, it cannot be replaced with a less restrictive Password Policy.

Minimum password length 4

Password Complexity

Choose any 3 at most

Password History 3

Password Expiration Never

Idle time until Lock 10

Maximum number of failed attempts before reboot 15

Disallow convenience logon ○ Yes ● No

Note If this is set to Yes, it is not reversible through EMM.

Windows 8.1 Passcode - Microsoft Accounts

Enforce Passcode ○ Yes ● No

Minimum password length 4

Password Complexity

Choose any 2 at most

Idle time until Lock 10

Maximum number of failed attempts before reboot 15

Disallow convenience logon ○ Yes ● No

Note If this is set to Yes, it is not reversible through EMM.

Windows 8.1 Passcode - Local Accounts

a. **Enforce Passcode**: By default, this option is set to **No**. You can modify it to **Yes**. If you select the option as Yes, all remaining fields become active. You can enter details and select the options.

b. **Minimum password length**: Set the minimum length of the password from the drop-down list.

c. **Password History**: Select the password history from the drop-down list.

d. **Password Expiration**: Enter the number of days until the passcode expires.

e. **Idle time until Lock**: Enter the number of days until the passcode expires.

f. **Maximum number of failed attempts before reboot**: Set the maximum number of attempts a user can make before rebooting the device.

Windows 8.1 Passcode - Microsoft Accounts

a. **Enforce Passcode**: By default, this option is set to No. You can modify it to Yes. If you select the option as Yes, all remaining fields become active. You can enter details and select the options.

b. **Minimum Passcode Length**: Select the minimum passcode length from the drop-down list.

c. **Idle time until Lock**: Enter the number of days after that passcode expires.

d. **Maximum number of failed attempts before reboot**: Set the maximum number of attempts a user can make before rebooting the device.

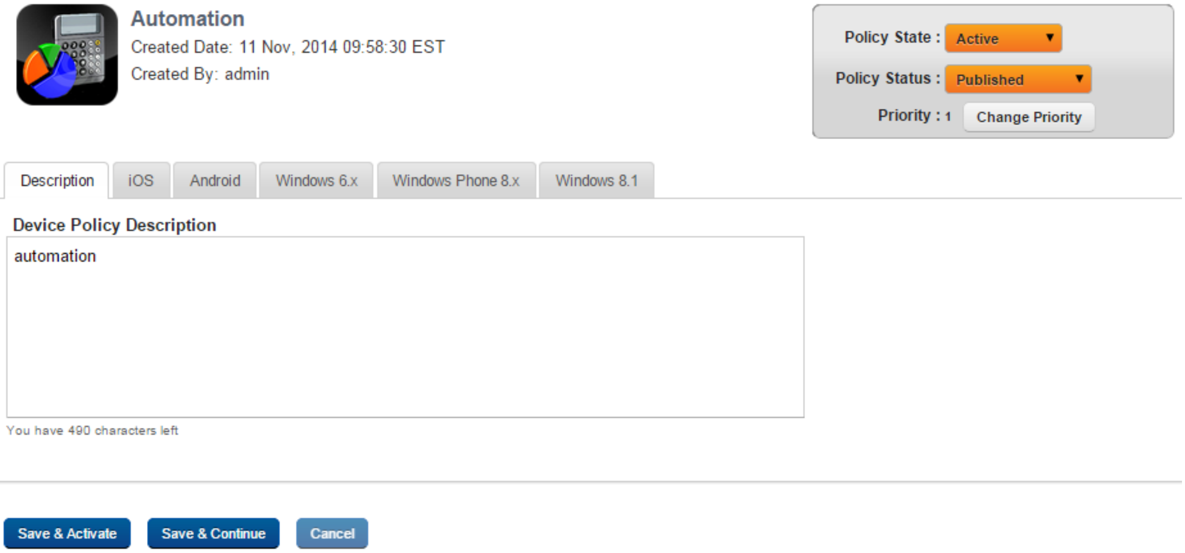
2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.3 Device Restrictions Policy

The primary purpose of the Device Restriction policy is to control approved devices to protect the device data and restrict unapproved features and applications.



Device Policy Description

automation

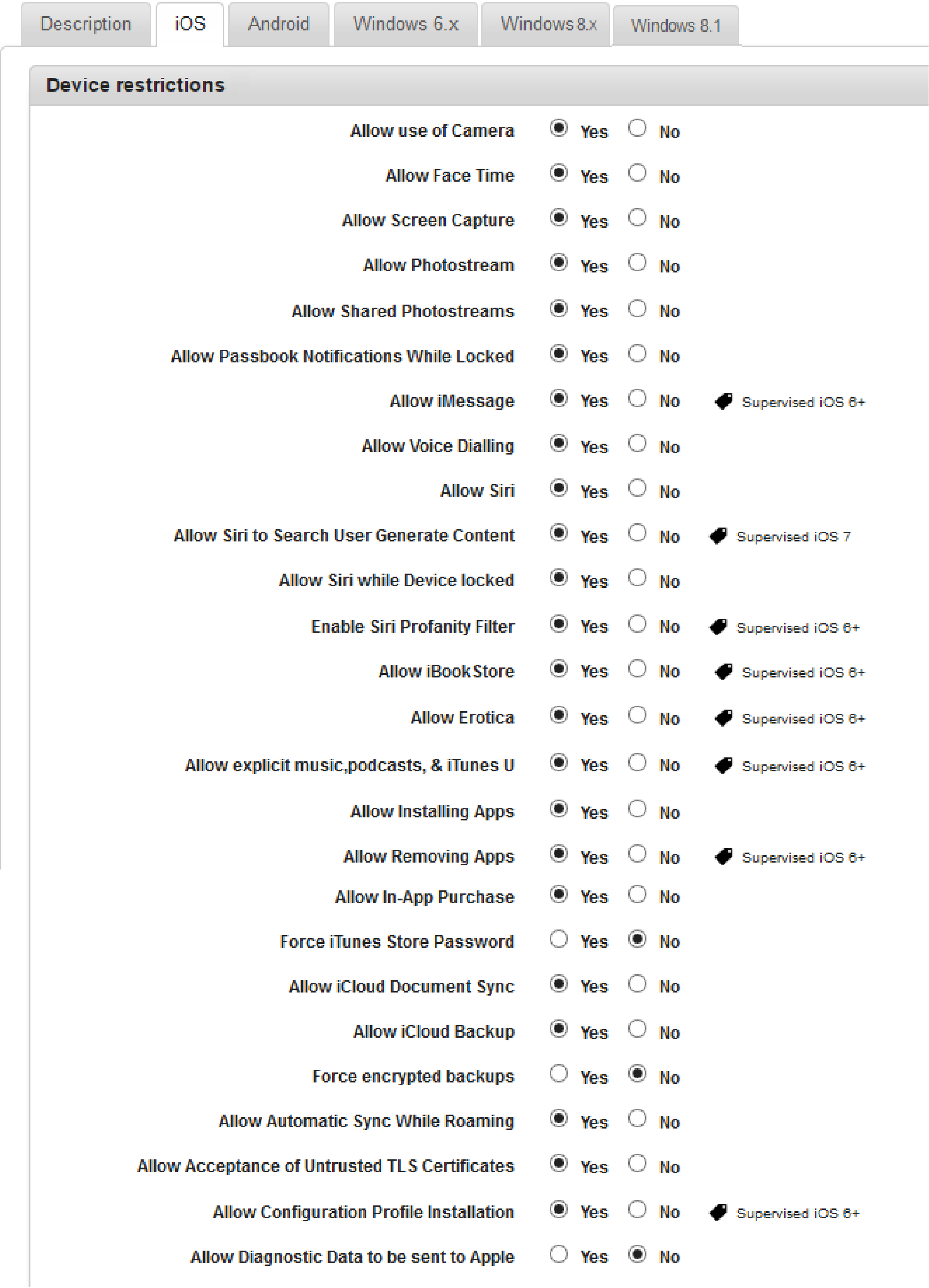
You have 490 characters left

You can set device restrictions policies for the following operating systems.

- Set Device Restriction Policy for iOS
- Set Device Restriction Policy for Android
- Device Restriction Policy for Windows 6.x
- Device Restriction Policy for Windows Phone 8.x
- Device Restriction Policy for Windows 8.1

10.4.3.1 Set Device Restriction Policy for iOS

1. To set device restrictions policy for iOS, complete the following fields:



Device restrictions

Allow use of Camera	● Yes	○ No	
Allow Face Time	● Yes	○ No	
Allow Screen Capture	● Yes	○ No	
Allow Photostream	● Yes	○ No	
Allow Shared Photostreams	● Yes	○ No	
Allow Passbook Notifications While Locked	● Yes	○ No	
Allow iMessage	● Yes	○ No	Supervised iOS 6+
Allow Voice Dialling	● Yes	○ No	
Allow Siri	● Yes	○ No	
Allow Siri to Search User Generate Content	● Yes	○ No	Supervised iOS 7
Allow Siri while Device locked	● Yes	○ No	
Enable Siri Profanity Filter	● Yes	○ No	Supervised iOS 6+
Allow iBookStore	● Yes	○ No	Supervised iOS 6+
Allow Erotica	● Yes	○ No	Supervised iOS 6+
Allow explicit music,podcasts, & iTunes U	● Yes	○ No	Supervised iOS 6+
Allow Installing Apps	● Yes	○ No	
Allow Removing Apps	● Yes	○ No	Supervised iOS 6+
Allow In-App Purchase	● Yes	○ No	
Force iTunes Store Password	○ Yes	● No	
Allow iCloud Document Sync	● Yes	○ No	
Allow iCloud Backup	● Yes	○ No	
Force encrypted backups	○ Yes	● No	
Allow Automatic Sync While Roaming	● Yes	○ No	
Allow Acceptance of Untrusted TLS Certificates	● Yes	○ No	
Allow Configuration Profile Installation	● Yes	○ No	Supervised iOS 6+
Allow Diagnostic Data to be sent to Apple	○ Yes	● No	

- **Allow use of Camera**: By default, this option is set to Yes to enable you to use the camera. You can modify it to No.

  This functionality enables you to use camera.

- **Allow FaceTime**: By default, this option is set to Yes. You can modify it to No.

  FaceTime is a video chat application for supported mobile devices. Camera use must be enabled.

- **Allow Screen Capture**: By default, this option is set to Yes. You can modify it to No.

  Configures the screen capture feature. Setting this to no will disable the screen capture feature.

- **Allow Photostream**: By default, this option is set to Yes. You can modify it to No.

  Controls the Photo stream feature. Configuring this to no will disable the Photo stream feature.

- **Allow Shared Photostreams**: By default, this option is set to Yes. You can modify it to No.

  Controls the Shared Photo stream feature. Configuring this to no will disable the Shared Photo stream feature.

- **Allow Passbook Notifications While Locked:** By default, this option is set to Yes. You can modify it to No.

  Controls the Passbook notifications. Configuring this to no will disable displaying Passbook notifications while the device is locked.

- **Allow iMessage**: By default, this option is set to Yes. You can modify it to No.

  Controls the iMessage feature. Configuring this to no will disable the iMessage feature.

- **Allow Voice Dialing**: By default, this option is set to Yes. You can modify it to No.

  Controls the Voice Dialing feature. Configuring this to no will disable dialing a phone number through voice commands.

- **Allow Siri**: By default, this option is set to Yes. You can modify to No.

  Controls the Siri feature. Configuring this to no will disable the Siri feature.

- **Allow Siri to Search User Generate Content**: By default, this option is set to Yes. You can modify to No.

  Controls the Siri feature. Configuring this to yes will allow Siri to search the user generated content and include those in the search results. You need the Allow Siri feature enabled for this feature to work.

- **Allow Siri While Device Locked**: By default, this option is set to Yes. You can modify it to No.

  Controls the Siri feature. Configuring this to yes will allow Siri to activate even when the phone is locked. You need the Allow Siri feature enabled for this feature to work.

- **Enable Siri Profanity Filter**: By default, this option is set to Yes. You can modify to No.

  Controls the Siri feature. Configuring this to yes will allow Siri to filter any cuss words used in the voice commands. You need the Allow Siri feature enabled for this feature to work.

- **Allow iBooks Store**: By default, this option is set to Yes. You can modify to No.

  This feature allows access to iBooks app. This app enables you to access online books library and download them.

- **Allow Erotica**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the adult literature and art on the device. If configured to No, all songs, videos, and images that contain adult material are not displayed on the device through Safari browsing and AppStore results.

- **Allow Explicit Music, Podcasts & iTunes U**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the adult literature and art on the device. If configured to No, all adult content in Podcasts, iBooks, and iTunes Store is hidden from the search results.

- **Allow Installing Apps**: By default, this option is set to Yes. You can modify it to No.

  Controls user's ability to install apps on the device. If configured to No, users cannot install apps on the device.

- **Allow Removing Apps**: By default, this option is set to Yes. You can modify it to No.

  Controls user's ability to remove apps on the device. If configured to No, users cannot remove apps on the device.

- **Allow in-App Purchase**: By default, this option is set to Yes. You can modify it to No.

  Controls user's ability to make In-App purchases for apps on the device. If configured to No, users cannot make any purchases within apps on the device.

- **Force iTunes Store Password**: By default, this option is set to Yes. You can modify it to No.

  This feature restricts the access to iTunes Store and a user needs to provide credentials before accessing the store.

- **Allow iCloud Document Sync**:By default, this option is set to Yes. You can modify it to No.

  This feature restricts synching documents on iCloud. If configured to Yes, all documents are synched with the user's iCloud account.

- **Allow iCloud Backup**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the iCloud Backup. If configured to Yes, all the data will be backed up on iCloud. The default storage capacity on iCloud is 5GB. If your data exceeds 5 GB, you may have to buy additional storage space.

- **Force Encrypted Backups:** By default, this option is set to No. You can modify it to Yes.

  This feature controls forced backups on devices. Under Force Encrypted Backups, all backups for an iOS device enrolled in MDM be encrypted.

- **Allow Automatic Sync While Roaming**: By default, this option is set to Yes. You can modify it to No.

  This feature enables a cellular device's automatic sync of apps (like mail, calendar or contacts) while device is in roaming. If turned off, user might need to manually sync the apps.

- **Allow Acceptance of Untrusted TLS Certificates** By default, this option is set to Yes. You can modify it to No.

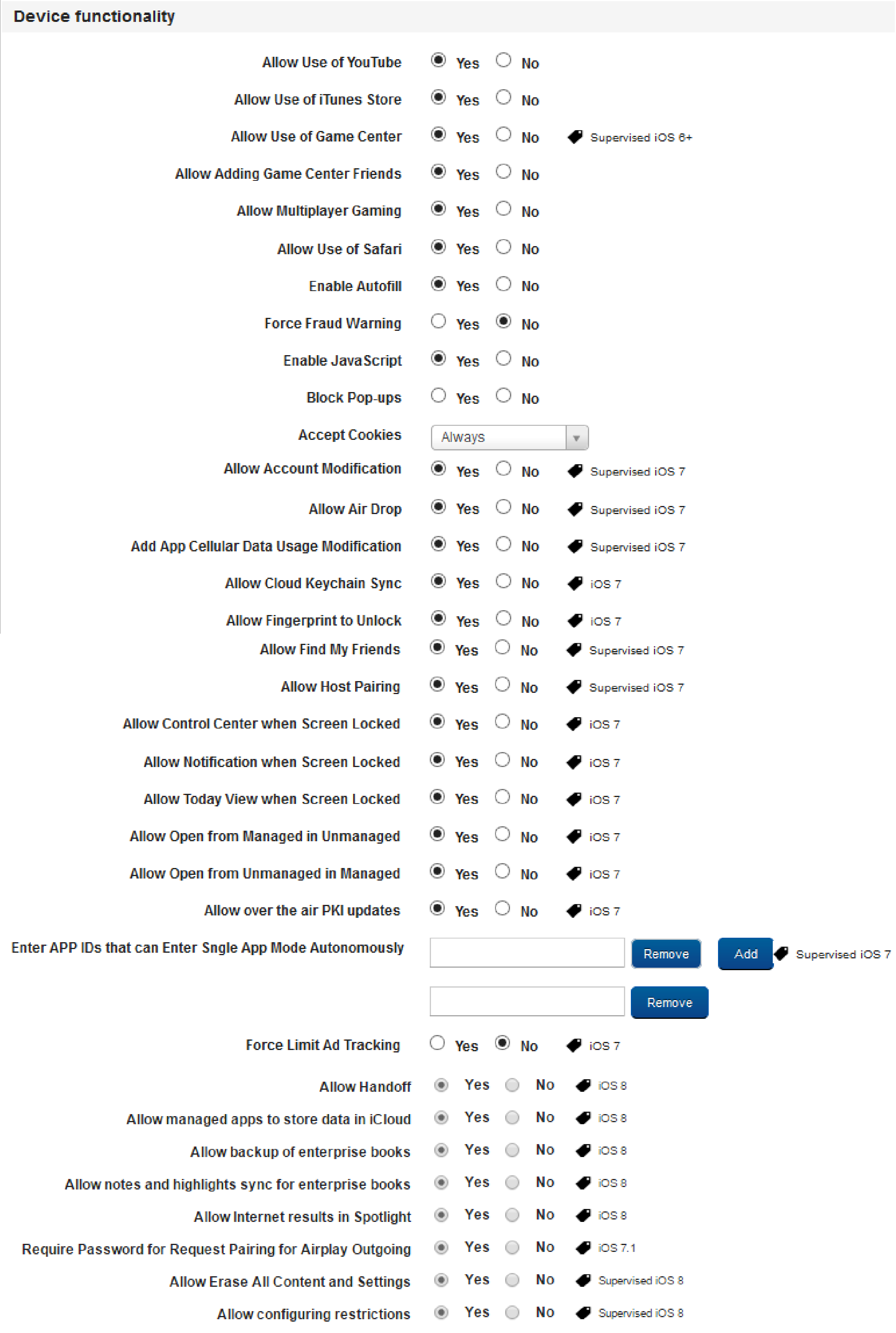
  This feature controls accepting untrusted TLS certificates. If configured to Yes, the device will accept untrusted TLS certificates. Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet.

- **Allow Configuration Profile Installation**: By default, this option is set to Yes. You can modify it to No.

  This feature controls installing profiles on the device. If configured to Yes, configuration profiles can be installed on the device.

- **Allow Diagnostic Data to be sent to Apple**: By default, this option is set to Yes. You can modify it to No.

  This feature controls data to be sent to Apple. If configured to No, diagnostic data will not be shared with Apple.



Device functionality

Allow Use of YouTube	● Yes	○ No	
Allow Use of iTunes Store	● Yes	○ No	
Allow Use of Game Center	● Yes	○ No	Supervised iOS 6+
Allow Adding Game Center Friends	● Yes	○ No	
Allow Multiplayer Gaming	● Yes	○ No	
Allow Use of Safari	● Yes	○ No	
Enable Autofill	● Yes	○ No	
Force Fraud Warning	○ Yes	● No	
Enable JavaScript	● Yes	○ No	
Block Pop-ups	○ Yes	○ No	
Accept Cookies	Always		
Allow Account Modification	● Yes	○ No	Supervised iOS 7
Allow Air Drop	● Yes	○ No	Supervised iOS 7
Add App Cellular Data Usage Modification	● Yes	○ No	Supervised iOS 7
Allow Cloud Keychain Sync	● Yes	○ No	iOS 7
Allow Fingerprint to Unlock	● Yes	○ No	iOS 7
Allow Find My Friends	● Yes	○ No	Supervised iOS 7
Allow Host Pairing	● Yes	○ No	Supervised iOS 7
Allow Control Center when Screen Locked	● Yes	○ No	iOS 7
Allow Notification when Screen Locked	● Yes	○ No	iOS 7
Allow Today View when Screen Locked	● Yes	○ No	iOS 7
Allow Open from Managed in Unmanaged	● Yes	○ No	iOS 7
Allow Open from Unmanaged in Managed	● Yes	○ No	iOS 7
Allow over the air PKI updates	● Yes	○ No	iOS 7
Enter APP IDs that can Enter Sngle App Mode Autonomously	Remove	Add	Supervised iOS 7
	Remove		
Force Limit Ad Tracking	○ Yes	● No	iOS 7
Allow Handoff	● Yes	○ No	iOS 8
Allow managed apps to store data in iCloud	● Yes	○ No	iOS 8
Allow backup of enterprise books	● Yes	○ No	iOS 8
Allow notes and highlights sync for enterprise books	● Yes	○ No	iOS 8
Allow Internet results in Spotlight	● Yes	○ No	iOS 8
Require Password for Request Pairing for Airplay Outgoing	● Yes	○ No	iOS 7.1
Allow Erase All Content and Settings	● Yes	○ No	Supervised iOS 8
Allow configuring restrictions	● Yes	○ No	Supervised iOS 8

- **Allow Use of You Tube**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the YouTube application on the device. If configured to No, the YouTube app will not work on the device.

- **Allow Use of iTunes Store**: By default, this option is set to Yes. You can modify to No.

  This feature controls the iTunes Store application on the device. If configured to No, the iTunes Store app will not work on the device

- **Allow Use of Games Center**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Game Centre application on the device. If configured to No, the Game Centre app will not work on the device. Game Center is an app that allows creating an online persona, playing online games, and interacting with other players anonymously through their alias.

- **Allow Adding Game Center Friends:** By default, this option is set to Yes. You can modify it to No.

  This feature controls the Game Center application on the device. If configured to No, the Game Centre app will not allow you to add friends in it.

- **Allow Multiplayer Gaming**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Game Center application on the device. If configured to No, the Game Centre app will not allow Multiplayer gaming work on the device.

- **Allow Use of Safari**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Safari application on the device. If configured to No, the Safari app will not work on the device.

- **Enable Autofill**: By default, this option is set to Yes. You can modify to No.

  This feature controls the Autofill feature on the device. If configured to Yes, the Autofill feature will store your details to fill forms and will offer to provide that data automatically when you visit the login page of saved details again.

- **Force Fraud Warning**: By default, this option is set to No. You can modify to Yes.

  This feature controls the Fraud waring feature in the Safari application on the device. If configured to Yes, Safari app will warn you about a fraud site if the site is a malicious site. The fraud warning feature adds a small level of protection against a possible phishing attacks.

- **Enable JavaScript**: By default, this option is set to Yes. You can modify to No.

  This feature controls the JavaScript feature on the device. If configured to Yes, the Safari app will allow JavaScripts to run on websites.

- **Block Pop-ups**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the Pop-ups feature in the Safari App. If configured to Yes, the Safari app will block all pop-ups from any website.

- **Accept Cookies**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the cookies feature in the Safari App. If configured to Yes, the Safari app will accept cookies from the websites it visits.

- **Allow Account Modification**: By default, this option is set to Yes. You can modify it to No.

  Applies to a Supervised Device. If Allowed, lets users to modify the device account.

- **Allow Air Drop**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Air Drop feature. Air Drop enables the transfer of files among supported Macintosh computers and iOS devices over Wi-Fi and Bluetooth, without using mail or a mass storage device.

- **Add App Cellular Data Usage Modification**: By default, this option is set to Yes. You can modify it to No.

  Applies to a Supervised Device. If permitted, let users manage which app could use cellular data.

- **Allow Cloud Keychain Sync**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Keychain feature. If configured to Yes, the device will sync Keychain data with your cloud account.

- **Allow Fingerprint to Unlock**: By default, this option is set to Yes. You can modify it to No.

  This feature controls unlocking the device. If configured to Yes, the fingerprint reader will be allowed to read your fingerprint to unlock the device.

- **Allow Find My Friends**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Find My Friends app on the device. If configured to No, the Find My Friends app will not work on the device.

- **Allow Host Pairing**: By default, this option is set to Yes. You can modify it to No.

  Applies to Supervised Device. If Allowed, a Device can pair to any Host Computer. If Disallowed, Device can pair only with the supervising Host.

- **Allow Control Center when Screen Locked**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the Control Center on the device. I configured to No, the control center will not be accessible when the screen is locked.

- **Allow Notification when Screen Locked**: By default, this option is set to Yes. You can modify it to No.

This feature controls notifications on the device. If configured to No, notifications will not be pushed when the screen is locked.

- **Allow Today View when Screen Locked**: By default, this option is set to Yes. You can modify it to No.

  If allowed, enables the Today View in Notification Center on the Lock Screen.

- **Allow Open from Managed to Unmanaged**: By default, this option is set to No. You can modify it to Yes.

  If allowed, Documents from Managed Apps and accounts can be opened in Unmanaged apps and accounts. If not allowed, documents from managed apps and accounts can be opened only in other managed apps and accounts.

- **Allow Open from Unmanaged to Managed**: By default, this option is set to No. You can modify it to Yes.

  If allowed, Documents from Unmanaged Apps and Accounts can be opened in Managed Apps and Accounts. If not allowed, documents from unmanaged apps and accounts can be opened only in other unmanaged apps and accounts

- **Allow over the air PKI updates**: By default, this option is set to Yes. You can modify it to No.

  If Allowed, allows over the Air PKI updates (primarily for root certificates). Useful in case of having certificates for mobile environments.

- **Enter APP IDs that can Enter Single App Mode Autonomously**: By default, this option is set to Yes. You can modify it to No.

  App Bundle IDs which are permitted to enter Single App Mode Autonomously. Apps configured here can enter into Single App Mode as per the coded trigger / behavior.

- **Force Limit Ad Tracking**: By default, this option is set to No. You can modify it to Yes.

If forced, enables Limit Ad Tracking (Advertisement) setting.

- **Allow Handoff**: By default, this option is set to Yes. You can modify it to No.

  If Yes, Allows Handoff feature. If No, user handoff will be disabled on the device

- **Allow managed apps to store data in iCloud**: By default, this option is set to Yes. You can modify it to No.

  This feature controls data storage on iCloud. If configured to Yes, data from managed apps will be allowed to store data on iCloud.

- **Allow backup of enterprise books**: By default, this option is set to Yes. You can modify it to No.

  This feature controls enterprise books backup on iCloud. If configured to Yes, enterprise books will be allowed to store data on iCloud.

- **Allow notes and highlights sync for enterprise books**: By default, this option is set to Yes. You can modify it to No.

  This feature controls synching notes and highlights of enterprise books in iCloud. If configured to Yes, enterprise books will be allowed to store notes and highlights on iCloud.

- **Allow Internet results in Spotlight**: By default, this option is set to Yes. You can modify it to No.

  This feature controls the internet results in the Spotlight search feature on the device. If configured to Yes, when you search in the spotlight, internet results will also display in the results.

- **Require Password for Request Pairing for Airplay Outgoing**: By default, this option is set to Yes. You can modify it to No.

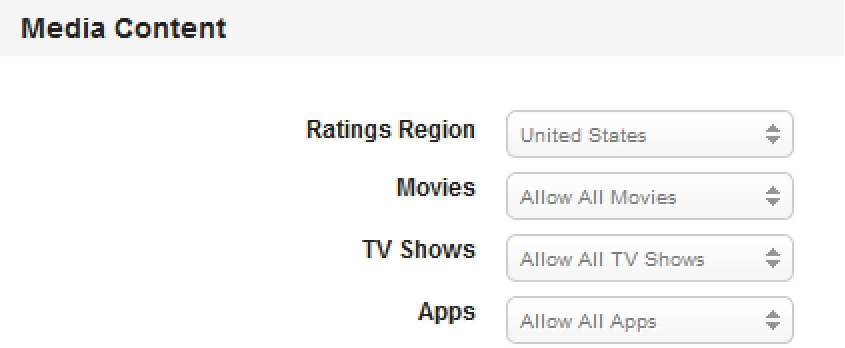
  This feature controls Airplay settings. If configured to Yes, all outgoing Airplay pairing requests will require password.

- **Allow Erase All Content and Settings**: By default, this option is set to Yes. You can modify it to No.

  This feature controls erasing content and settings. If configured to No, the user will not be able to use the Erase All Content and Settings feature on the device.

- **Allow configuring restrictions**: By default, this option is set to Yes. You can modify it to No.

  Applies to Supervised Device. If Allowed, user can set a password (different password than device password) to restrict the device. Primarily for parental controls.



Media Content

Ratings Region: United States
Movies: Allow All Movies
TV Shows: Allow All TV Shows
Apps: Allow All Apps

- **Ratings Region**: Select the required region from the drop-down menu. By default, it is set to **United States**.

  This feature controls the region for media content rating.

- **Movies**: Select the desired movie from the drop-down menu. By default, it is set to **Allow All Movies**.

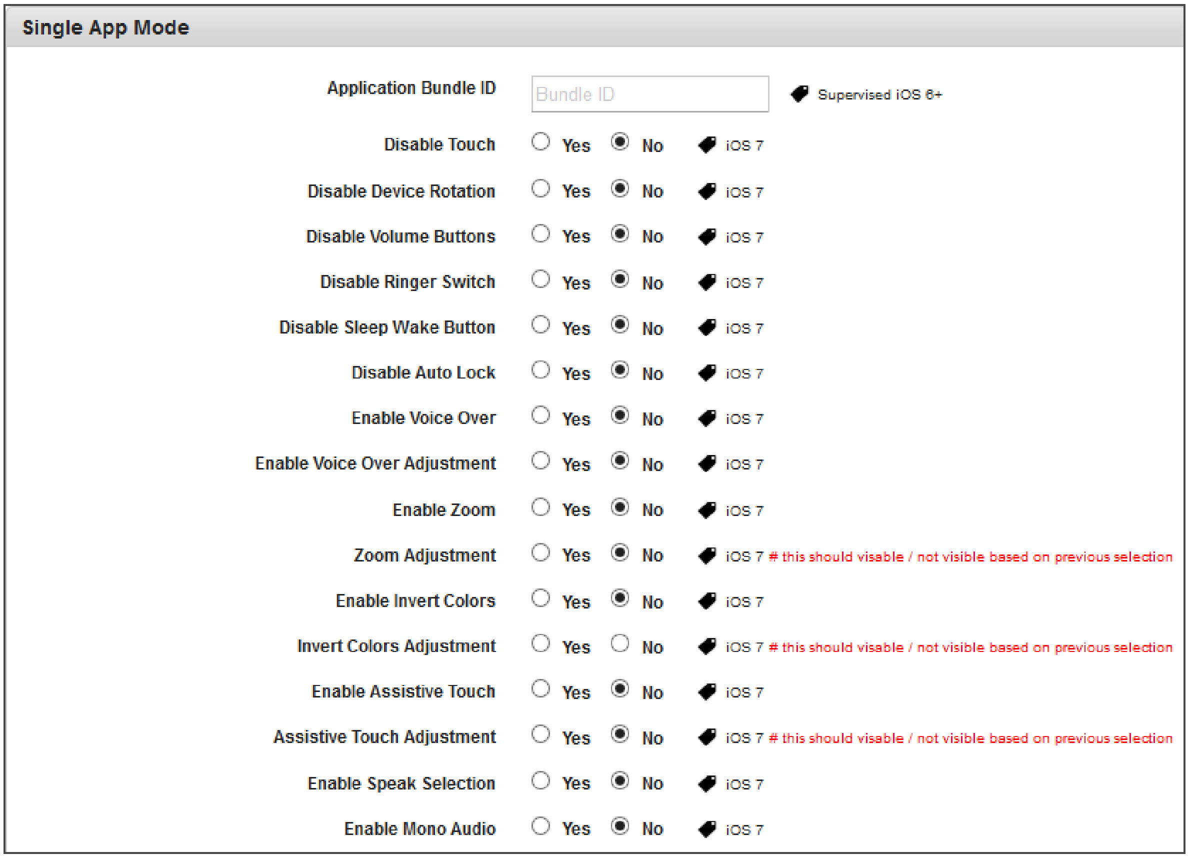
  This feature controls the movies that are allowed on the device based on their rating.

- **TV Shows**: Select the desired TV shows from the drop-down menu. By default, it is set to **Allow All TV Shows**.

  This feature controls the TV shows that are allowed on the device based on their rating.

- **Apps**: Select the desired apps from the drop-down menu. By default, it is set to **Allow All Apps**.

  This feature controls the Apps that are allowed on the device based on their rating.



Single App Mode

Application Bundle ID	Bundle ID		Supervised iOS 6+
Disable Touch	○ Yes	● No	iOS 7
Disable Device Rotation	○ Yes	● No	iOS 7
Disable Volume Buttons	○ Yes	● No	iOS 7
Disable Ringer Switch	○ Yes	● No	iOS 7
Disable Sleep Wake Button	○ Yes	● No	iOS 7
Disable Auto Lock	○ Yes	● No	iOS 7
Enable Voice Over	○ Yes	● No	iOS 7
Enable Voice Over Adjustment	○ Yes	● No	iOS 7
Enable Zoom	○ Yes	● No	iOS 7
Zoom Adjustment	○ Yes	● No	iOS 7 # this should visable / not visible based on previous selection
Enable Invert Colors	○ Yes	● No	iOS 7
Invert Colors Adjustment	○ Yes	○ No	iOS 7 # this should visable / not visible based on previous selection
Enable Assistive Touch	○ Yes	● No	iOS 7
Assistive Touch Adjustment	○ Yes	● No	iOS 7 # this should visable / not visible based on previous selection
Enable Speak Selection	○ Yes	● No	iOS 7
Enable Mono Audio	○ Yes	● No	iOS 7

- **Application Bundle ID**: Enter the application bundle ID.

  Enter the application bundle ID for which you want to configure the features further below.

- **Disable Touch**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the touch feature. If configured to Yes, the touch feature will be disabled on the device.

- **Disable Device Rotation**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the device rotation feature. If configured to Yes, the device rotation feature will be disabled on the device.

- **Disable Volume Buttons**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the volume buttons feature. If configured to Yes, volume buttons feature will be disabled on the device.

- **Disable Ringer Switch**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the ringer switch feature. If configured to Yes, the ringer switch feature will be disabled on the device.

- **Disable Sleep Wake Button**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the sleep wake button feature. If configured to Yes, the sleep wake button feature will be disabled on the device.

- **Disable Auto Lock**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the auto lock feature. If configured to Yes, the auto lock feature will be disabled on the device.

- **Enable Voice Over**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the voice over feature. If configured to Yes, the voice over feature will be disabled on the device.

- **Enable Voice Over Adjustment**: By default, this option is set to No. You can modify it to Yes.

- **Enable Zoom**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the zoom feature. If configured to No, the zoom feature will be disabled on the device.

- **Zoom Adjustment**: By default, this option is set to No. You can modify it to Yes.

- **Enable Invert Colors**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the invert colors feature. If configured to Yes, the colors will be inverted in the screen on the device.

- **Invert Colors Adjustment**: By default, this option is set to No. You can modify it to Yes.

- **Enable Assistive Touch**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the assistive touch feature. If configured to Yes, the assistive touch feature will be disabled on the device.

- **Assistive Touch Adjustment**: By default, this option is set to No. You can modify it to Yes.

- **Enable Speak Selection**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the speak selection feature. If configured to Yes, the speak selection feature will be disabled on the device.

- **Enable Mono Audio**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the mono audio feature. If configured to Yes, the mono audio feature will be enabled on the on the device.

2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

To Remove Single App Mode from a Device (For supervised iOS 6 only)

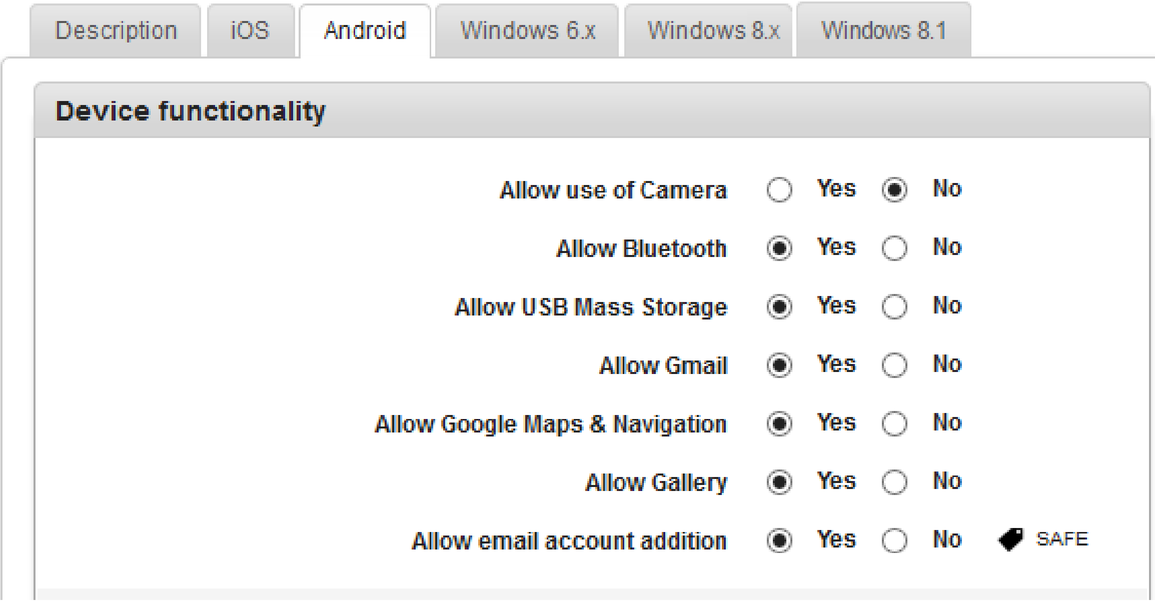
To remove the app lock, the Administrator should modify the device restriction policy and remove the name of the assigned app. Then, Admin should send a blank field to remove the Single App Mode.

10.4.3.2 Set Device Restriction Policy for Android

1. To set device restrictions policy for Android, follow these steps:

   The Android tab has the following sections:

   - **Device Functionality**
   - **Browser Policy**
   - **Restrictions Policy**
   - **Roaming**
   - **Phone Restrictions**
   - **Date Time**
   - **Location**
   - **App Restrictions**
   - **Stats Capture**
   - **Security**



Device functionality

Allow use of Camera ○ Yes ● No

Allow Bluetooth ● Yes ○ No

Allow USB Mass Storage ● Yes ○ No

Allow Gmail ● Yes ○ No

Allow Google Maps & Navigation ● Yes ○ No

Allow Gallery ● Yes ○ No

Allow email account addition ● Yes ○ No SAFE

a. **Allow Use of Camera**: By default, this option is set to Yes. You can modify it to No.

   This feature controls the usage of camera on the device. If configured to No, the camera will not function on the device.

b. **Allow Bluetooth**: By default, this option is set to Yes. You can modify it to No.

   This feature controls the usage of Bluetooth on the device. If configured to No, the Bluetooth will not function on the device.

c. **Allow USB Mass Storage**: By default, this option is set to Yes. You can modify it to No.

d. **Allow Gmail**: By default, this option is set to Yes. You can modify it to No.

   This feature controls the usage of the Gmail app on the device. If configured to No, the Gmail app will not function on the device.

e. **Allow Google Maps and Navigation**: By default, this option is set to Yes. You can modify it to No.

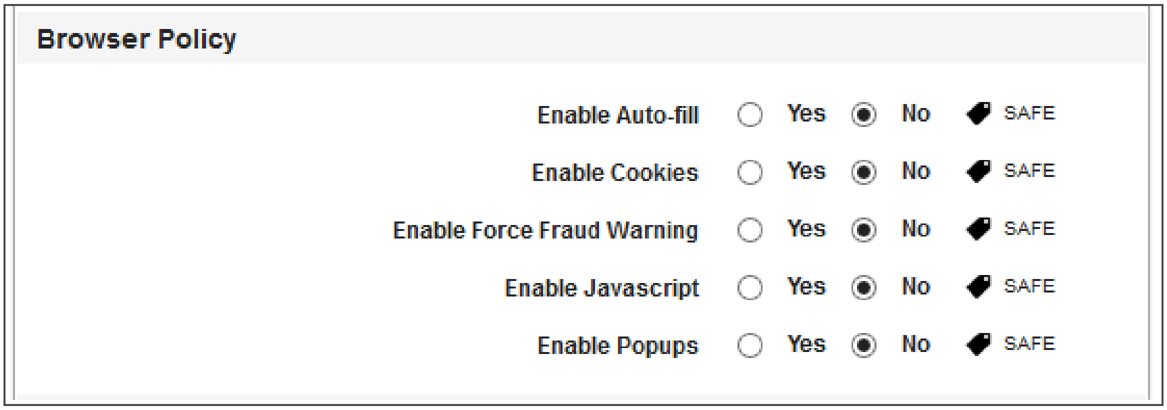
   This feature controls the usage of Google Maps and navigation on the device. If configured to No, Google Maps will not function on the device.

f. **Allow Gallery**: By default, this option is set to Yes. You can modify it to No.

This feature controls the usage of the Gallery on the device. If configured to No, the Gallery will not function on the device

g. **Allow email account addition**: By default, this option is set to Yes. You can modify it to No.

This feature controls adding a new email account on the device. If configured to No, the user cannot add a new email account on the device.



Browser Policy

Enable Auto-fill	○ Yes	● No	SAFE
Enable Cookies	○ Yes	● No	SAFE
Enable Force Fraud Warning	○ Yes	● No	SAFE
Enable Javascript	○ Yes	● No	SAFE
Enable Popups	○ Yes	● No	SAFE

- **Enable Auto-fill**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the Autofill feature on the device. If configured to Yes, the Autofill feature will store your details to fill forms and will offer to provide that data automatically when you visit the login page of saved details again.

- **Enable Cookies**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the cookies feature in the Chrome App. If configured to Yes, the Chrome app will accept cookies from the websites it visits.

- **Enable Force Fraud Warning**: By default, this option is set to No. You can modify it to Yes.

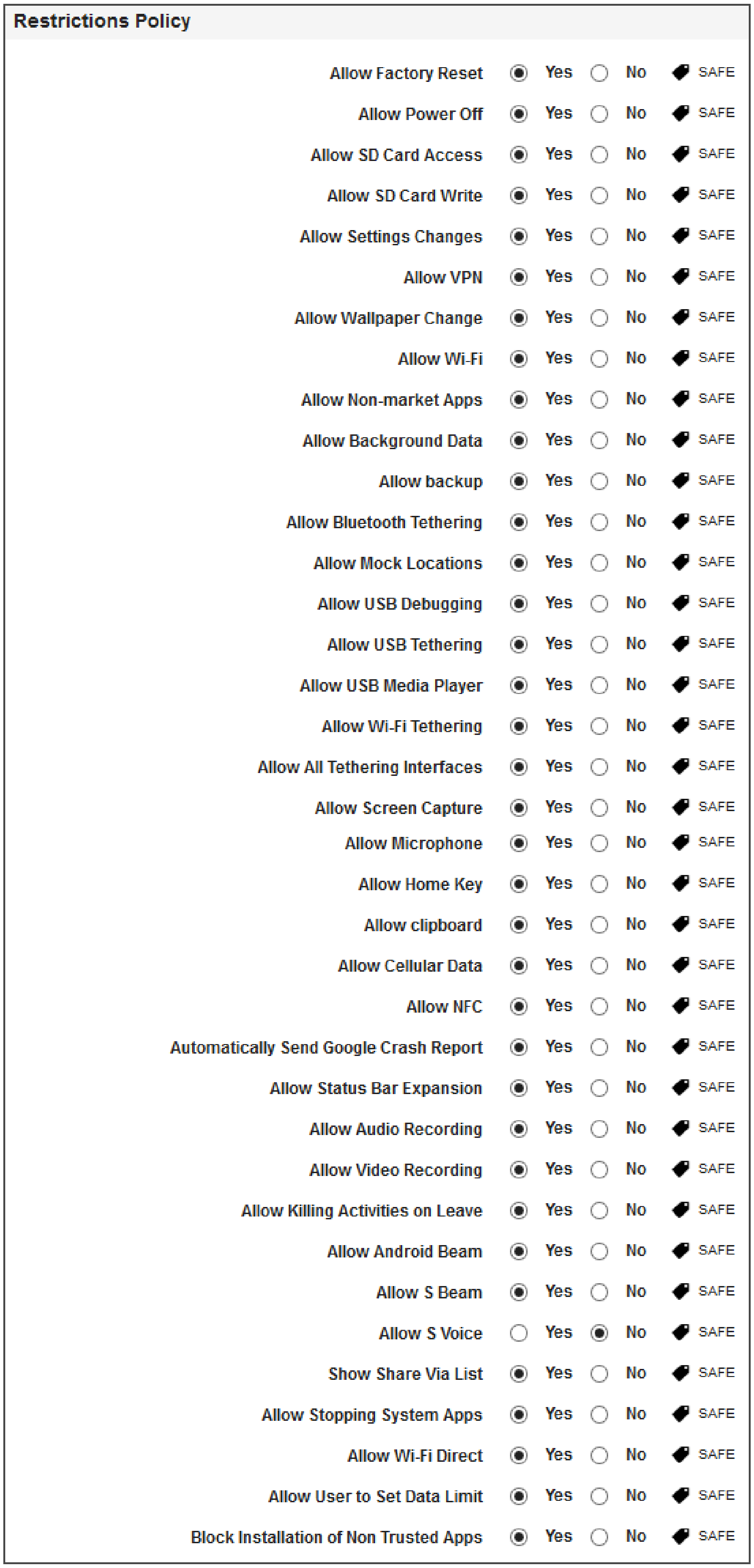
  This feature controls the Fraud waring feature in the Chrome app on the device. If configured to Yes, the Chrome app will warn you about a fraud site if the site is a malicious site. The fraud warning feature adds a small level of protection against a possible phishing attacks.

- **Enable JavaScript**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the JavaScript feature on the device. If configured to Yes, the Chrome app will allow JavaScripts to run on websites.

- **Enable Popups**: By default, this option is set to No. You can modify it to Yes.

  This feature controls the Pop-ups feature in the Safari App. If configured to No, the Chrome app will block all pop-ups from any website.



Restrictions Policy

Allow Factory Reset	● Yes	○ No	SAFE
Allow Power Off	● Yes	○ No	SAFE
Allow SD Card Access	● Yes	○ No	SAFE
Allow SD Card Write	● Yes	○ No	SAFE
Allow Settings Changes	● Yes	○ No	SAFE
Allow VPN	● Yes	○ No	SAFE
Allow Wallpaper Change	● Yes	○ No	SAFE
Allow Wi-Fi	● Yes	○ No	SAFE
Allow Non-market Apps	● Yes	○ No	SAFE
Allow Background Data	● Yes	○ No	SAFE
Allow backup	● Yes	○ No	SAFE
Allow Bluetooth Tethering	● Yes	○ No	SAFE
Allow Mock Locations	● Yes	○ No	SAFE
Allow USB Debugging	● Yes	○ No	SAFE
Allow USB Tethering	● Yes	○ No	SAFE
Allow USB Media Player	● Yes	○ No	SAFE
Allow Wi-Fi Tethering	● Yes	○ No	SAFE
Allow All Tethering Interfaces	● Yes	○ No	SAFE
Allow Screen Capture	● Yes	○ No	SAFE
Allow Microphone	● Yes	○ No	SAFE
Allow Home Key	● Yes	○ No	SAFE
Allow clipboard	● Yes	○ No	SAFE
Allow Cellular Data	● Yes	○ No	SAFE
Allow NFC	● Yes	○ No	SAFE
Automatically Send Google Crash Report	● Yes	○ No	SAFE
Allow Status Bar Expansion	● Yes	○ No	SAFE
Allow Audio Recording	● Yes	○ No	SAFE
Allow Video Recording	● Yes	○ No	SAFE
Allow Killing Activities on Leave	● Yes	○ No	SAFE
Allow Android Beam	● Yes	○ No	SAFE
Allow S Beam	● Yes	○ No	SAFE
Allow S Voice	○ Yes	● No	SAFE
Show Share Via List	● Yes	○ No	SAFE
Allow Stopping System Apps	● Yes	○ No	SAFE
Allow Wi-Fi Direct	● Yes	○ No	SAFE
Allow User to Set Data Limit	● Yes	○ No	SAFE
Block Installation of Non Trusted Apps	● Yes	○ No	SAFE

- **Allow Admin Control Removal:** If allowed, User can Deactivate an App a Device Administrator.In EMM Mode, if user Deactivates Launchpad as Device Administrator, enrolment will be void. Also, based on compliance policy (if configured), this action might trigger a compliance violation.
- **Allow Factory Reset**:This feature controls the factory reset feature on the device. If configured to No, the user will not be able to reset the device to factory defaults..
- **Allow Power Off**: By default, this option is set to No. You can modify it to Yes.
- **Allow SD Card Access**: By default, this option is set to No. You can modify it to Yes.
- **Allow SD Card Write**: By default, this option is set to No. You can modify it to Yes.
- **Allow Settings Changes**: By default, this option is set to No. You can modify it to Yes.
- **Allow VPN**: By default, this option is set to No. You can modify it to Yes.
- **Allow Wallpaper Change**: By default, this option is set to No. You can modify it to Yes.
- **Allow Wi-Fi**: By default, this option is set to No. You can modify it to Yes.
- **Allow Non-market Apps**: By default, this option is set to No. You can modify it to Yes.
- **Allow Background Data**: By default, this option is set to No. You can modify it to Yes.
- **Allow backup**: By default, this option is set to No. You can modify it to Yes.
- **Allow Bluetooth Tethering**: By default, this option is set to No. You can modify it to Yes.
- **Allow Mock Locations**: By default, this option is set to No. You can modify it to Yes.
- **Allow USB Debugging**: By default, this option is set to No. You can modify it to Yes.
- **Allow USB Tethering**: By default, this option is set to No. You can modify it to Yes.
- **Allow USB Media Player**: By default, this option is set to No. You can modify it to Yes.
- **Allow Wi-Fi Tethering**: By default, this option is set to No. You can modify it to Yes.

- **Allow All Tethering Interfaces**: By default, this option is set to No. You can modify it to Yes.

> *Note:* If the allow all tethering interfaces is set to No, all other tethering will not work. Wi-fi, USB, and Bluetooth tethering can be enabled only if this option is Yes.

- **Allow Screen Capture**: By default, this option is set to No. You can modify it to Yes.
- **Allow Microphone**: By default, this option is set to No. You can modify it to Yes.
- **Allow Home Key**: By default, this option is set to No. You can modify it to Yes.
- **Allow clipboard**: By default, this option is set to No. You can modify it to Yes.
- **Allow Cellular Data**: By default, this option is set to No. You can modify it to Yes.
- **Allow NFC**: By default, this option is set to No. You can modify it to Yes.
- **Automatically Send Google Crash Report**: By default, this option is set to No. You can modify it to Yes.
- **Allow Status Bar Expansion**: By default, this option is set to No. You can modify it to Yes.
- **Allow Audio Recording**: By default, this option is set to No. You can modify it to Yes.
- **Allow Video Recording**: By default, this option is set to No. You can modify it to Yes.

> *Note:* Video Recording is blocked when **Allow Audio Recording** is set to No.

- **Allow Killing Activities on Leave**: By default, this option is set to No. You can modify it to Yes.

- **Allow Android Beam**: By default, this option is set to No. You can modify it to Yes.

  An administrator can set this policy to block the use of Android Beam on the device. When Android Beam is disabled, the user cannot send information (for example, contacts, e-mails, and Web addresses) using Android Beam. S Beam is also disabled when Android Beam is disabled.

- **Allow S Beam**: By default, this option is set to No. You can modify it to Yes.

  An administrator can set this policy to block the use of S Beam on the device. S Beam allows users to share content using near field communication (NFC) and Wi-Fi Direct. When S Beam is disabled, the user cannot send or receive files using S Beam.

- **Allow S Voice**: By default, this option is set to No. You can modify it to Yes.

  An administrator can use this API to allow or disallow launching the S Voice application (Samsung personal assistant). When S Voice is disabled, the user can neither set a new wake-up command nor unlock the device by using a wake-up command set prior to disallowing S Voice. In addition, once disallowed, the administrator can no longer set a new face and voice lock screen. However, the device can still be unlocked if the lock screen had already been set prior to disallowing S Voice.

- **Show Share Via List**: By default, this option is set to No. You can modify it to Yes.

  The Share Via List is displayed in certain applications that share data with other applications.

- **Allow Stopping System Apps**: By default, this option is set to No. You can modify it to Yes.

  > ***Note:*** An administrator can use this API to disable:
  > - the **Force Stop** button for system-signed applications on the App Info UI in Settings.
  > - the **Stop** button for the system application process on the Running App UI in Settings.

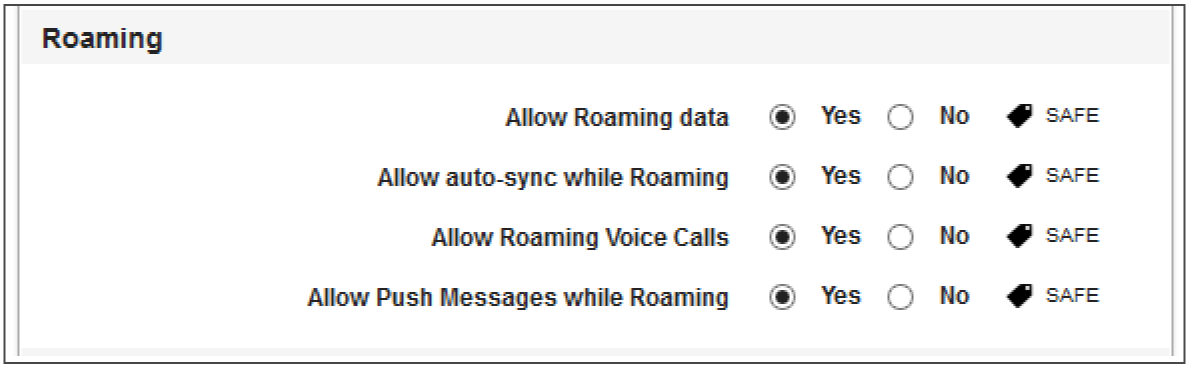
- **Allow Wi-Fi Direct**: By default, this option is set to No. You can modify it to Yes.

  An administrator can enable or disable Wi-Fi Direct without user interaction. When Wi-Fi Direct is disabled, any ongoing Wi-Fi Direct connection is interrupted, and the user cannot turn on Wi-Fi Direct.

- **Allow User to Set Data Limit**: By default, this option is set to No. You can modify it to Yes.

  An administrator can allow or disallow a user to set the mobile data limit. When disabled, the background process limit is set to the maximum value.

- **Block Installation of Non-Trusted Apps**: By default, this option is set to No. You can modify it to Yes to prevent users from installing non CAcert apps.



Roaming

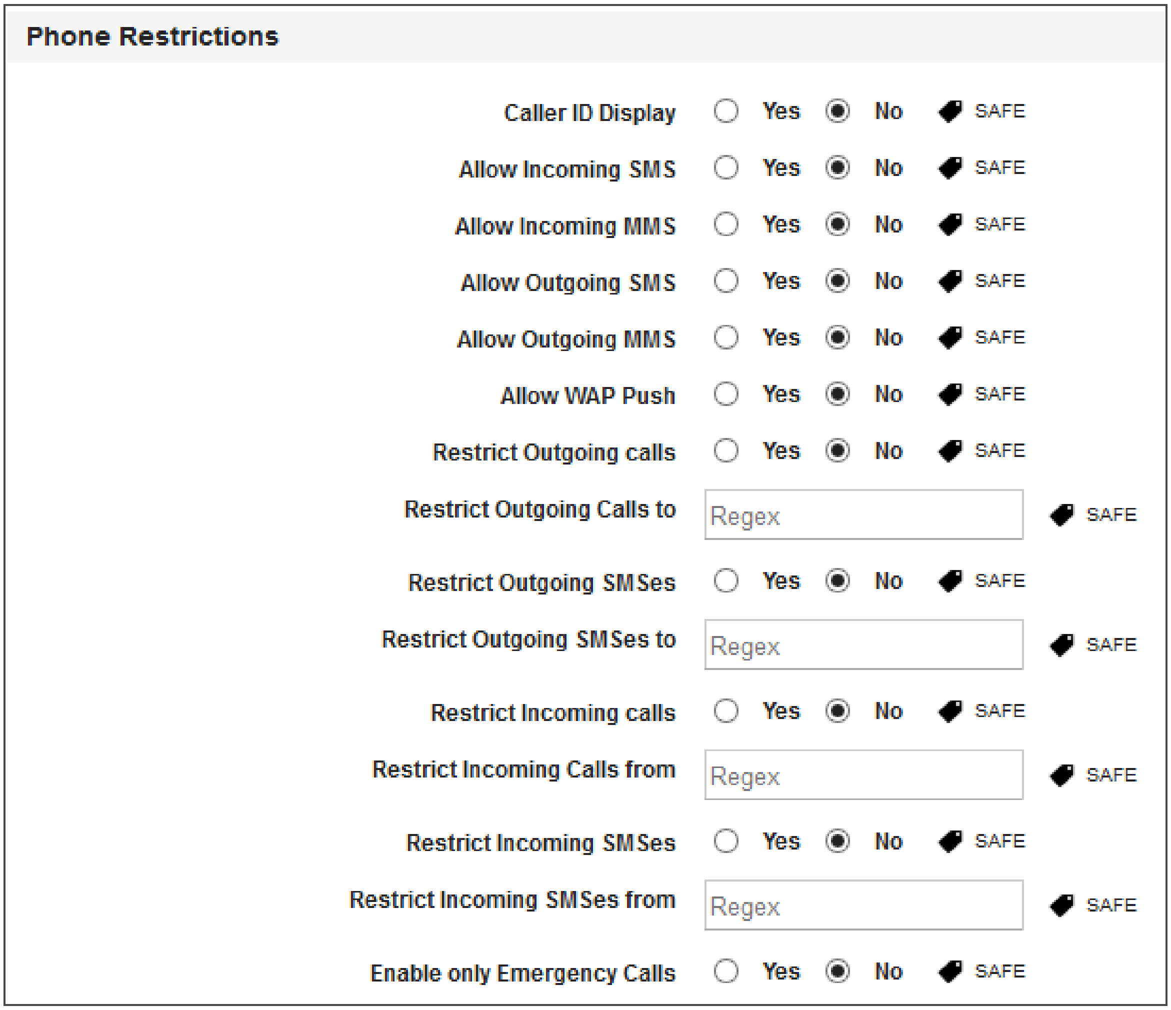
Allow Roaming data ● Yes ○ No SAFE

Allow auto-sync while Roaming ● Yes ○ No SAFE

Allow Roaming Voice Calls ● Yes ○ No SAFE

Allow Push Messages while Roaming ● Yes ○ No SAFE

- **Allow Roaming data**: By default, this option is set to No. You can modify it to Yes.
- **Allow Auto-Sync While Roaming**: By default, this option is set to No. You can modify it to Yes.
- **Allow Roaming Voice Calls**: By default, this option is set to No. You can modify it to Yes.
- **Allow Push Messages While Roaming**: By default, this option is set to No. You can modify it to Yes.

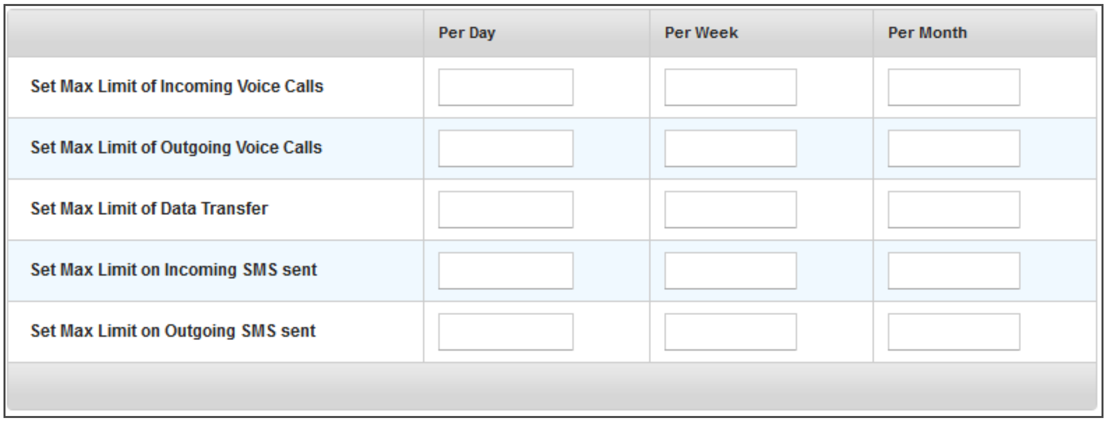


Phone Restrictions

Caller ID Display	○ Yes ● No	SAFE
Allow Incoming SMS	○ Yes ● No	SAFE
Allow Incoming MMS	○ Yes ● No	SAFE
Allow Outgoing SMS	○ Yes ● No	SAFE
Allow Outgoing MMS	○ Yes ● No	SAFE
Allow WAP Push	○ Yes ● No	SAFE
Restrict Outgoing calls	○ Yes ● No	SAFE
Restrict Outgoing Calls to	Regex	SAFE
Restrict Outgoing SMSes	○ Yes ● No	SAFE
Restrict Outgoing SMSes to	Regex	SAFE
Restrict Incoming calls	○ Yes ● No	SAFE
Restrict Incoming Calls from	Regex	SAFE
Restrict Incoming SMSes	○ Yes ● No	SAFE
Restrict Incoming SMSes from	Regex	SAFE
Enable only Emergency Calls	○ Yes ● No	SAFE

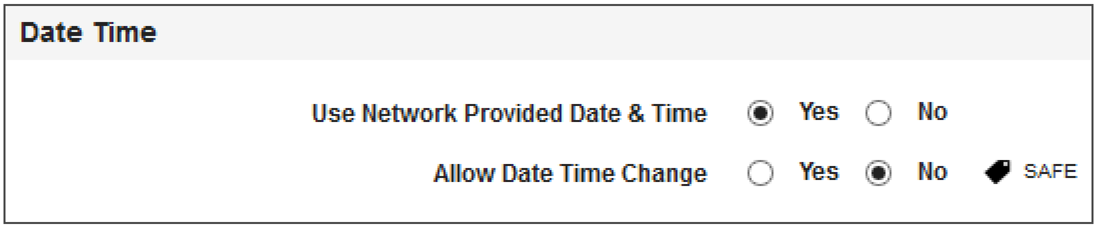
- **Caller ID Display:** : By default, this option is set to No. You can modify it to Yes.
- **Allow Incoming SMS**: By default, this option is set to No. You can modify it to Yes.
- **Allow Incoming MMS**: By default, this option is set to No. You can modify it to Yes.
- **Allow Outgoing SMS**: By default, this option is set to No. You can modify it to Yes.
- **Allow Outgoing MMS**: By default, this option is set to No. You can modify it to Yes.
- **Allow WAP Push**: By default, this option is set to No. You can modify it to Yes.
- **Restrict Outgoing calls**: By default, this option is set to No. You can modify it to Yes.

- **Restrict Outgoing Calls to**: By default, this option is set to No. You can modify it to Yes. This option is shown only if you set **Yes** in Restrict Outgoing calls. This field even takes the regular expression for list of all numbers to be blocked. For more information, see tool tips.
- **Restrict Outgoing SMSs**: By default, this option is set to No. You can modify it to Yes.
- **Restrict Outgoing SMSs to**: By default, this option is set to No. You can modify it to Yes. This option is shown only if you set **Yes** in Restrict Outgoing SMSs. This field even takes the regular expression for a list of all numbers to be blocked.
- **Restrict Incoming calls**: By default, this option is set to No. You can modify it to Yes.
- **Restrict Incoming Calls from**: By default, this option is set to No. You can modify it to Yes.
  This option is shown only if you set **Yes** in Restrict Incoming calls. This field even takes the regular expression for a list of all numbers to be blocked. For more information, see tool tips.
- **Restrict Incoming SMSs**: By default, this option is set to No. You can modify it to Yes.
- **Restrict Incoming SMSs from**: By default, this option is set to No. You can modify it to Yes.
  This option is shown only if you set **Yes** in Restrict Incoming SMSs. This field even takes the regular expression for a list of all numbers to be blocked.
- **Enable only Emergency Calls**: By default, this option is set to No. You can modify it to Yes.



	Per Day	Per Week	Per Month
Set Max Limit of Incoming Voice Calls			
Set Max Limit of Outgoing Voice Calls			
Set Max Limit of Data Transfer			
Set Max Limit on Incoming SMS sent			
Set Max Limit on Outgoing SMS sent			

- **Set Max Limit of Incoming Voice Calls**: You can set three numbers for per day, per week, and per month. When no number is set, the default value “0” which means unlimited.
- **Set Max Limit of Outgoing Voice Calls**: You can set three numbers for per day, per week and per month. When no number is set, this is set to default value “0” that means unlimited.
- **Set Max Limit of Data Transfer**: You can set three numbers for per day, per week and per month. When no number is set, this is set to default value “0” that means unlimited.
- **Set Max Limit on Incoming SMS sent**: You can set three numbers for per day, per week and per month. When no number is set, this is set to default value “0” that means unlimited.
- **Set Max Limit on Outgoing SMS sent**: You can set three numbers for per day, per week and per month. When no number is set, this is set to default value “0” that means unlimited.

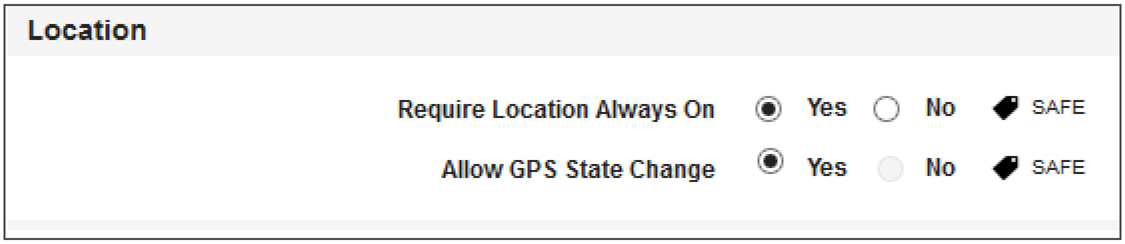


Date Time

Use Network Provided Date & Time ● Yes ○ No

Allow Date Time Change ○ Yes ● No SAFE

- **Use Network Provided Date & Time**: By default, this option is set to Yes. You can modify it to No.
- **Allow Date Time Change**: By default, this option is set to No. You can modify it to Yes.

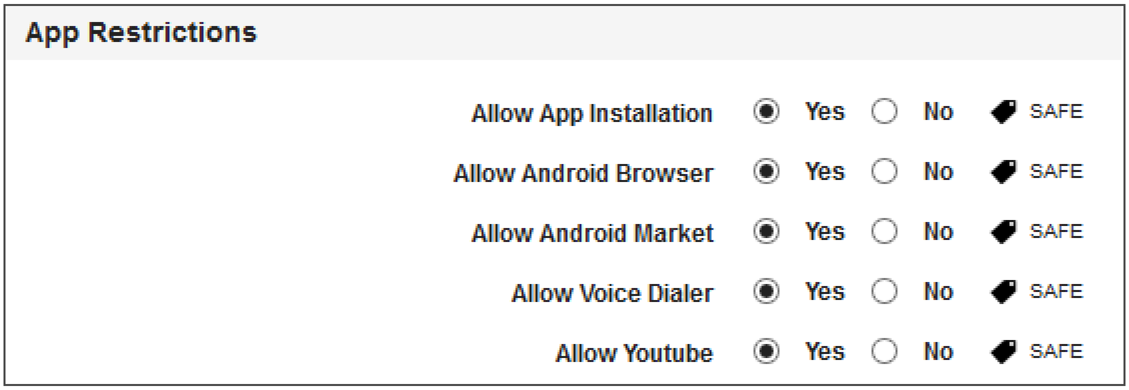


Location

Require Location Always On ● Yes ○ No SAFE

Allow GPS State Change ● Yes ○ No SAFE

- **Require Location Always On**: By default, this option is set to Yes. You can modify it to No.
- **Allow GPS State Change**: By default, this option is set to Yes. You can modify it to No.



App Restrictions

Allow App Installation ● Yes ○ No SAFE

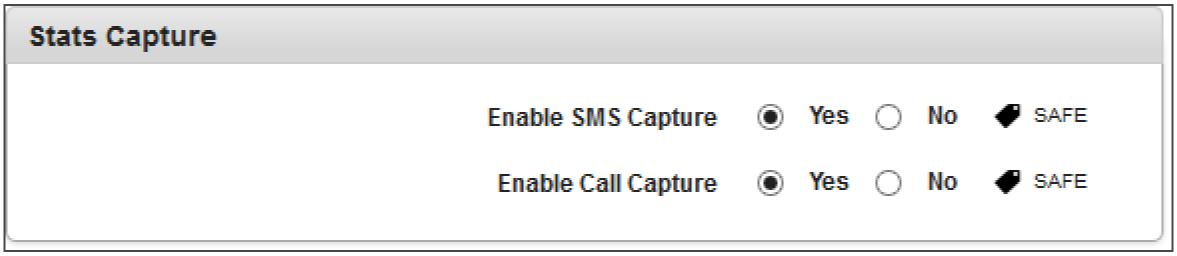
Allow Android Browser ● Yes ○ No SAFE

Allow Android Market ● Yes ○ No SAFE

Allow Voice Dialer ● Yes ○ No SAFE

Allow Youtube ● Yes ○ No SAFE

- **Allow App Installation**: By default, this option is set to Yes. You can modify it to No.
- **Allow Android Browser**: By default, this option is set to Yes. You can modify it to No.
- **Allow Android Market**: By default, this option is set to Yes. You can modify it to No.
- **Allow Voice Dialer**: By default, this option is set to Yes. You can modify it to No.
- **Allow Youtube:** By default, this option is set to Yes. You can modify it to No.

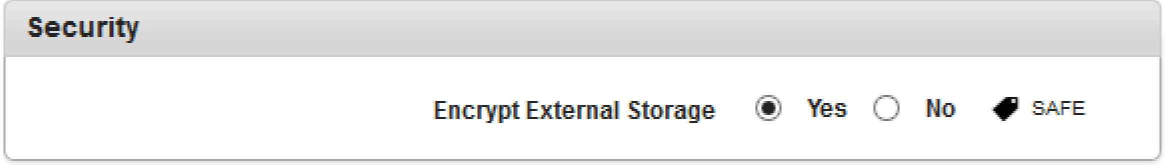


Stats Capture

Enable SMS Capture ● Yes ○ No SAFE

Enable Call Capture ● Yes ○ No SAFE

- **Enable SMS Capture**: By default, this option is set to Yes. You can modify it to No.
- **Enable Call Capture**: By default, this option is set to Yes. You can modify it to No.



Security

Encrypt External Storage ● Yes ○ No SAFE

- **Encrypt External Storage**: By default, this option is set to Yes. You can modify it to No.

2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

> *Note:* If you disable Settings such as **Allow Settings Changes**, **Allow Wi-Fi**, **Factory Reset**, **Block Installation of Non Trusted Apps**, and **Allow Cellular Data**, the device can not communicate later on with the server (due to no network as you have disabled all the mentioned above). To avoid blocking the device from communicating with the server, ensure that you enable atleast one of the above settings.

Call restrictions Code Examples

The following section provides information on examples for call restrictions.

Restricting Outgoing Calls

To restrict outgoing calls, use the following:

- To block all calls: ___.*___
- To block phone numbers starting with +11 or 11: ___^\+{0,1}11.*$___
- To block phone numbers ending with 789: ___.*789$___
- To block phone numbers not ending with 789: ___^(?!.*789$).*___
- To block phone numbers not containing 789: ___^(?!.*789.*).*___
- To block phone numbers containing 789: ___^(.*789.*)___
- To block all phone numbers other than 911: ___^(?!911$).*___
- To block all numbers except numbers like 1-123-XXX-XXXX or 1123XXXXXXX or 123-XXX-XXX or 123XXXXXX ___(?![1]?[\-]?123[\-]?[0-9]{3}[\-]?[0-9]{4}$).*___

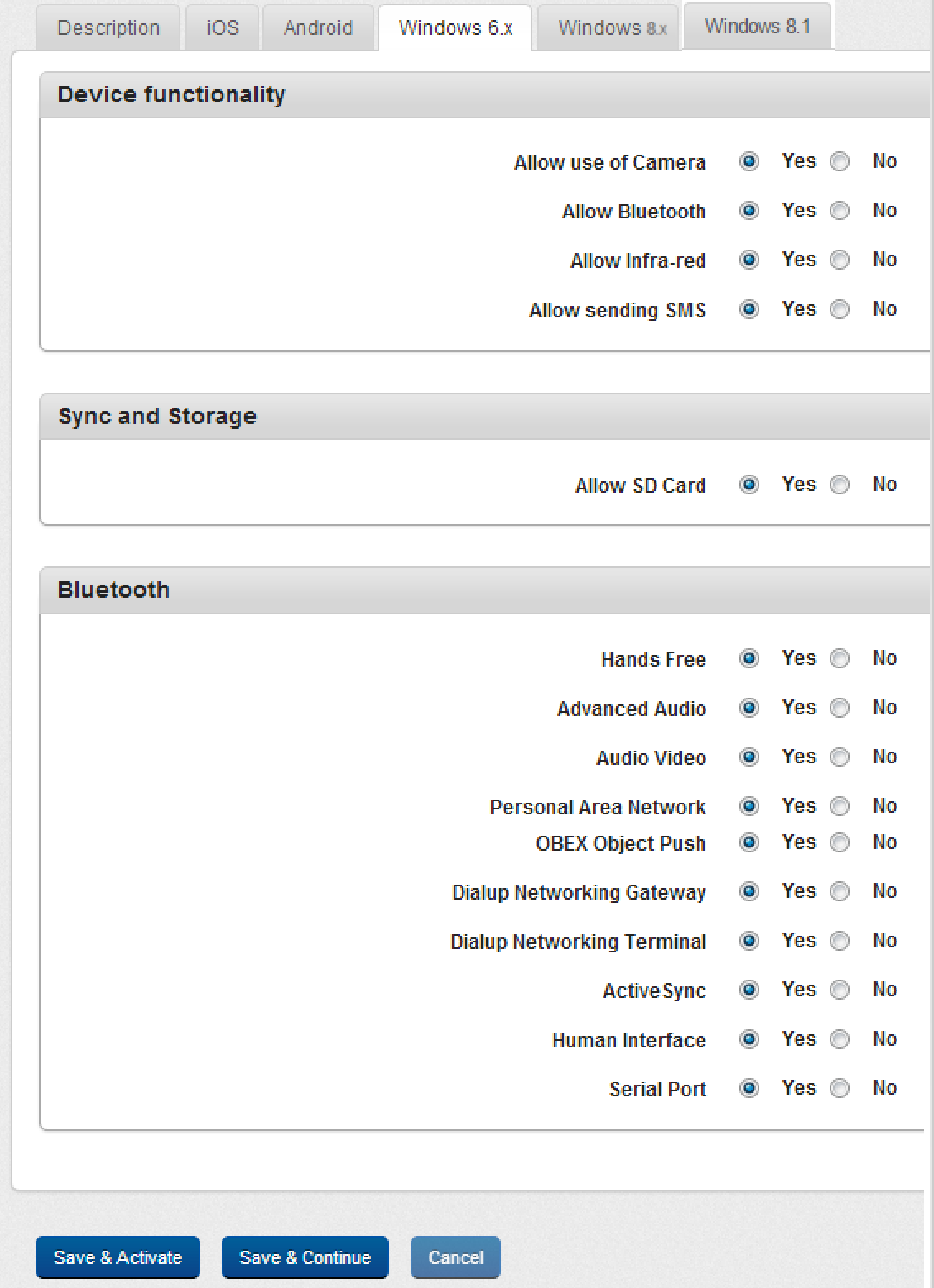
Restricting Incoming Calls

To restrict incoming calls, use the following:

- To block all calls: ___.*___
- To block phone numbers starting with +11 or 11: ___^\+{0,1}11.*$___
- To block phone numbers ending with 789: ___.*789$___
- To block phone numbers not ending with 789: ___^(?!.*789$).*___
- To block phone numbers not containing 789: ___^(?!.*789.*).*___
- To block phone numbers containing 789: ___^(.*789.*)___
- To block all numbers except numbers like 1-123-XXX-XXXX or 1123XXXXXXX or 123-XXX-XXX or 123XXXXXX ___(?![1]?[\-]?123[\-]?[0-9]{3}[\-]?[0-9]{4}$).*___

10.4.3.3 Device Restriction Policy for Windows 6.x

1. To set device restrictions policy for Windows 6.x, follow these steps:



Device functionality

Allow use of Camera ● Yes ○ No

Allow Bluetooth ● Yes ○ No

Allow Infra-red ● Yes ○ No

Allow sending SMS ● Yes ○ No

Sync and Storage

Allow SD Card ● Yes ○ No

Bluetooth

Hands Free ● Yes ○ No

Advanced Audio ● Yes ○ No

Audio Video ● Yes ○ No

Personal Area Network ● Yes ○ No

OBEX Object Push ● Yes ○ No

Dialup Networking Gateway ● Yes ○ No

Dialup Networking Terminal ● Yes ○ No

ActiveSync ● Yes ○ No

Human Interface ● Yes ○ No

Serial Port ● Yes ○ No

a. **Allow Use of Camera**: By default, this option is set to Yes. You can modify it to No.

b. **Allow Bluetooth**: By default, this option is set to Yes. You can modify it to No.

c. **Allow Infra-red**: By default, this option is set to Yes. You can modify it to No.

d. **Allow Sending SMS**: By default, this option is set to Yes. You can modify it to No.

e. **Allow SD Card**: By default, this option is set to Yes. You can modify it to No.

f. **Hands Free**: By default, this option is set to Yes. You can modify it to No.

g. **Advanced Audio**: By default, this option is set to Yes. You can modify it to No.

h. **Audio Video**: By default, this option is set to Yes. You can modify it to No.

i. **Personal Area Network**: By default, this option is set to Yes. You can modify to No.

j. **OBEX Object Push**: By default, this option is set to Yes. You can modify it to No.

   OBEX Object Push is a communications protocol that facilitates the exchange of binary objects between devices.

k. **Dialup Networking Gateway**: By default, this option is set to Yes. You can modify it to No.

l. **Dialup Networking Terminal**: By default, this option is set to Yes. You can modify it to No.

m. **Active Sync**: By default, this option is set to Yes. You can modify it to No.

n. **Human Interface**: By default, this option is set to Yes. You can modify it to No.

o. **Serial Port**: By default, this option is set to Yes. You can modify it to No.

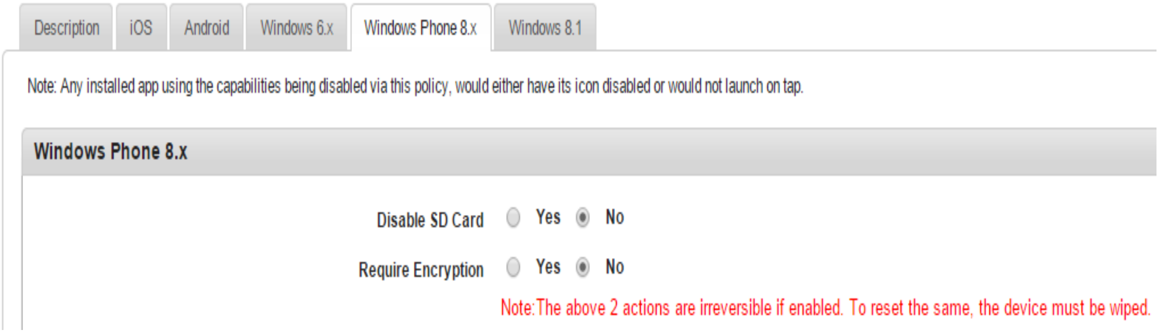
2. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

3. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.3.4 Device Restriction Policy for Windows 8.x

1. To set device restrictions policy for Windows 8, follow these steps:



Note: Any installed app using the capabilities being disabled via this policy, would either have its icon disabled or would not launch on tap.

Windows Phone 8.x

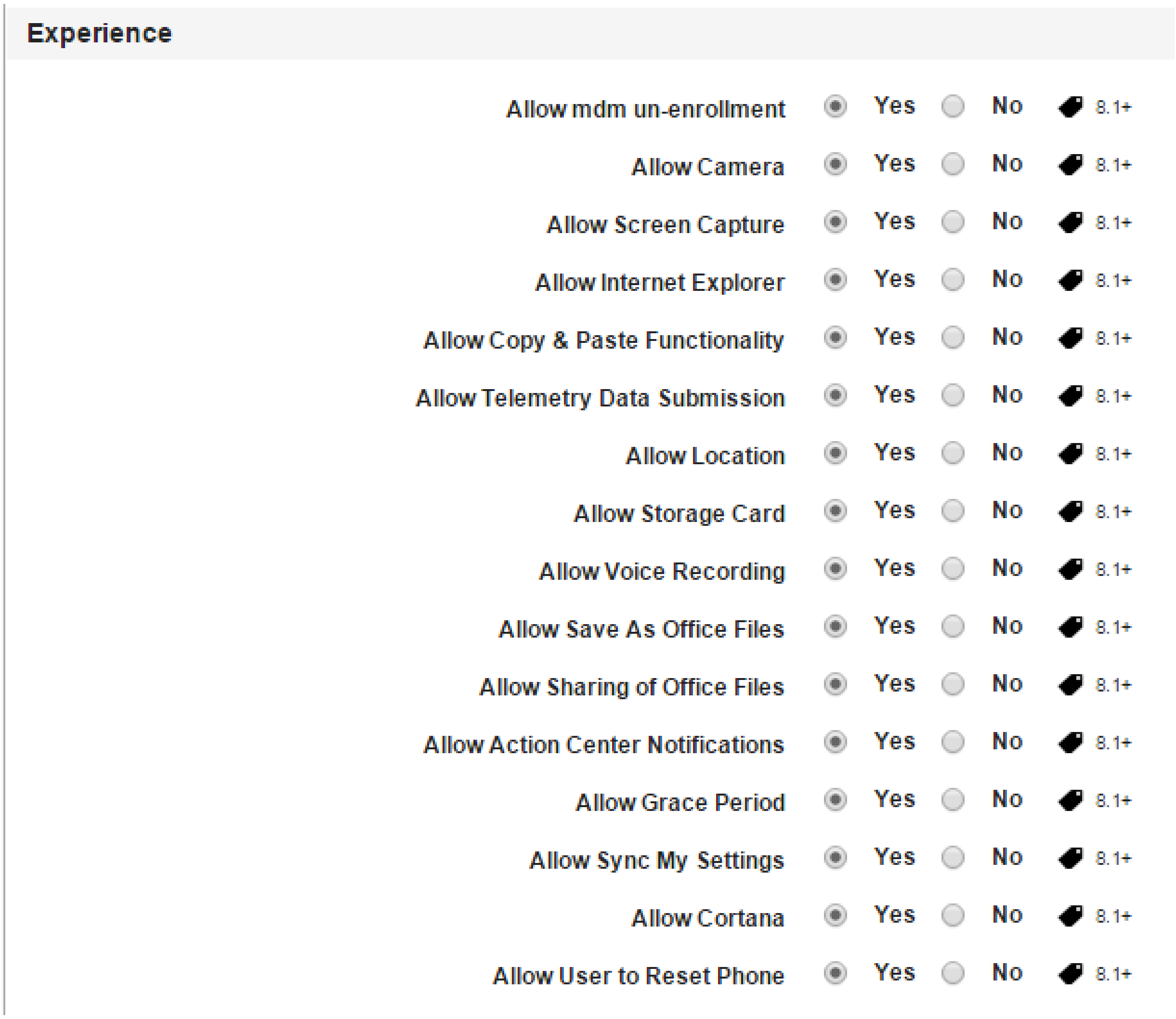
Disable SD Card ○ Yes ● No

Require Encryption ○ Yes ● No

Note:The above 2 actions are irreversible if enabled. To reset the same, the device must be wiped.

2. **Disable SD Card**: By default, this option is set to **Yes**. You can modify it to **No.**

3. **Require Encryption**: By default, this option is set to **Yes**. You can modify it to **No**.



Experience

Allow mdm un-enrollment	● Yes	○ No	8.1+
Allow Camera	● Yes	○ No	8.1+
Allow Screen Capture	● Yes	○ No	8.1+
Allow Internet Explorer	● Yes	○ No	8.1+
Allow Copy & Paste Functionality	● Yes	○ No	8.1+
Allow Telemetry Data Submission	● Yes	○ No	8.1+
Allow Location	● Yes	○ No	8.1+
Allow Storage Card	● Yes	○ No	8.1+
Allow Voice Recording	● Yes	○ No	8.1+
Allow Save As Office Files	● Yes	○ No	8.1+
Allow Sharing of Office Files	● Yes	○ No	8.1+
Allow Action Center Notifications	● Yes	○ No	8.1+
Allow Grace Period	● Yes	○ No	8.1+
Allow Sync My Settings	● Yes	○ No	8.1+
Allow Cortana	● Yes	○ No	8.1+
Allow User to Reset Phone	● Yes	○ No	8.1+

4. **Allow mdm un-enrollment**: By default, this option is set to **Yes**. You can modify it to **No**.

5. **Allow Camera**: By default, this option is set to **Yes**. You can modify it to **No**.

6. **Allow Screen Capture**: By default, this option is set to **Yes**. You can modify it to **No**.

7. **Allow Internet Explorer**: By default, this option is set to **Yes**. You can modify it to **No**.

8. **Allow Copy & Paste Functionality**: By default, this option is set to **Yes**. You can modify it to **No**.

9. **Allow Telemetry Data Submission**: By default, this option is set to **Yes**. You can modify it to

No.

10. **Allow Location**: By default, this option is set to **Yes**. You can modify it to **No**.

11. **Allow Storage Card**: By default, this option is set to **Yes**. You can modify it to **No**.

12. **Allow Voice Recording**: By default, this option is set to **Yes**. You can modify it to **No**.

13. **Allow Save As Office Files**: By default, this option is set to **Yes**. You can modify it to **No**.

14. **Allow Sharing of Office Files**: By default, this option is set to **Yes**. You can modify it to **No**.

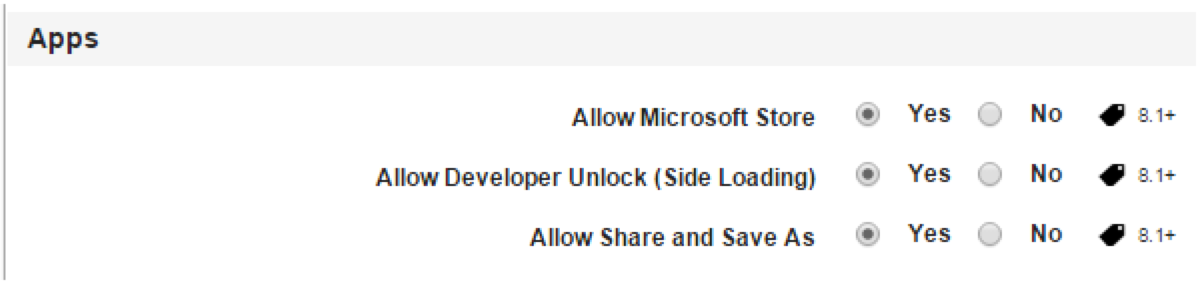
15. **Allow Action Center Notifications**: By default, this option is set to **Yes**. You can modify it to **No**.

16. **Allow Grace Period**: By default, this option is set to **Yes**. You can modify it to **No**.

17. **Allow Sync My Settings**: By default, this option is set to **Yes**. You can modify it to **No**.

18. **Allow Cortana**: By default, this option is set to **Yes**. You can modify it to **No**.

19. **Allow User to Reset Phone**: By default, this option is set to **Yes**. You can modify it to **No**.



Apps

Allow Microsoft Store ● Yes ○ No 8.1+

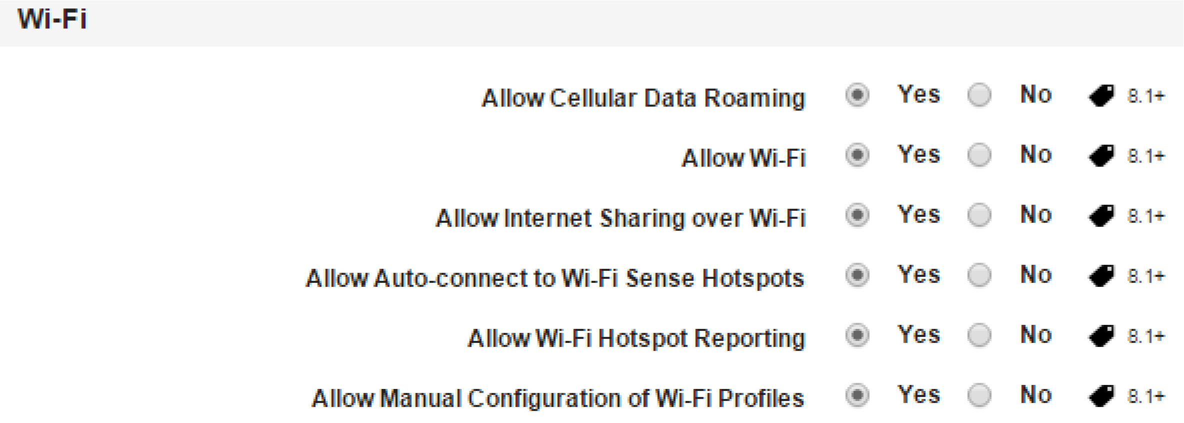
Allow Developer Unlock (Side Loading) ● Yes ○ No 8.1+

Allow Share and Save As ● Yes ○ No 8.1+

20. **Allow Microsoft Store**: By default, this option is set to **Yes**. You can modify it **to** No.

21. **Allow Developer Unlock (Side Loading)**: By default, this option is set to **Yes**. You can modify it to **No**.

22. **Allow Share and Save As**: By default, this option is set to **Yes**. You can modify it to **No**.



Wi-Fi

Allow Cellular Data Roaming ● Yes ○ No 8.1+

Allow Wi-Fi ● Yes ○ No 8.1+

Allow Internet Sharing over Wi-Fi ● Yes ○ No 8.1+

Allow Auto-connect to Wi-Fi Sense Hotspots ● Yes ○ No 8.1+

Allow Wi-Fi Hotspot Reporting ● Yes ○ No 8.1+

Allow Manual Configuration of Wi-Fi Profiles ● Yes ○ No 8.1+

23. **Allow Cellular Data Roaming**: By default, this option is set to **Yes**. You can modify it to **No**.

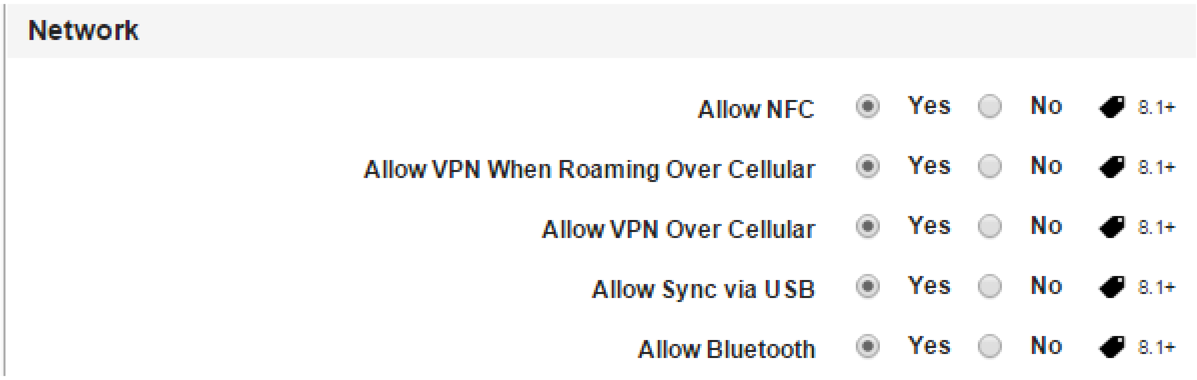
24. **Allow Wi-Fi**: By default, this option is set to **Yes**. You can modify it to **No**.

25. **Allow Internet Sharing over Wi-Fi**: By default, this option is set to **Yes**. You can modify it to **No**.

26. **Allow Auto-connect to Wi-Fi Sense Hotspots**: By default, this option is set to **Yes**. You can modify it to **No**.

27. **Allow Wi-Fi Hotspot Reporting**: By default, this option is set to **Yes**. You can modify it to **No**.

28. **Allow Manual Configuration of Wi-Fi Profiles**: By default, this option is set to Yes. You can modify it to **No**.



Network

Allow NFC ● Yes ○ No 8.1+

Allow VPN When Roaming Over Cellular ● Yes ○ No 8.1+

Allow VPN Over Cellular ● Yes ○ No 8.1+

Allow Sync via USB ● Yes ○ No 8.1+

Allow Bluetooth ● Yes ○ No 8.1+

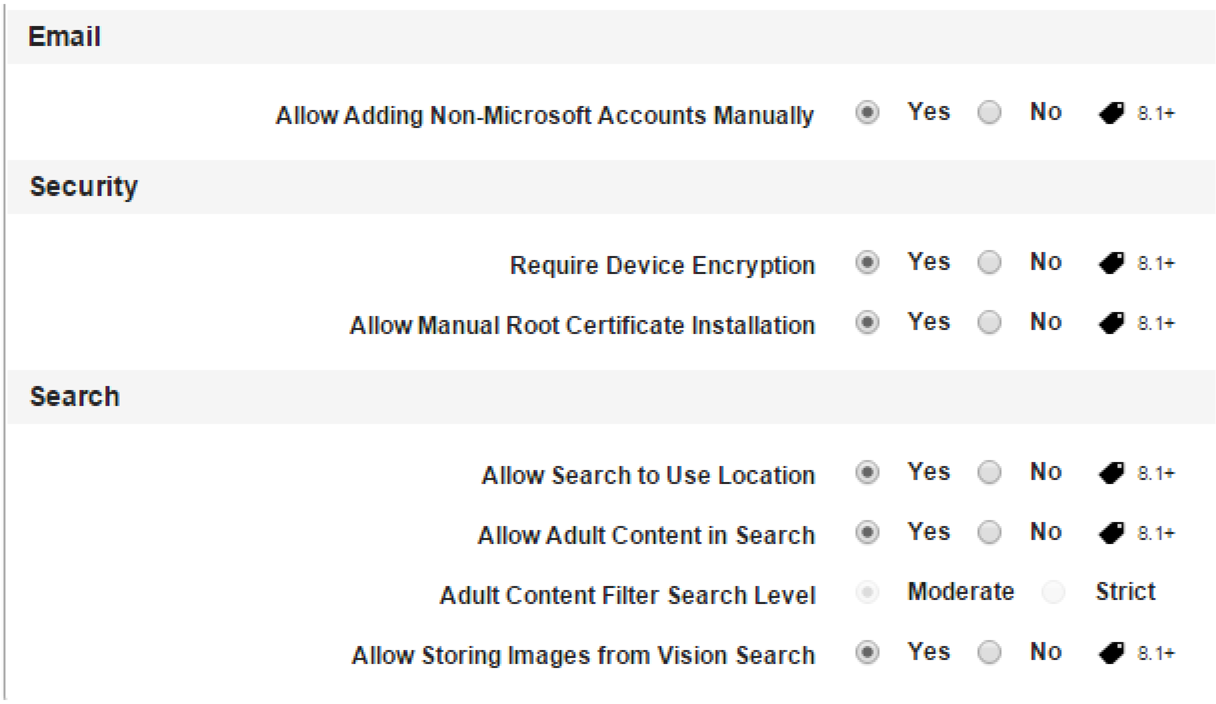
29. **Allow NFC**: By default, this option is set to **Yes**. You can modify it to **No**.

30. **Allow VPN When Roaming Over Cellular**: By default, this option is set to **Yes**. You can modify it to **No**.

31. **Allow VPN Over Cellular**: By default, this option is set to **Yes**. You can modify it to **No**.

32. **Allow Sync via USB**: By default, this option is set to **Yes**. You can modify it to **No**.

33. **Allow Bluetooth**: By default, this option is set to **Yes**. You can modify it to **No**.



Email

Allow Adding Non-Microsoft Accounts Manually ● Yes ○ No 8.1+

Security

Require Device Encryption ● Yes ○ No 8.1+

Allow Manual Root Certificate Installation ● Yes ○ No 8.1+

Search

Allow Search to Use Location ● Yes ○ No 8.1+

Allow Adult Content in Search ● Yes ○ No 8.1+

Adult Content Filter Search Level ● Moderate ○ Strict

Allow Storing Images from Vision Search ● Yes ○ No 8.1+

34. **Allow Adding Non-Microsoft Accounts Manually**: By default, this option is set to **Yes**. You can modify it to **No**.

35. **Require Device Encryption**: By default, this option is set to **Yes**. You can modify it to **No**.

36. **Allow Manual Root Certificate Installation**: By default, this option is set to **Yes**. You can modify it to **No**.

37. **Allow Search to Use Location**: By default, this option is set to **Yes**. You can modify it to **No**.

38. **Allow Adult Content in Search**: By default, this option is set to **Yes**. You can modify it to **No**.

39. **Adult Content Filter Search Level**: By default, this option is set to **Yes**. You can modify it to **No**.

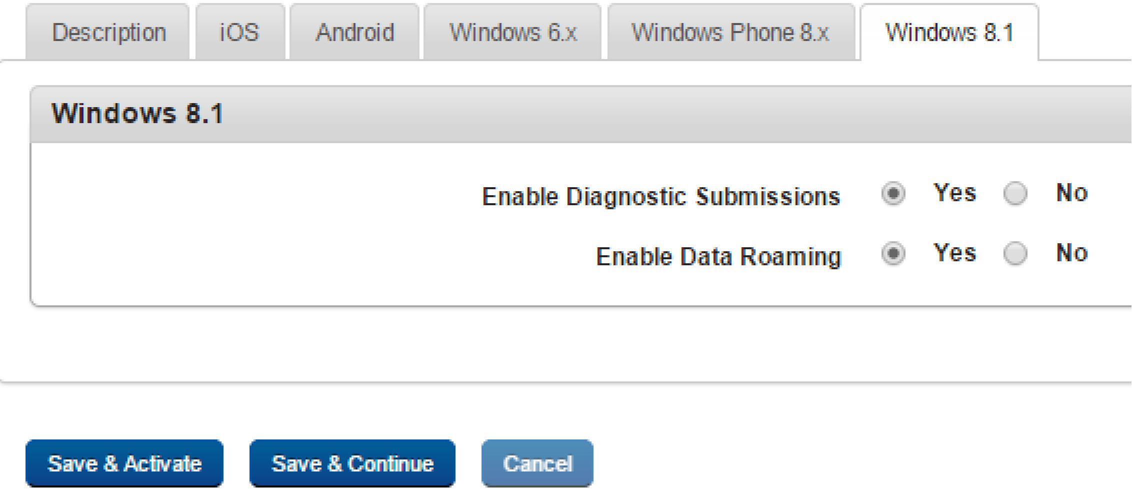
40. **Allow Storing Images from Vision Search**: By default, this option is set to **Yes**. You can modify it to **No**.

41. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

42. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

10.4.3.5 Device Restriction Policy for Windows 8.1

To set device restrictions policy for Windows 8.1, follow these steps:



Windows 8.1

Enable Diagnostic Submissions ● Yes ○ No

Enable Data Roaming ● Yes ○ No

1. **Enable Diagnostic Submissions**: By default, this option is set to **No**. You can modify it to **Yes**.

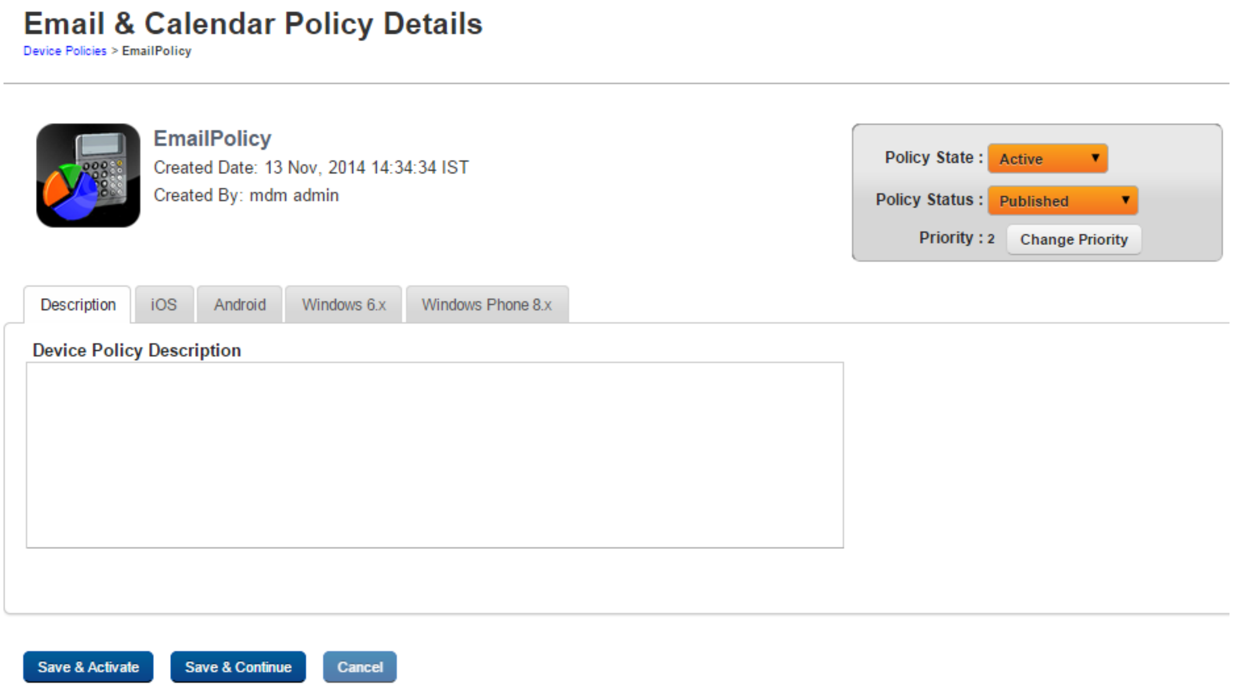
2. **Enable Data Roaming**: By default, this option is set to **No**. You can modify it to **Yes**.

3. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

4. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

10.4.4 Email and Calendar Policy

The primary purpose of the email and calendar policy is to configure email and calendar settings for a user based on existing business rules. This policy ensures that email settings are configured, and a device user can access an email account.



Email & Calendar Policy Details

Device Policies > EmailPolicy

EmailPolicy

Created Date: 13 Nov, 2014 14:34:34 IST

Created By: mdm admin

Policy State : Active

Policy Status : Published

Priority : 2

Device Policy Description

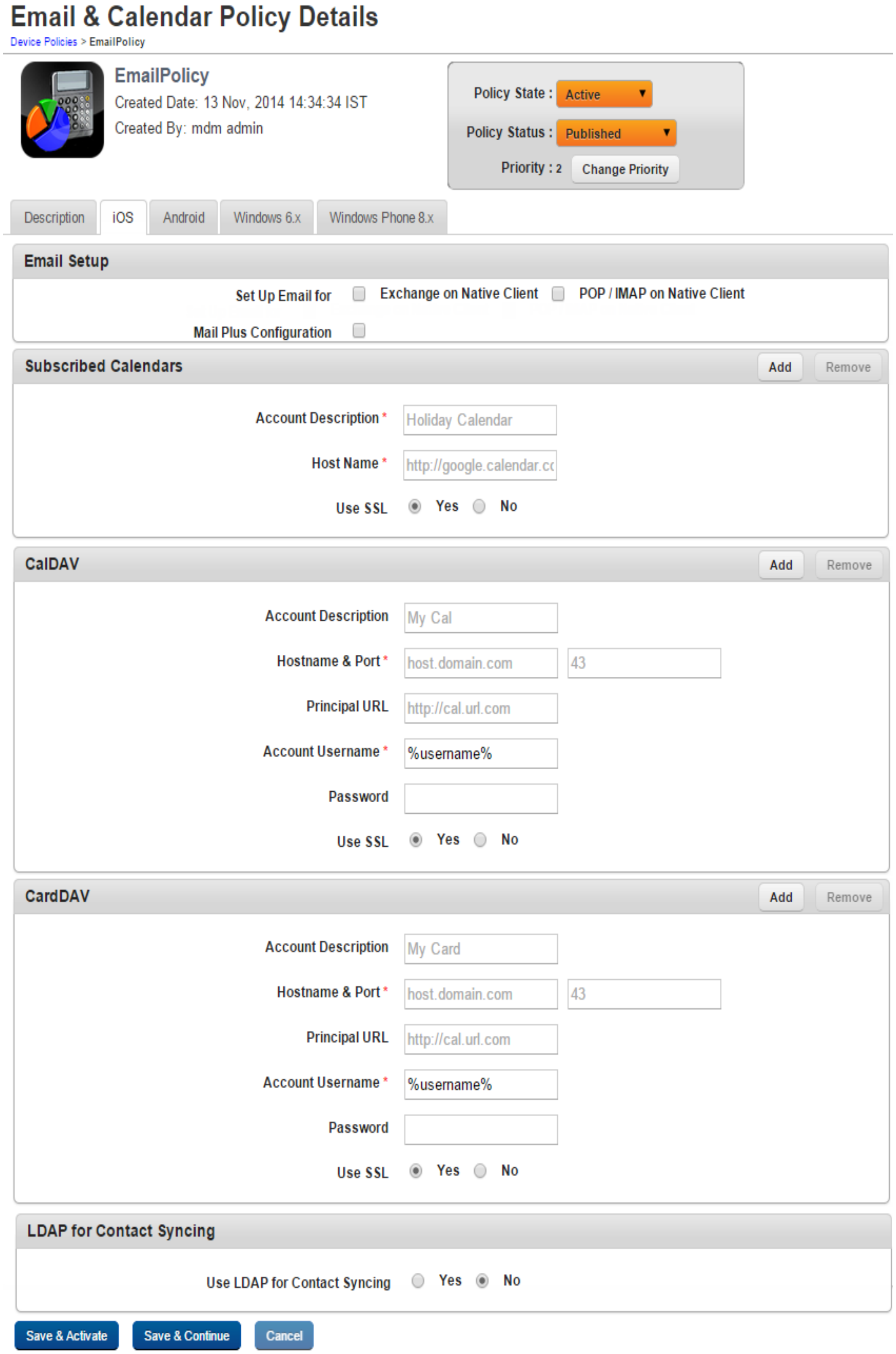
You can set email and calendar policy for the following operating systems:

- Set Email and Calendar Policy for iOS
- Set Email and Calendar Policy for Android

- Set Email and Calendar for Windows 6.x
- Set Email and Calendar Policy for Windows Phone 8.x

10.4.4.1 Set Email and Calendar Policy for iOS

The email policy for an iOS page includes following sections:



Email & Calendar Policy Details

Device Policies > EmailPolicy

EmailPolicy

Created Date: 13 Nov, 2014 14:34:34 IST

Created By: mdm admin

Policy State : Active

Policy Status : Published

Priority : 2

Email Setup

Set Up Email for □ Exchange on Native Client □ POP / IMAP on Native Client

Mail Plus Configuration □

Subscribed Calendars

Account Description * Holiday Calendar

Host Name * http://google.calendar.cc

Use SSL ● Yes ○ No

CalDAV

Account Description My Cal

Hostname & Port * host.domain.com 43

Principal URL http://cal.url.com

Account Username * %username%

Password

Use SSL ● Yes ○ No

CardDAV

Account Description My Card

Hostname & Port * host.domain.com 43

Principal URL http://cal.url.com

Account Username * %username%

Password

Use SSL ● Yes ○ No

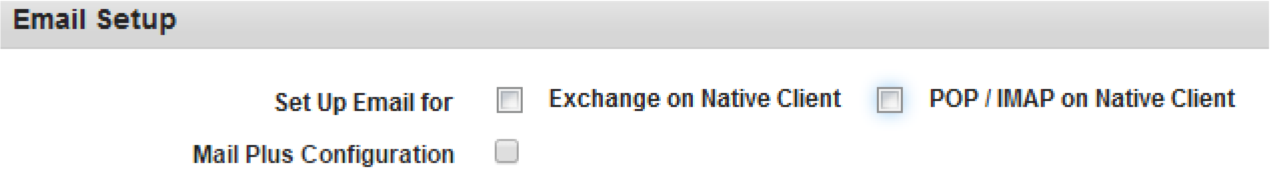
LDAP for Contact Syncing

Use LDAP for Contact Syncing ○ Yes ● No

- Email Setup
- Subscribed Calendars
- CalDAV
- CardDAV
- LDAP for Contact Syncing

Email Setup

Email Setup section includes two options.



Email Setup

Set Up Email for □ Exchange on Native Client □ POP / IMAP on Native Client

Mail Plus Configuration □

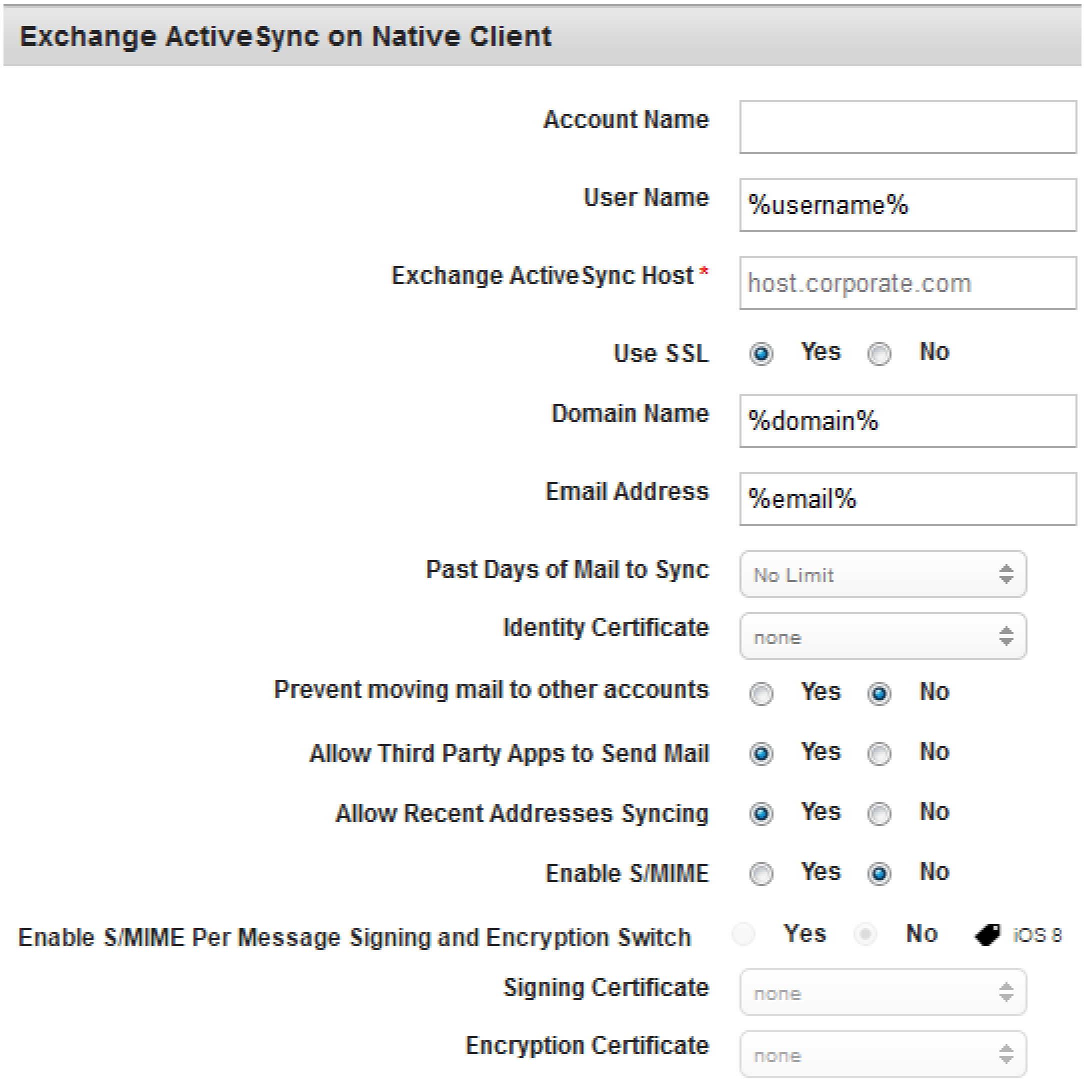
- Exchange on Native Client
- POP/MAP on Native Client
- Mail Plus Configuration

You can configure these options.

Exchange on Native Client

Select the check box to display Exchange on Native Client window.

To set up Exchange on Native Client functionality, follow these steps:



Exchange ActiveSync on Native Client

Account Name	
User Name	%username%
Exchange ActiveSync Host *	host.corporate.com
Use SSL	● Yes ○ No
Domain Name	%domain%
Email Address	%email%
Past Days of Mail to Sync	No Limit
Identity Certificate	none
Prevent moving mail to other accounts	○ Yes ● No
Allow Third Party Apps to Send Mail	● Yes ○ No
Allow Recent Addresses Syncing	● Yes ○ No
Enable S/MIME	○ Yes ● No
Enable S/MIME Per Message Signing and Encryption Switch	○ Yes ○ No iOS 8
Signing Certificate	none
Encryption Certificate	none

1. **Account Name**: Enter the Account name.

2. **User Name**: Enter the User name.

3. **Exchange Active Sync Host**: Enter the host URL address.

4. **Use SSL**: By default, this option is set to Yes. You can modify it to No.

5. **Domain Name**: Enter the domain details.

6. **Email Address**: Enter the email address of the Administrator.

7. **Past Days of Mail to Sync**: Select the required option from the drop-down list. By default, it is set to No-Limit.

8. **Identity Certificate**: Select the required option from the drop-down list. By default, it is set to None.

9. **Prevent Moving Mail to Other Accounts**: By default, this option is set to No. You can modify it to Yes.

10. **Allow Third Party Apps to Send Mail**: By default, this option is set to Yes. You can modify it to No.

11. **Allow Recent Addresses Syncing**: By default, this option is set to Yes. You can modify it to No.

12. **Enable S/MME**: By default, this option is set to No. If you select the option as Yes, then Signing Certificate and Encryption Certificate fields become active.

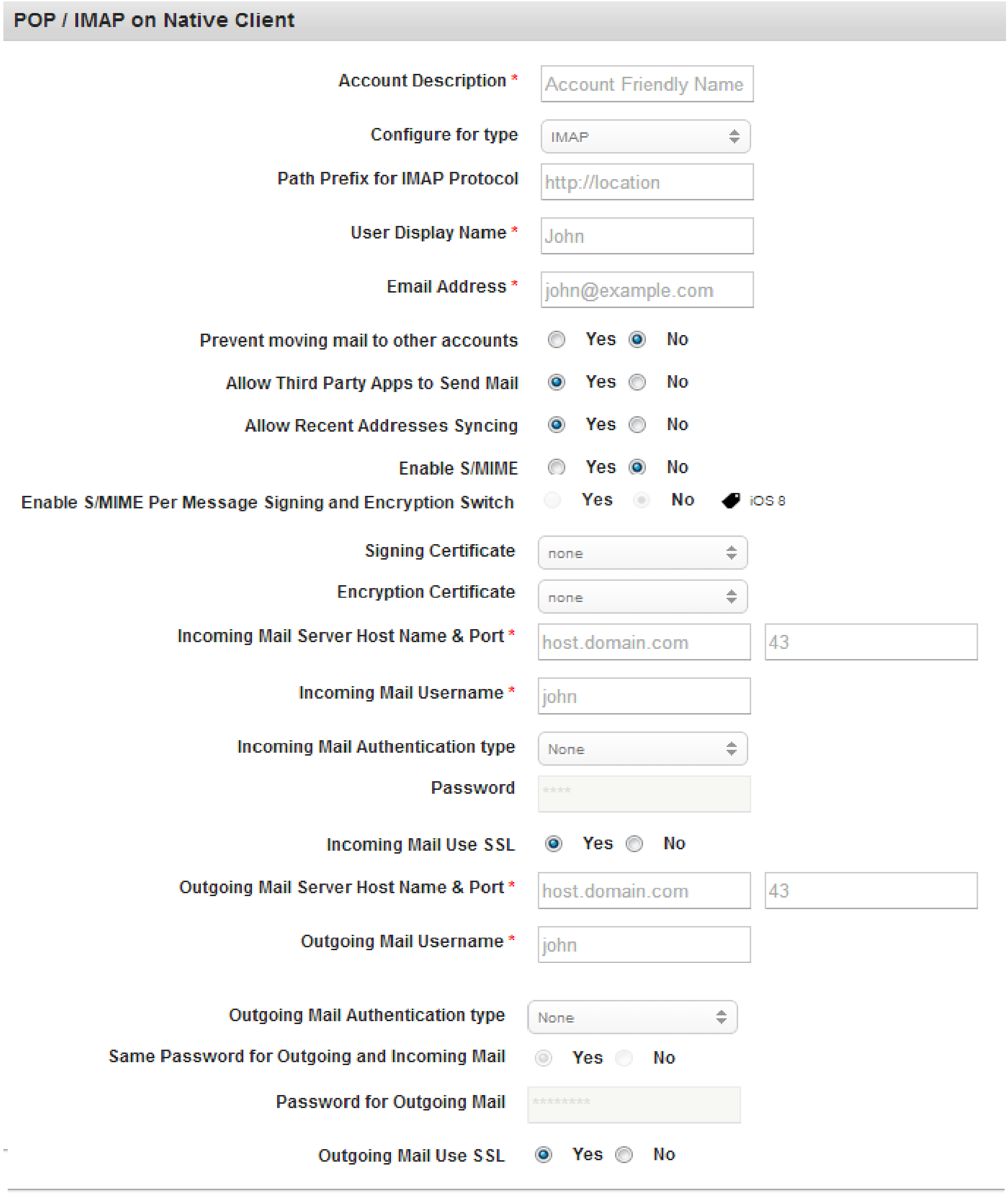
13. **Enable S/MME Per Message Signing and Encryption Switch**: By default, this option is set to No. If you select the option as Yes, then you can choose to sign and encrypt each message before you send it out. This feature is available only on iOS 8.

14. **Signing Certificate**: Select the required signing certificate from the drop-down list. By default, it is set to None.

15. **Encryption Certificate**: Select the required signing certificate from the drop-down menu. By default, it is set to None.

POP/MAP on Native Client

Select the check box to display POP/MAP on Native Client window



POP / IMAP on Native Client

Account Description * Account Friendly Name

Configure for type IMAP

Path Prefix for IMAP Protocol http://location

User Display Name * John

Email Address * john@example.com

Prevent moving mail to other accounts ○ Yes ● No

Allow Third Party Apps to Send Mail ● Yes ○ No

Allow Recent Addresses Syncing ● Yes ○ No

Enable S/MIME ○ Yes ● No

Enable S/MIME Per Message Signing and Encryption Switch ○ Yes ○ No iOS 8

Signing Certificate none

Encryption Certificate none

Incoming Mail Server Host Name & Port * host.domain.com 43

Incoming Mail Username * john

Incoming Mail Authentication type None

Password ****

Incoming Mail Use SSL ● Yes ○ No

Outgoing Mail Server Host Name & Port * host.domain.com 43

Outgoing Mail Username * john

Outgoing Mail Authentication type None

Same Password for Outgoing and Incoming Mail ○ Yes ○ No

Password for Outgoing Mail ********

Outgoing Mail Use SSL ● Yes ○ No

To setup Exchange on **POP/MAP Native Client** functionality, follow these steps:

1. **Account Description**: Enter the Account name.
2. **Configure for Type**: Select the required option from the drop-down list.
3. **Path Prefix for IMAP Protocol**: Enter the address for IMAP protocol.

4. **User Display Name**: Enter the user name for display.
5. **Email Address**: Enter email address of the user.
6. **Prevent moving mail to other Accounts**: By default, this option is set to No. You can modify it to Yes.
7. **Allow Third Party Apps to Send Mail**: By default, this option is set to Yes. You can modify it to No.
8. **Allow Recent Addresses Syncing**: By default, this option is set to Yes. You can modify it to No
9. **Enable S/MIME**: By default, this option is set to No. You can modify it to Yes.
10. **Enable S/MME Per Message Signing and Encryption Switch**: By default, this option is set to No. If you select the option as Yes, then you can choose to sign and encrypt each message before you send it out. This feature is available only on iOS8.
11. **Signing Certificate**: Select the required certificate from the drop-down list. By default,this option is set to None.
12. **Encryption Certificate**: Select the required certificate from the drop-down list. By default this option is set to None.
13. **Incoming Mail server Host Name & Port**: Enter the host name and the port number.
14. **Incoming Mail Username**: Enter the user name for all the incoming mails.
15. **Incoming Mail Authentication type**: Select the required incoming mail authentication type from the drop-down list. By default it is set to None. if you select the option as Password, then Password field becomes active.
16. **Password:** Enter the password.
17. **Incoming Mail Use SS**L: By default this option is set to Yes. You can modify it to No.
18. **Outgoing Mail server Host Name and Port**: Enter the host name and the port number for the out going mail.

19. **Outgoing Mail User Name**: Enter the user name for the out going mail.
20. **Outgoing Mail Authentication type**: Select the required outgoing mail authentication type from the drop-down list. If you select the option as Yes, then Same Password for Outgoing and Incoming Mail, Password for Outgoing Mail, and Outgoing Mail Use SSL fields becomes active.
21. **Same Password for Outgoing and Incoming Mail**: By default, this option is set to Yes. You can modify it to No. If you select the option as Yes, then Password for Outgoing Mail field become disabled.
22. **Password for Outgoing Mail**: Enter the password for the outgoing mail.
23. **Outgoing Mail Use SSL**: By default, this option is set to Yes. You can modify to No.

Mail Plus Configuration

Select the check box to display Mail Plus for the Enterprise window.

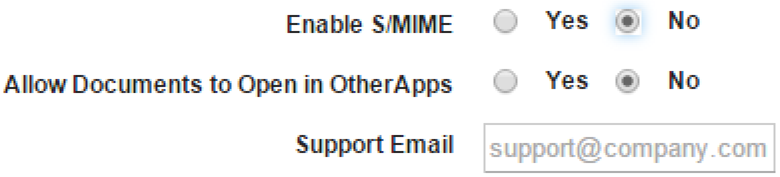
To set up Mail Plus for Enterprise, follow these steps:

1. **User Name**: The default value is %username%.

   > ***Note:*** If you have a single domain, retain default value macro %username%. If you have multiple domains, provide %email% OR %username% in the User Name field.

2. **Exchange Host Name**: Enter your exchange host name.
3. **Email Address**: The default value is %email%.
4. **Allow iTunes Backup**: The default value is **No**. Select **Yes** to enable iTunes backup of the Mail Plus Enterprise App.
5. **Allow Passcode**: The default value is **No**. Select **Yes** to enable a passcode on the Mail Plus Enterprise App.
6. **Enable S/MIME**: The default value is **No**. Select **Yes** to enable Secure/Multipurpose Internet Mail Extensions (SMIME). When you select **Yes**, **Allow Same Certificate for Signing and**

Encryption feature appears.

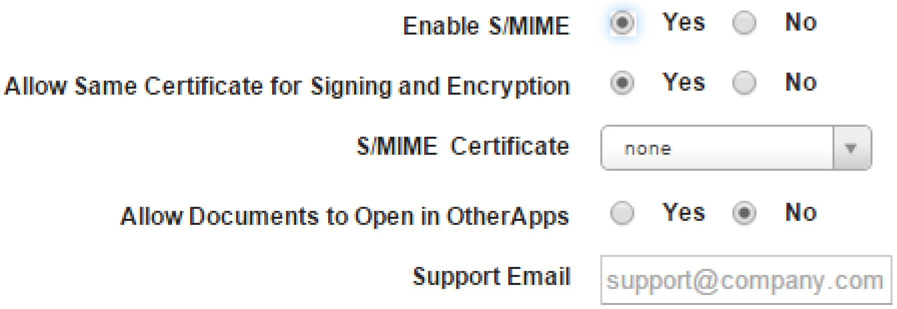


Enable S/MIME ○ Yes ● No

Allow Documents to Open in OtherApps ○ Yes ● No

Support Email support@company.com

7. **Allow Same Certificate for Signing and Encryption:** The default value is **Yes,** which allows you to use one certificate for S/MIME signing and encryption. Select the S/MIME certificate from the list.



Enable S/MIME ● Yes ○ No

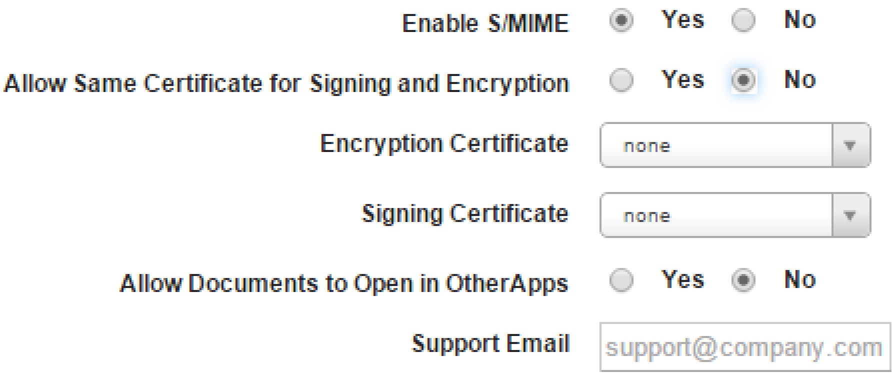
Allow Same Certificate for Signing and Encryption ● Yes ○ No

S/MIME Certificate none

Allow Documents to Open in OtherApps ○ Yes ● No

Support Email support@company.com

If you select **No**, the Encryption and Signing certificate fields appear.



Enable S/MIME ● Yes ○ No

Allow Same Certificate for Signing and Encryption ○ Yes ● No

Encryption Certificate none

Signing Certificate none

Allow Documents to Open in OtherApps ○ Yes ● No

Support Email support@company.com

8. **Encryption Certificate**: Select an encryption certificate from the list.

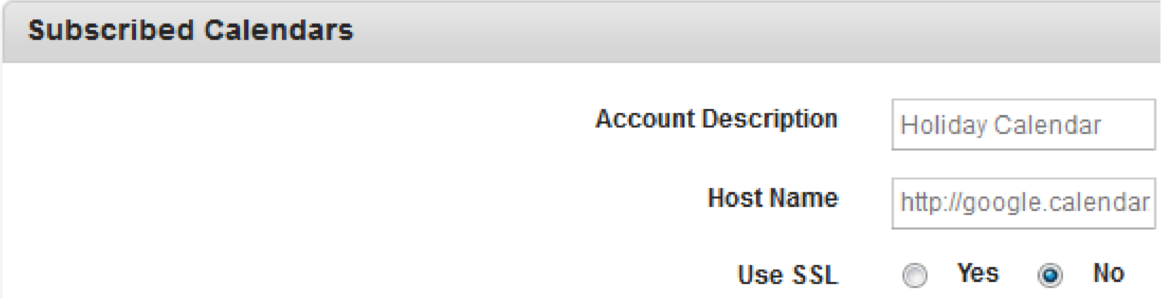
9. **Signing Certificate**: Select a signing certificate from the list.

10. **Allow Documents to Open in Other Apps**: By default, the setting is configured to **No**. Configure to **Yes** if you want to allow documents in the Mail Plus Enterprise app to open in other apps.

11. **Support Email**: Enter the email ID of Mail Plus configuration support.

Subscribed Calendars

1. Enter details for the following fields:



Subscribed Calendars

Account Description: Holiday Calendar

Host Name: http://google.calendar

Use SSL ○ Yes ● No

   a. **Account Description**: Enter the description of the account, such as Holiday Calendar.

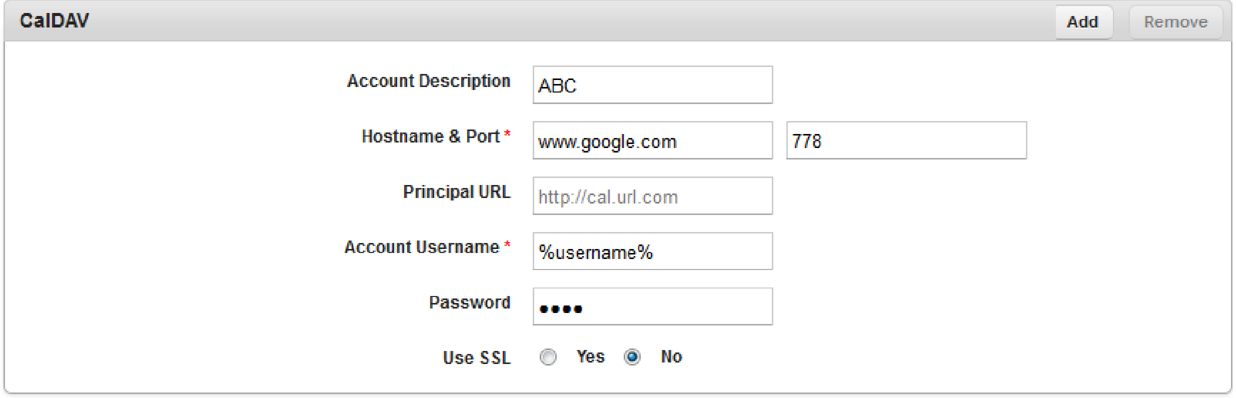
   b. **Host Name**: Enter the Host URL.

   c. **USE SSL**: By default, this option is set to No. You you can modify to Yes.

CalDAV

This option is used to set Dates, Times and Events to sync between the Calendar and the Device.

To set CalDAV properties, follow these steps:



Account Description: ABC

Hostname & Port *: www.google.com 778

Principal URL: http://cal.url.com

Account Username *: %username%

Password: ••••

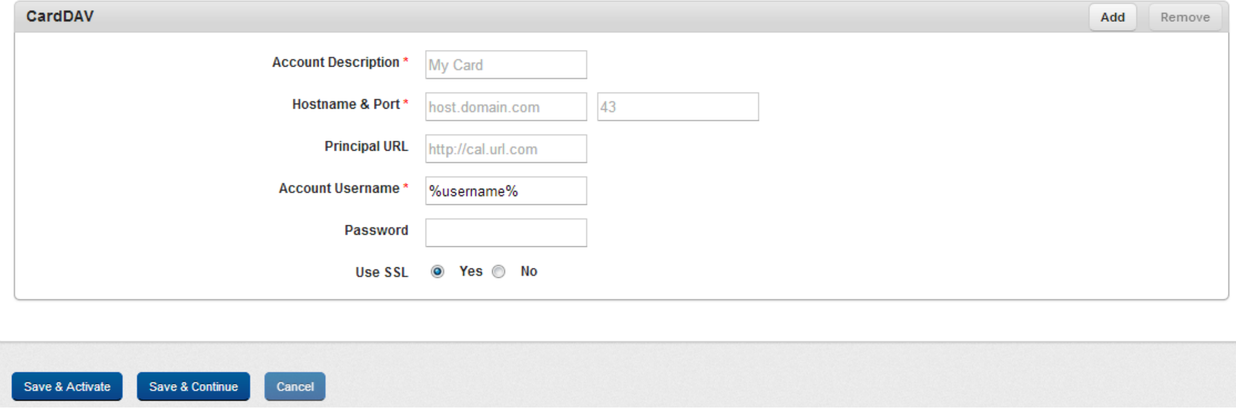
Use SSL ○ Yes ● No

1. **Account Description:** Enter the Account description.
2. **Hostname and Port**: Enter the Host name and Host Port number of the CalDAV account.
3. **Principal URL**: Enter the URL address of CalDAV account.
4. **Account User Name**: Enter the user name.
5. **Password**: The the user password.
6. **Use SSL**: By default, this option is set to Yes. No can modify it to No.

CardDAV

The device user must have his Contact List in sync in order to communicate with contacts across multiple media.

To set CardDAV properties, follow these steps:



Account Description *: My Card

Hostname & Port *: host.domain.com 43

Principal URL: http://cal.url.com

Account Username *: %username%

Password:

Use SSL ● Yes ○ No

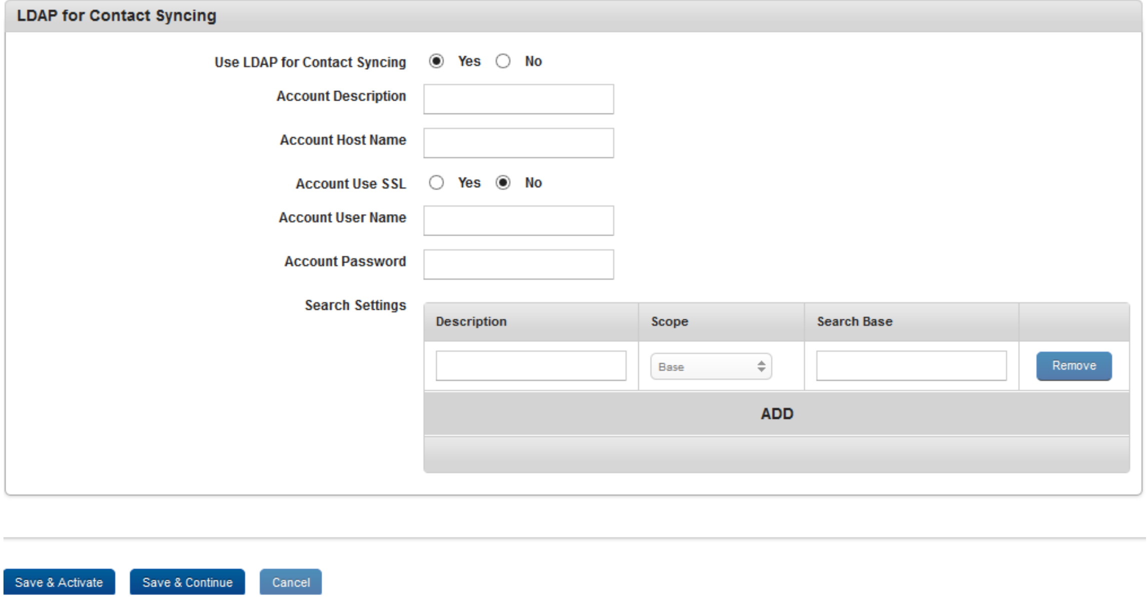
1. **Account Description**: Enter the user account details. This is the display name for the CardDAV account.
2. **Hostname and Port**: Enter the host URL and the Port number.
3. **Principal URL**: Enter the principal URL.
4. **Account User Name**: Enter the account user name for CardDAV.
5. **Password**: Enter the user password.
6. **Use SSL**: By default, this option is set to No. You can modify it to Yes.

> ***Note:*** SSL is used to communicate with CardDAV.

LDAP for Contact Syncing

This option is used to import and sync contacts from LDAP.

To set LDAP for Contact Syncing properties, follow these steps:



LDAP for Contact Syncing

Use LDAP for Contact Syncing ● Yes ○ No

Account Description

Account Host Name

Account Use SSL ○ Yes ● No

Account User Name

Account Password

Search Settings

Description	Scope	Search Base	
	Base		Remove

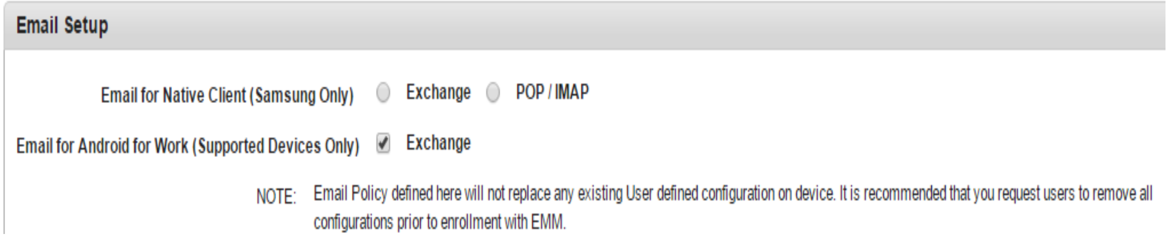
- **Use LDAP for Contact Syncing**: By default this option is set to No. You can modify it to Yes. If this is set to Yes, only then the below fields will be active.
- **Account Description**: Enter the description of the LDAP Account.
- **Account Host Name**: Enter LDAP account Host name you wish to connect with
- **Account Use SSL**: By default this option is set to No. You can modify it to Yes.
- **Account User Name**: Enter the user name of the LDAP Account.
- **Account Password**: Enter the password of the LDAP Account.
- **Search Settings**: Click the **ADD** button to add search settings shown below:
    - **Description**: Enter description for search settings.
    - **Scope**: Select the scope from the list.
    - **Search Base**: Enter search base for search settings.

  You can remove multiple search settings by clicking the **Remove** button.

10.4.4.2 Set Email and Calendar Policy for Android

To set Email and Calendar policy for Android, follow these steps:

1. Under **Email Setup**, select one of the check boxes:



Email Setup

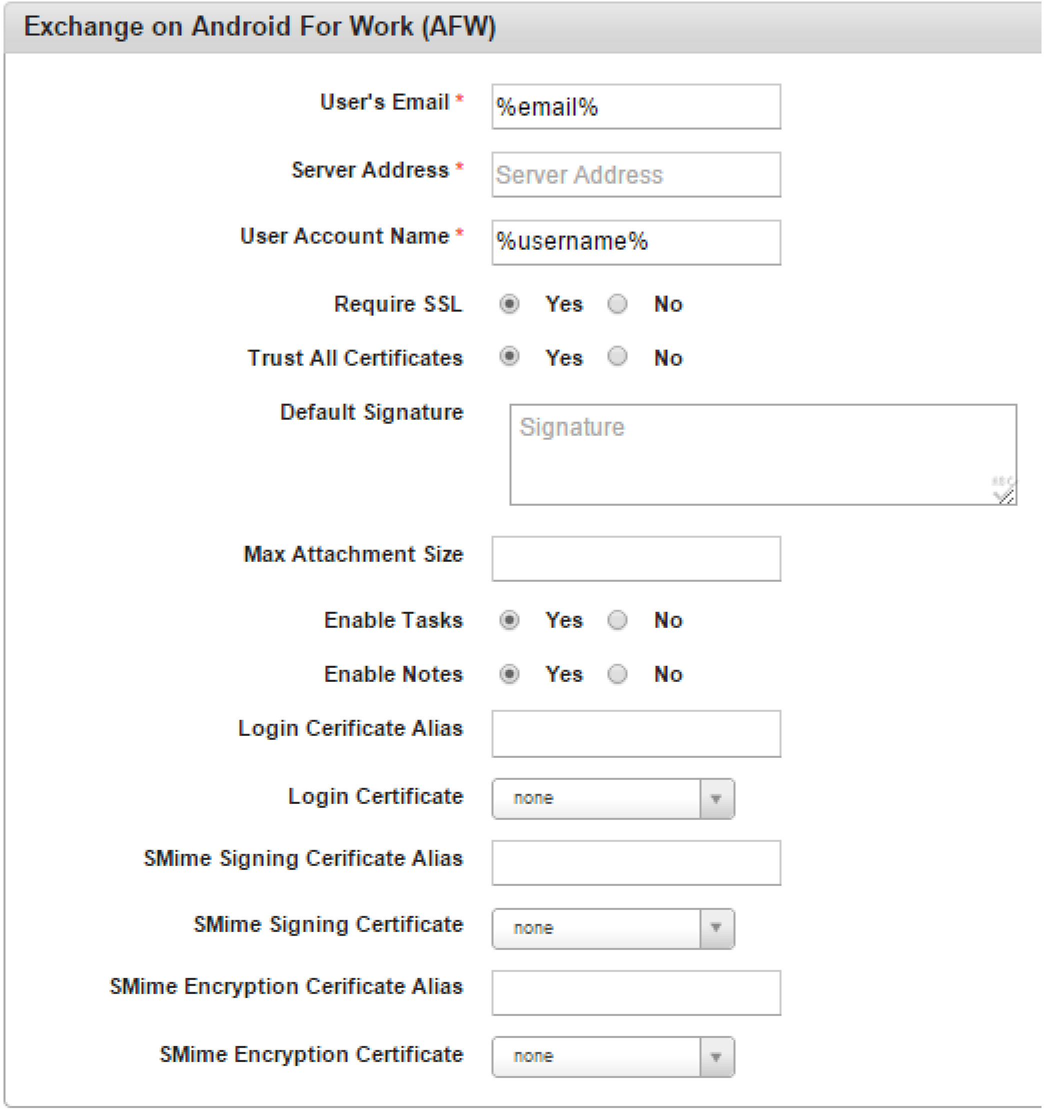
Email for Native Client (Samsung Only) ○ Exchange ○ POP / IMAP

Email for Android for Work (Supported Devices Only) ☑ Exchange

NOTE: Email Policy defined here will not replace any existing User defined configuration on device. It is recommended that you request users to remove all configurations prior to enrollment with EMM.

- Exchange
- POP / IMAP
- Email for Android For Work (supported Devices only) Exchange

Email for Android For Work (supported Devices only) Exchange



Exchange on Android For Work (AFW)

User's Email * %email%

Server Address * Server Address

User Account Name * %username%

Require SSL ● Yes ○ No

Trust All Certificates ● Yes ○ No

Default Signature Signature

Max Attachment Size

Enable Tasks ● Yes ○ No

Enable Notes ● Yes ○ No

Login Cerificate Alias

Login Certificate none

SMime Signing Cerificate Alias

SMime Signing Certificate none

SMime Encryption Cerificate Alias

SMime Encryption Certificate none

- **User's Email**: Enter the email of the exchange account.
- **Server Address:** Enter the email server address.
- **User Account Name**: Enter the user account name.
- **Require SSL:** By default, Require SSL is configured to **Yes.** If the email server does not require Secure Sockets Layer (SSL), configure to **No.**
- **Trust ALL Certificates:** By default, Trust All Certificates is configured to **Yes.** If you do not want to trust all certificates, configure this to **No.**
- **Default Signature:** Enter your email signature details that can be used as the default signature for the email being configured.
- **Max Attachment Size:** Enter the maximum size of the attachments that are allowed for the email.
- **Enable Tasks:** By default, Enable Tasks is configured to **Yes.** If you do not want to enable tasks associated with the email account to sync with the device tasks feature, configure to **No.**
- **Enable Notes:** By default, Enable Notes is configured to **Yes.** If you do not want to enable notes associated with the email account to sync with the device notes feature, configure to **No.**
- **Login Certificate Alias:** Enter an alias for the log-in certificate.
- **Login Certificate:** Select a certificate from the list.
- **SMIME Signing Certificate Alias:** Enter an alias for the SMIME signing certificate.
- **SMIE Signing Certificate:** Select a certificate from the list.
- **SMIME Encryption Certificate Alias:** Enter an alias for the SMIME encryption certificate.
- **SMIME Encryption Certificate:** Select a certificate from the list.

Exchange on Native Client (Samsung only)

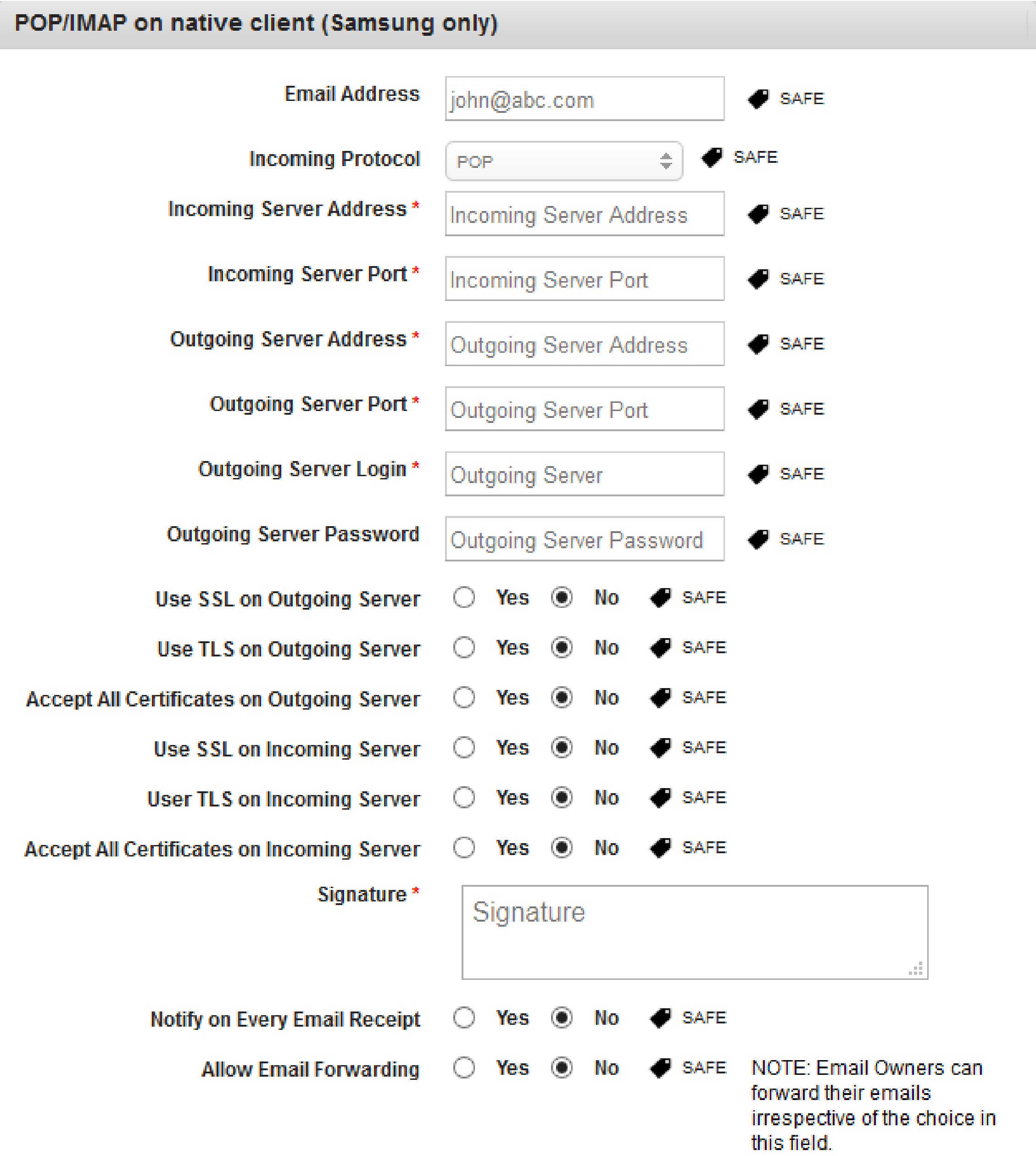
> *Important:* When the enterprise store is uninstalled on a SAFE device, all SAFE emails are removed from the device.

- **Display Name ***: Enter the name to be displayed for exchange account.
- **User's Email**: Enter the email of the exchange account.
- **Exchange User Account Name ***: Enter user name of the exchange account.
- **Exchange Domain Name ***: Domain name of the exchange account
- **Sync Email for**: Select one of the numbers of previous days of Email to sync.
- **Peak Email Synchronization Frequency**: Select one of the options of frequency to sync email during peak time.
- **Make this the Default Account**: By default this option is set to No. You can modify it to Yes.
- **Protocol Version ***: Enter EAS server protocol version. For example, V 12.0
- **Signature ***: Enter your signature details.
- **Always Vibrate on Email Notification**: By default this option is set to No. You can modify it to Yes.
- **Vibrate on Email Notification When Silent**: By default this option is set to No. You can modify it to Yes.
- **Server Address ***: Enter the address of the exchange server. For example, "mail.xyz.com"
- **Use SSL**: By default, this option is set to No. You can modify it to Yes.
- **Use TLS**: By default, this option is set to No. You can modify it to Yes.
- **Accept All Certificates**: By default, this option is set to No. You can modify it to Yes.
- **Server Password ***: Enter the password of the exchange account.

- **Server Path Prefix**: Enter the prefix to be added to server path (optional can be null)
- **Peak Start Time ***:
    1. Click in Peak Start Time field.
    2. Choose Time dialog appears.
    3. Drag the cursor to select Hour and Minute. Click Done to continue.
    4. The selected time appears in Peak Start Time field.
- **Peak End Time:** Follow the similar process to select peak end time.
- **Peak Days ***: Select checkboxes for peak days for sync schedule.
- **Off Peak Schedule**: Select one of the options for frequency to sync email during off peak time.
- **Roaming Sync Schedule**: By default, this option is set to Use Sync settings. You can modify it to Manual.
    - **Manual**
    - **Use Sync settings**
- **Max Size to be Retrieved**: Select the option from the drop-down list.
- **Notify on Every Email Receipt**: By default, this option is set to No. You can modify it to Yes.
- **Synchronize Contacts**: By default, this option is set to No. You can modify it to Yes.
- **Synchronize Calendar**: By default, this option is set to No. You can modify it to Yes.
- **Calendar Synchronization Period**: Select the option from the drop-down list.
- **Certificate**: Select the certificate from the drop-down list.
- **Synchronize Tasks**: By default, this option is set to No. You can modify it to Yes to synchronize tasks.

- **Synchronize Notes**: By default, this option is set to No. You can modify it to Yes to synchronize notes.

POP / IMAP on Native Client (Samsung Only)



POP/IMAP on native client (Samsung only)

Email Address	john@abc.com	SAFE
Incoming Protocol	POP	SAFE
Incoming Server Address *	Incoming Server Address	SAFE
Incoming Server Port *	Incoming Server Port	SAFE
Outgoing Server Address *	Outgoing Server Address	SAFE
Outgoing Server Port *	Outgoing Server Port	SAFE
Outgoing Server Login *	Outgoing Server	SAFE
Outgoing Server Password	Outgoing Server Password	SAFE
Use SSL on Outgoing Server	○ Yes ● No	SAFE
Use TLS on Outgoing Server	○ Yes ● No	SAFE
Accept All Certificates on Outgoing Server	○ Yes ● No	SAFE
Use SSL on Incoming Server	○ Yes ● No	SAFE
User TLS on Incoming Server	○ Yes ● No	SAFE
Accept All Certificates on Incoming Server	○ Yes ● No	SAFE
Signature *	Signature	
Notify on Every Email Receipt	○ Yes ● No	SAFE
Allow Email Forwarding	○ Yes ● No	SAFE NOTE: Email Owners can forward their emails irrespective of the choice in this field.

> *Important:* Currently, outgoing server details are not honored by SAFE (a defect in SAFE). SAFE presumes that outgoing server details are the same as incoming server details. This issue might get fixed in updated versions of the SAFE API.

> *Important:* When the enterprise store is uninstalled on a SAFE device, all SAFE emails are removed from the device.

- **Email Address**: This field populates the email address of the enrolled user when a policy a is applied.
- **Incoming Protocol**: Select the Incoming server protocol from the list.
- **Incoming Server Address ***: Enter the incoming server address.
- **Incoming Server Port ***: Enter the incoming server port number.
- **Outgoing Server Address ***: Enter the OutGoing server address.
- **Outgoing Server Port ***: Enter the OutGoing server port number.
- **Outgoing Server Login ***: Enter Outgoing Server Login address.
- **Outgoing Server Password**: Enter Outgoing Server Login password.
- **Use SSL on Outgoing Server**: By default this option is set to No. You can modify it to Yes.
- **Use TLS on Outgoing Server**: By default this option is set to No. You can modify it to Yes.
- **Accept All Certificates on Outgoing Server**: By default this option is set to No. You can modify it to Yes.
- **Use SSL on Incoming Server**: By default this option is set to No. You can modify it to Yes.
- **User TLS on Incoming Server**: By default this option is set to No. You can modify it to Yes.

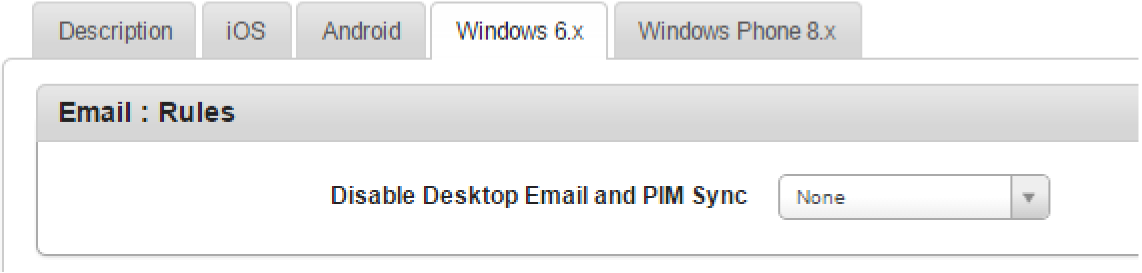
- **Accept All Certificates on Incoming Server**: By default this option is set to No. You can modify it to Yes.
- **Signature *:** Enter the signature text.
- **Notify on Every Email Receipt**: By default this option is set to No. You can modify it to Yes.
- **Allow Email Forwarding**: By default this option is set to No. You can modify it to Yes.

10.4.4.3 Set Email and Calendar for Windows 6.x

Windows 6.x support following subset of Email and Calendar policy settings.

To set Email and Calendar policy for Windows 6.x, follow these steps:

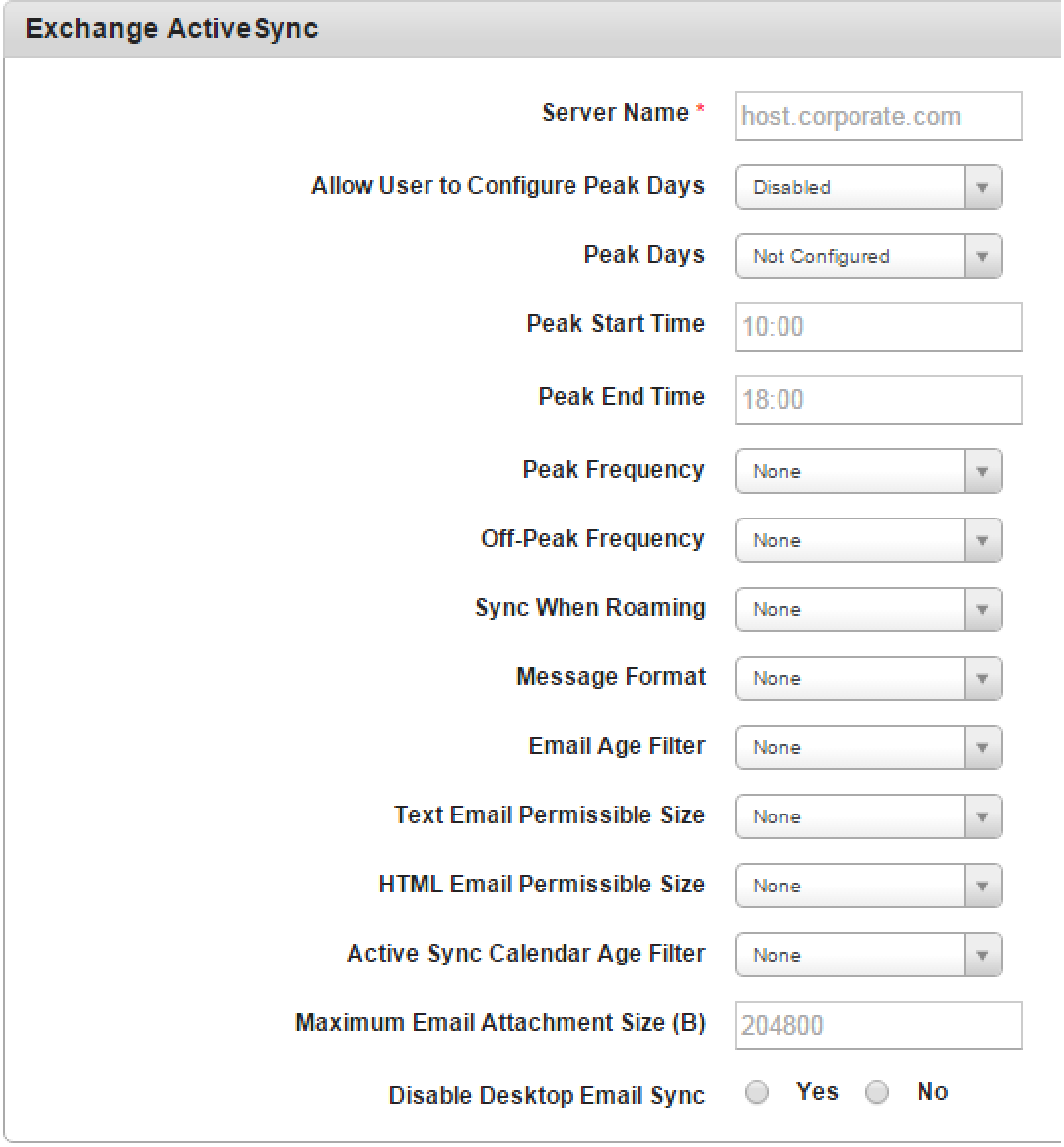
<u>Email: Rules</u>



Disable Desktop Email and PIM Sync: None

1. **Disable Desktop Email and PM Sync**: Select the required option from the drop-down list. By default, it is set to None.

This setting specifies whether the mobile phone can synchronize with a computer through a cable or Bluetooth connection. You can set the value as True or False.



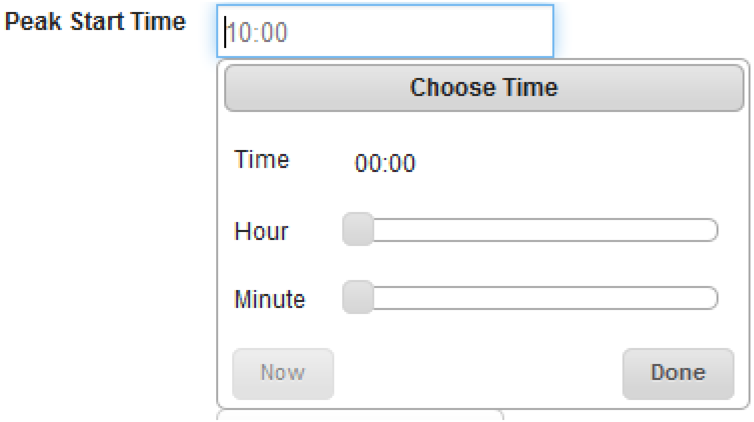
Exchange ActiveSync

Server Name *	host.corporate.com
Allow User to Configure Peak Days	Disabled
Peak Days	Not Configured
Peak Start Time	10:00
Peak End Time	18:00
Peak Frequency	None
Off-Peak Frequency	None
Sync When Roaming	None
Message Format	None
Email Age Filter	None
Text Email Permissible Size	None
HTML Email Permissible Size	None
Active Sync Calendar Age Filter	None
Maximum Email Attachment Size (B)	204800
Disable Desktop Email Sync	○ Yes ○ No

Exchange ActiveSync

1. **Server Name**: Enter the Server Name.

2. **Allow User to Select Peak Days**: Select the required option from the drop-down menu.



3. **Peak Start Time**: Click in Peak Start Time field.

   Choose Time dialog box appears.

4. Drag the cursor to select Hour and Minute. Click Done to continue.

   The selected time appears in Peak Start Time field.

5. **Peak End Time**: Follow the similar process to select peak end time.

6. **Peak Frequency**: Select the required option from the drop-down list. By default, it is set to None.

7. **Off-Peak Frequency**: Select the required option from the drop-down list. By default, it is set to None.

8. **Sync when roaming**: Select the required option from the drop-down list. By default, it is set to None.

   This setting specifies whether the mobile phone must synchronize manually while roaming.

9. **Message Format**: Select the required option from the drop-down list. By default, it is set to None.

This setting allows you to define rules to receive email as Plain Text or HTML format.

10. **Email Age Filter**: Select the required option from the drop-down list. By default, it is set to None.

11. **Text Email Permission Size**: Select the required option from the drop-down list. By default, it is set to None.

    This setting specifies the permissible size for Text-formatted e-mail messages when they are synchronized to the mobile phone.

12. **HTML Email Permission Size**: Select the required option from the drop-down list. By default, it is set to None.

    This setting specifies the permissible size for HTML-formatted e-mail messages when they are synchronized to the mobile phone. The value is specified in kilobytes (KB).

13. **Active Sync Calendar Age Filter**: Select the required option from the drop-down list. By default, it is set to None.

    This setting specifies the maximum range of calendar days that can be synchronized to the mobile phone. The value is specified in days.

14. **Maximum Email Attachment Size**: Enter the email attachment size.

    This setting specifies the size beyond which HTML-formatted e-mail messages are truncated when they are synchronized to the mobile phone.

15. **Disable Desktop Email Sync**. By default, this option is set to Yes, which you can modify to No.

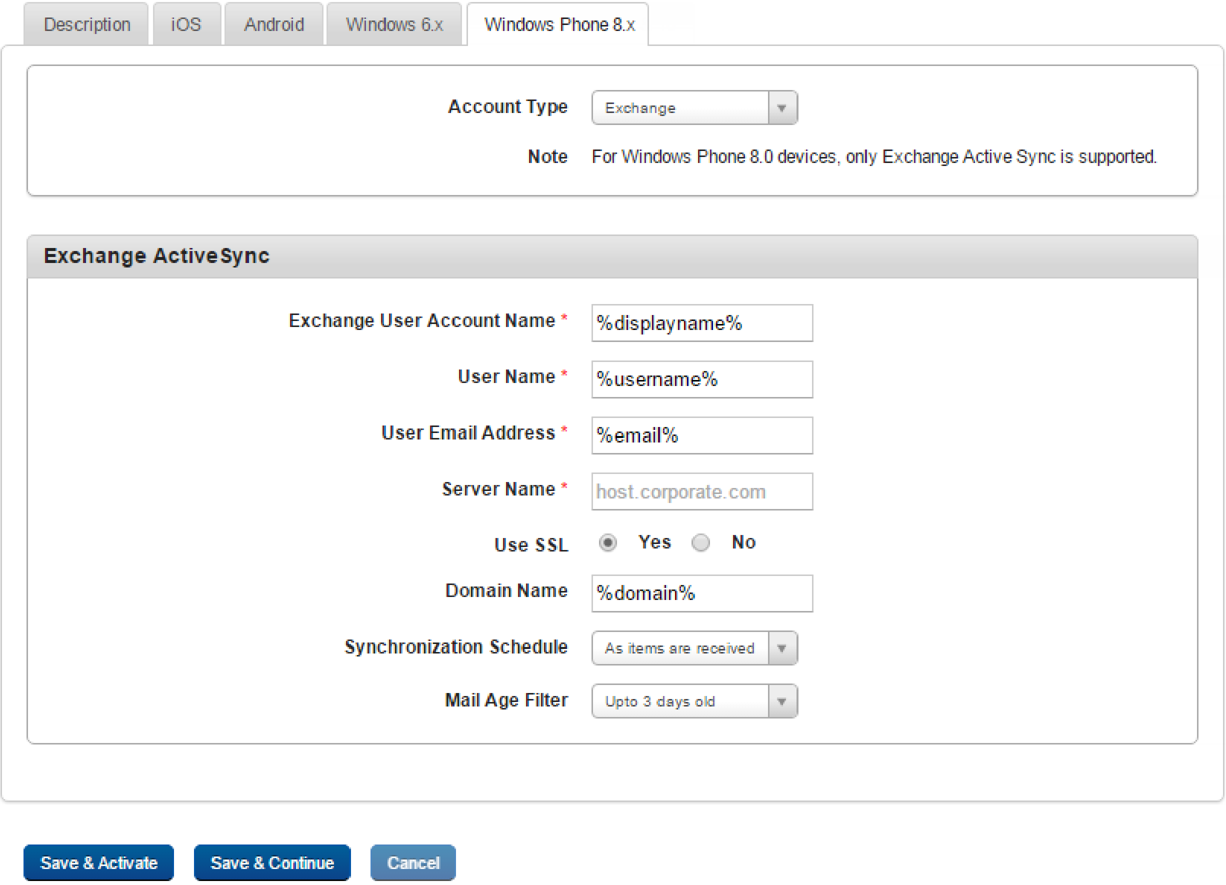
16. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

17. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.4.4 Set Email and Calendar Policy for Windows Phone 8.x

To set Email and Calendar policy for Windows Phone 8.x, follow these steps:



Account Type: Exchange ▾

Note: For Windows Phone 8.0 devices, only Exchange Active Sync is supported.

Exchange ActiveSync

Exchange User Account Name *: %displayname%

User Name *: %username%

User Email Address *: %email%

Server Name *: host.corporate.com

Use SSL: ● Yes ○ No

Domain Name: %domain%

Synchronization Schedule: As items are received ▾

Mail Age Filter: Upto 3 days old ▾

1. Account Type: Select the account type. Exchange or Pop/IMAP.

2. If you select **Exchange**, the following appear,

   i. **Exchange User Account Name**: Enter exchange user account name.

   ii. **User Name**: Enter user name.

   iii. **User Email Address**: Enter user email address.

   iv. **Server Name**: Enter the host URL in the text field.

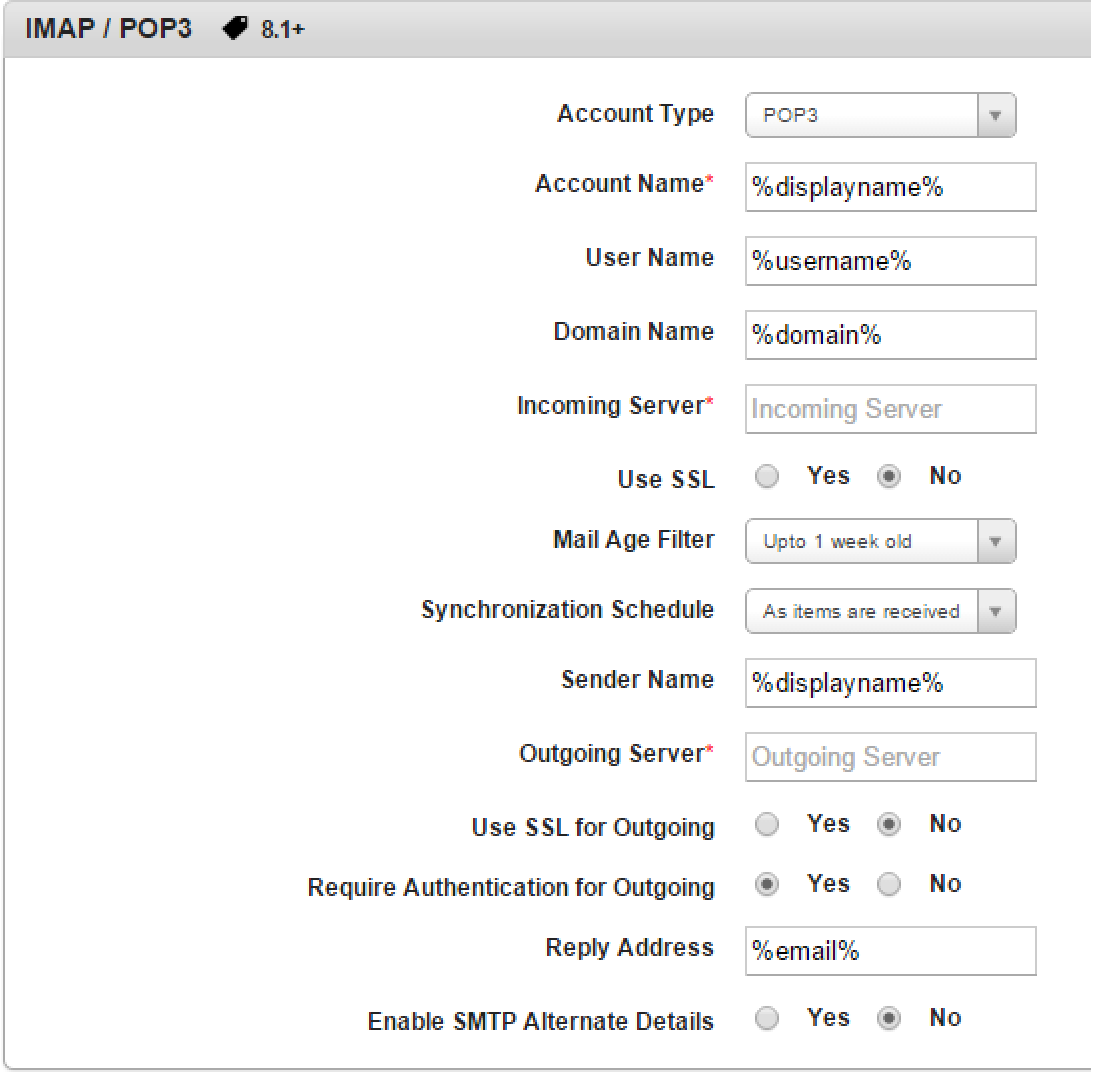
v. **Use SSL**: By default, this option is set to Yes. You can modify it to No.

vi. **Domain Name**: Enter the corporate domain URL in the text field.

vii. **Synchronized Schedule**: Select the required synchronized schedule from the drop-down list. By default, it is set to **As items are received**.

viii. **Mail Age Filter**: Select the required mail age filter from the drop-down list. By default, it is set to 3 days old.

3. If you select **POP/IMAP**, the following appear,



IMAP / POP3 8.1+

Account Type	POP3
Account Name*	%displayname%
User Name	%username%
Domain Name	%domain%
Incoming Server*	Incoming Server
Use SSL	○ Yes ● No
Mail Age Filter	Upto 1 week old
Synchronization Schedule	As items are received
Sender Name	%displayname%
Outgoing Server*	Outgoing Server
Use SSL for Outgoing	○ Yes ● No
Require Authentication for Outgoing	● Yes ○ No
Reply Address	%email%
Enable SMTP Alternate Details	○ Yes ● No

4. Enter details for the following,

    i. **Account Type**: Select POP3 or IMAP4 from the list.

    ii. **Account Name**: Enter account name.

    iii. **User Name**: Enter user name.

    iv. **Domain Name**: Enter domain name.

    v. **Incoming Server**: Enter incoming server details.

    vi. **Use SSL**: By default this is set to No. You can chose Yes.

    vii. **Mail Age Filter**: Select mail age filter time period from the list.

    viii. **Synchronization Schedule**: Select synchronization schedule interval from the list.

    ix. **Sender Name**: Enter sender name.

    x. **Outgoing Server**: Enter outgoing server details.

    xi. **Use SSL for Outgoing**: By default this is set to No. You can chose Yes.

    xii. **Require Authentication for Outgoing**: By default this is set to Yes. You can chose No.

    xiii. **Reply Address**: Enter reply email address.

    xiv. **Enable SMTP Alternate Details**: By default this is set to No. You can chose Yes.

    Choosing Yes will enable the following fields.

    - **Alternate Username**: Enter alternate username.
    - **Alternate User's Password**: Enter alternate user's password.
    - **Alternate Domain**: Enter alternate user's domain name.

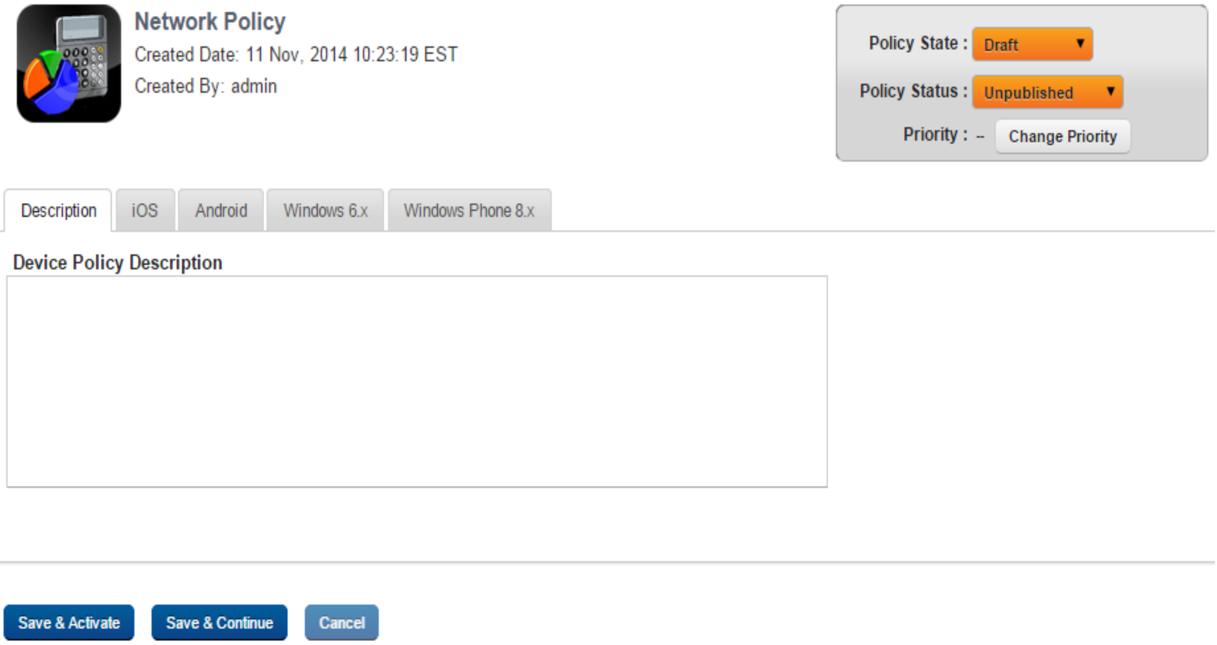
5. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

6. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.5 Network Policy

The primary purpose of the network policy is to ensure settings of the different network connections such as Wi-Fi and VPN, to authorize network connectivity on devices.


Network Policy
Created Date: 11 Nov, 2014 10:23:19 EST
Created By: admin

Policy State : Draft
Policy Status : Unpublished
Priority : --

Device Policy Description

Important: Network Policy on server side browsers like Opera Mini cannot be enforced. It is recommended to use other browsers. If you need high security, you may need to blacklist the Opera Mini browser.

You can set Network Policy for the following operating systems.

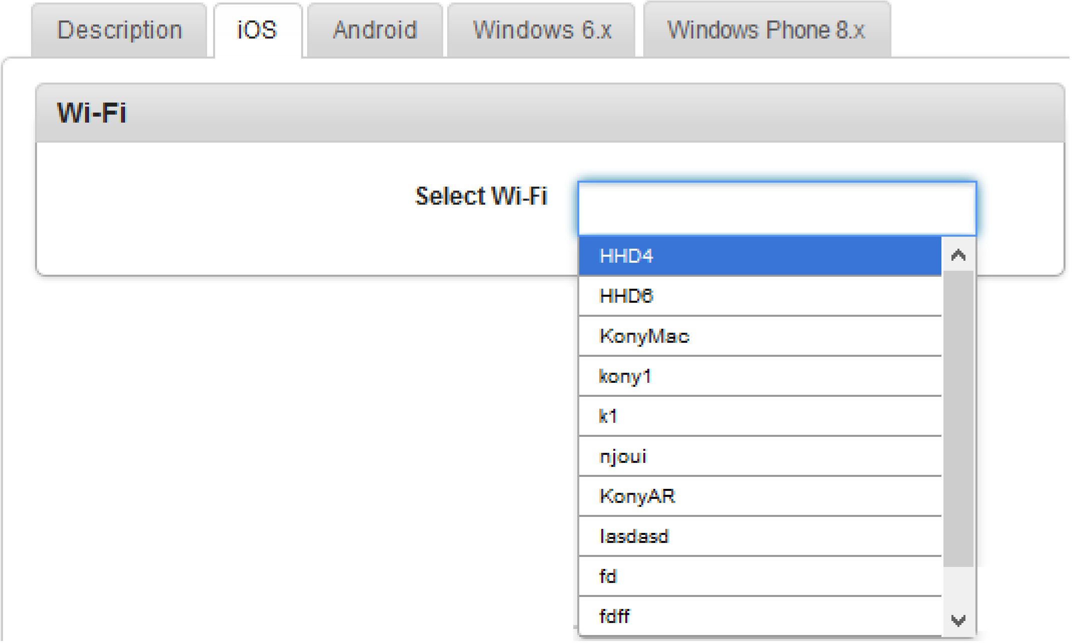
- Set Network Policy for iOS
- Set Network Policy for Android

- Set Network Policy for Windows 6.x
- Set Network Policy for Windows Phone 8.x

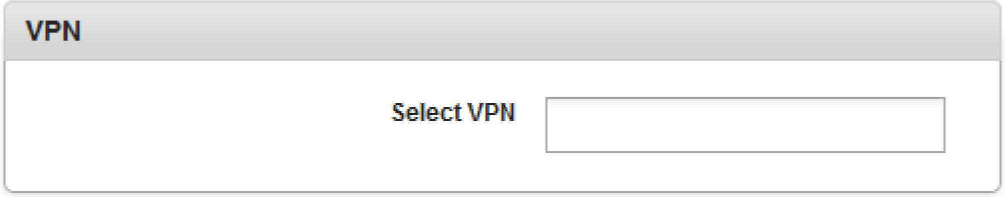
Set Network Policy for iOS

To specify Network policy for the iOS platform, follow these steps:

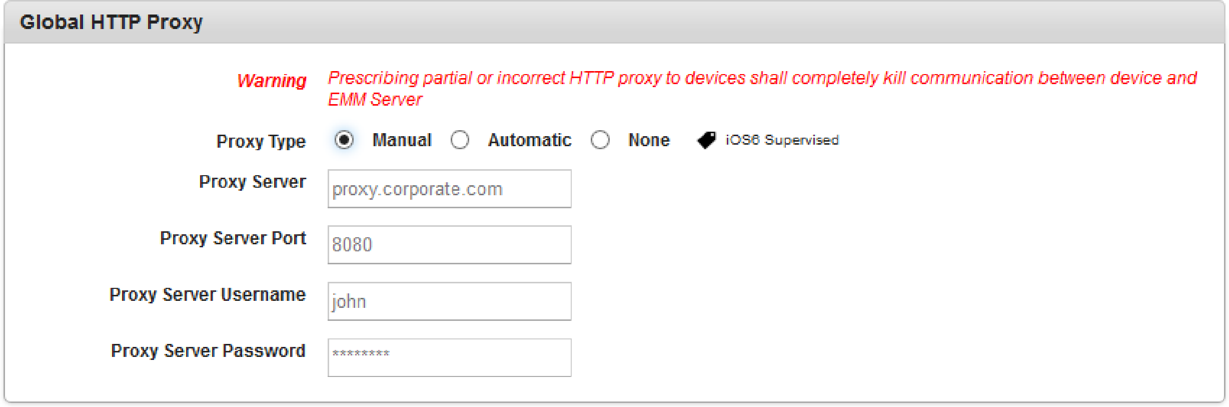
1. **Wi- Fi:** Select one of the Wi-Fis from the list.



2. In the **VPN**, select one of the VPNs from the list.



3. Enter details for the following fields to set **Global HTTP Proxy.**



Global HTTP Proxy

Warning: Prescribing partial or incorrect HTTP proxy to devices shall completely kill communication between device and EMM Server

Proxy Type: ● Manual ○ Automatic ○ None iOS6 Supervised

Proxy Server: proxy.corporate.com

Proxy Server Port: 8080

Proxy Server Username: john

Proxy Server Password: ********

a. **Proxy Type**:Select the required Proxy Type from the drop-down menu. By default, proxy type is set to **None**. You can modify your selection to **Manual** or **Automatic**.

b. If you select the Proxy Type as **Manual**, then you need to enter details for the following fields:

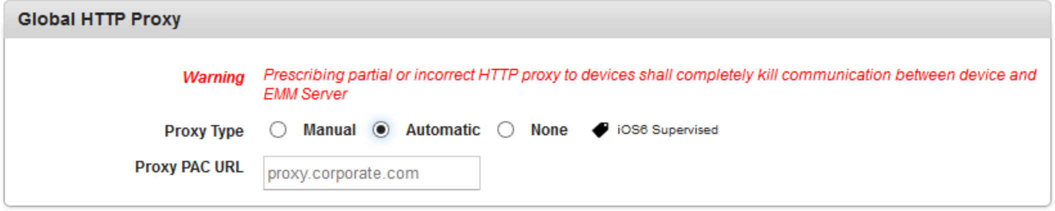
   i. **Proxy Server**: Enter details of the Proxy Server in the text field.

   ii. **Proxy Server Port**: Enter Proxy Server Port number in the text field.

   iii. **Proxy Server Username**: Enter Server Username in the text field.

   iv. **Proxy Server Password**: Enter Proxy Server Password. in the text field.

c. If you select Proxy Type as **Automatic**, then you need to enter details for the following fields:



Global HTTP Proxy

Warning: Prescribing partial or incorrect HTTP proxy to devices shall completely kill communication between device and EMM Server

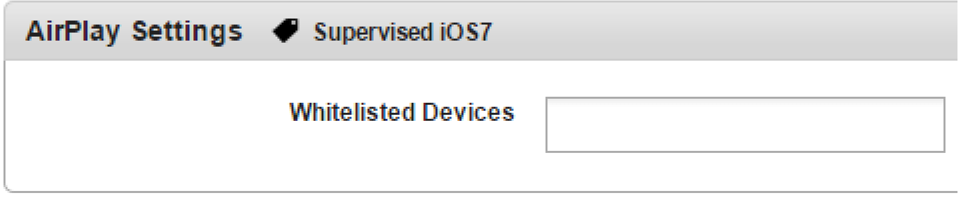
Proxy Type: ○ Manual ● Automatic ○ None iOS6 Supervised

Proxy PAC URL: proxy.corporate.com

i. **Proxy PAC URL**: Enter address of the proxy server.

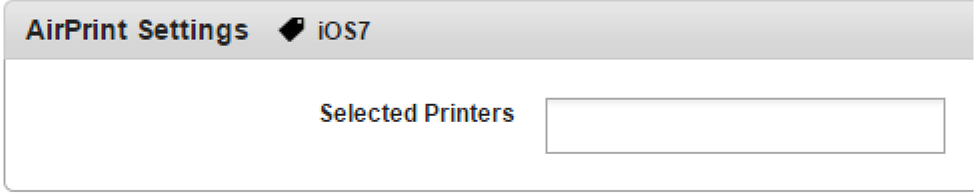
4. Enter whitelisted airplay devices details in the **Whitelisted Devices** field. (Supervised iOS7+)

   Based on the configuration done in **Enterprise Resources > AirPlay Settings**, you can search and select the device IDs for AirPlay.

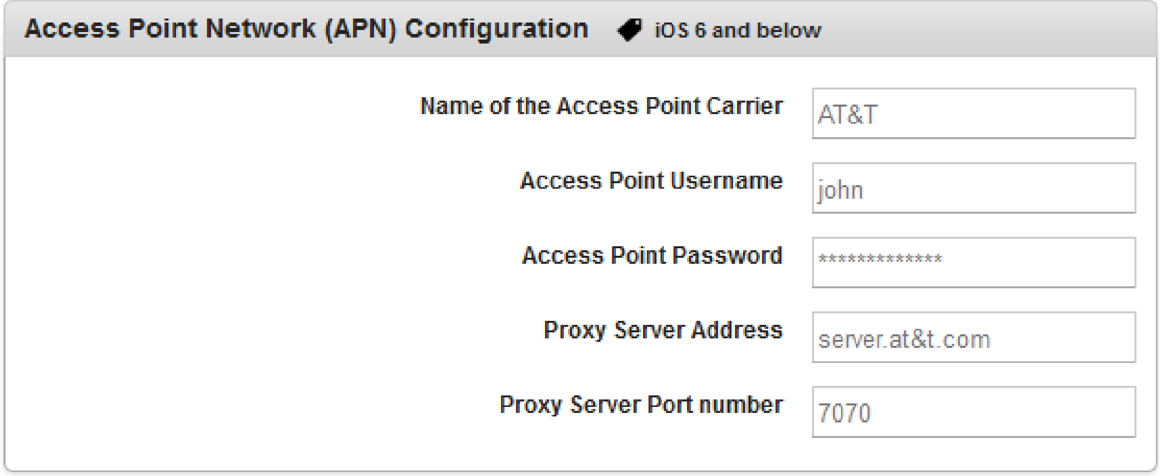


5. Enter selected AirPrint devices details in the **AirPrint Settings** field (Supervised iOS7+)

   Select the printers to support AirPrint functionality (iOS7+)
   Based on the configuration done in **Enterprise Resources > AirPrint Settings**, you can search and select the IP for AirPrint.



6. Enter details for the following fields to set **Access Point Network (APN) Configuration**:



Access Point Network (APN) Configuration iOS 6 and below

Name of the Access Point Carrier	AT&T
Access Point Username	john
Access Point Password	*************
Proxy Server Address	server.at&t.com
Proxy Server Port number	7070

a. **Name of the Access Point Carrier** Enter the name of the access point carrier in the text field. Access Point Carriers ensures network connectivity.

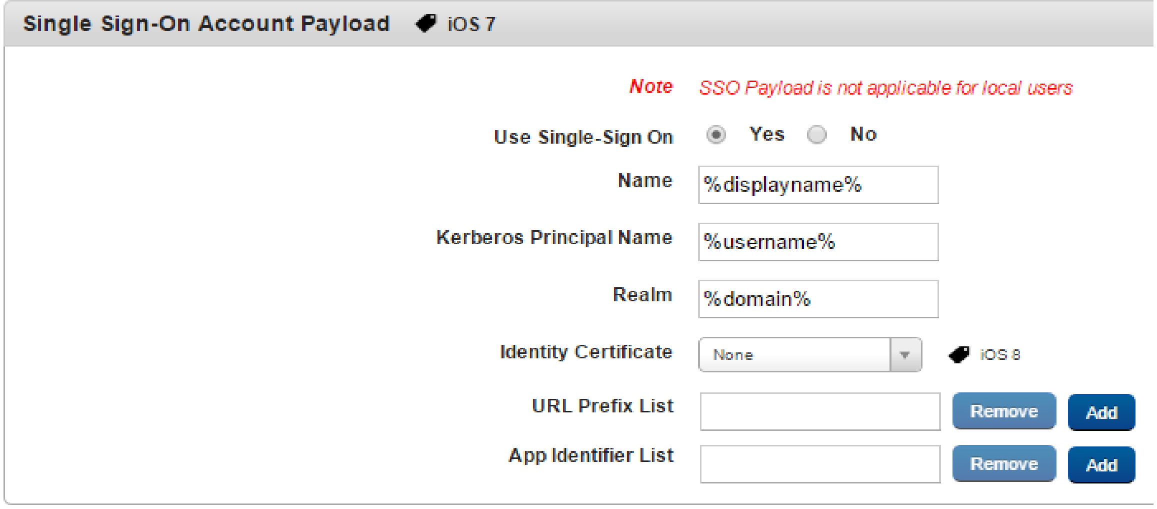
b. **Access Point Username**: Enter the name of the access point username in the text field.

c. **Access Point Password**: Enter the access point password in the text field.

d. **Proxy Server Address**: Enter the proxy server address in the text field.

e. **Proxy Server Port Number**: Enter the proxy server port number in the text field.

7. For iO7+, admin can create a single sign-on account for different web portals and apps as well. Enter details for the following fields to set **Single Sign-On Account Payload**.



Single Sign-On Account Payload iOS 7

Note SSO Payload is not applicable for local users

Use Single-Sign On ● Yes ○ No

Name %displayname%

Kerberos Principal Name %username%

Realm %domain%

Identity Certificate None iOS 8

URL Prefix List

App Identifier List

a. **Use Single-Sign On**: By default this option is set to No. You can modify it to Yes. If this is set to **Yes**, only then the below fields will be active.

b. **Name**: Enter the name for the account

c. **Kerberos Principal Name**: Enter the Kerberos Principal Name.

d. **Realm**: Enter the Kerberos Realm name.

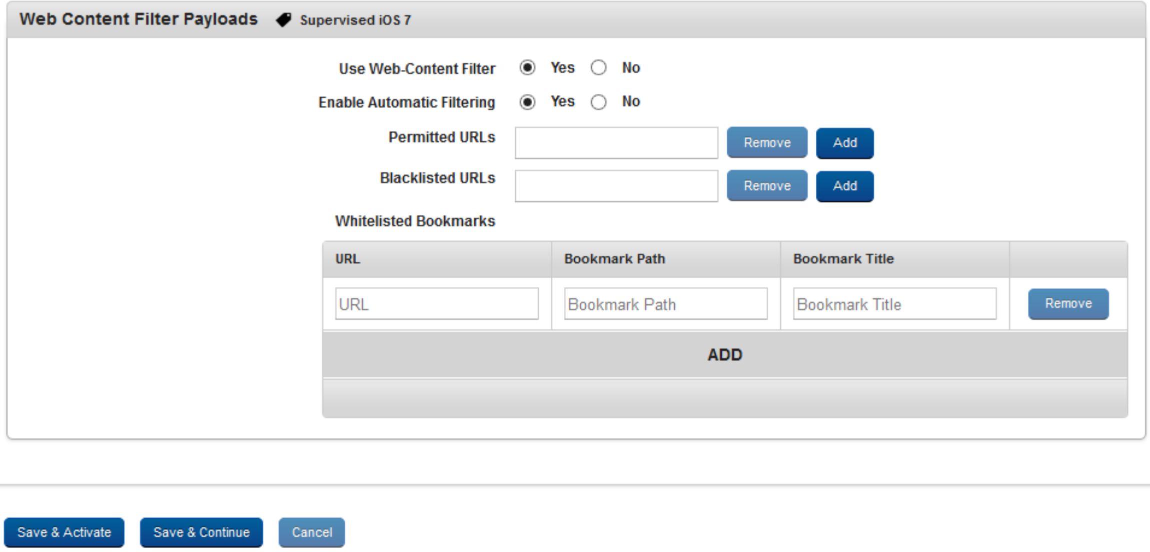
e. **Identity Certificate:** Select the identity certificate.

f. **URL Prefix List:**

Click **Add** to add additional fields. You can remove fields by clicking on the **Remove** button.

g. **App Identifier List**:
Click **Add** to add additional fields. You can remove fields by clicking on the **Remove** button.

8. Enter details for the following fields to set Web Content Filter Payloads.



Web Content Filter Payloads Supervised iOS 7

Use Web-Content Filter ● Yes ○ No

Enable Automatic Filtering ● Yes ○ No

a. **Use Web-Content Filter**: By default this option is set to No. You can modify it to Yes. When the Use Web-Content Filter is set to Yes, the following fields will be active.

b. **Enable Automatic Filtering:** By default, this option is set to No. You can modify it to Yes.

c. **Permitted URLs**: Enter the permitted URLs. The permitted URLs can only be accessed on the device. You can add more URLs by clicking the **Add** button. You can remove URLs by clicking the **Remove** button.

d. **Blacklisted URLs**: Enter the Blacklisted URLs. The blacklisted URLs can not be accessed on the device. You can add more URLs by clicking the **Add** button. You can remove URLs by clicking the **Remove** button.

e. **Whitelisted Bookmark**: You can configure only whitelisted URLs as bookmarks on the device. To add whitelisted URLs, click the **ADD** button and follow these steps:

   1. **URL**: Enter the URL of a website.

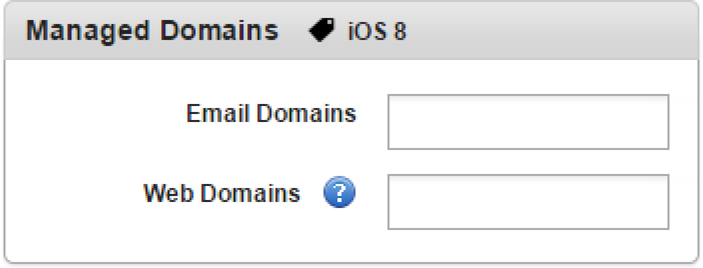
   2. **Bookmark Path**: Enter name for the bookmark folder. All your bookmarks will be

stored under this folder.

3. **Bookmark Title**: Enter the title for the bookmark URL.

You can add more URLs by clicking the **Add** button. You can remove URLs by clicking the **Remove** button.

9. Enter details for Managed Domains. This feature is available only for devices with iOS8.



a. **Email Domains**: Enter allowed email domain names.

b. **Web Domains**: Enter allowed web domain names.

10. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

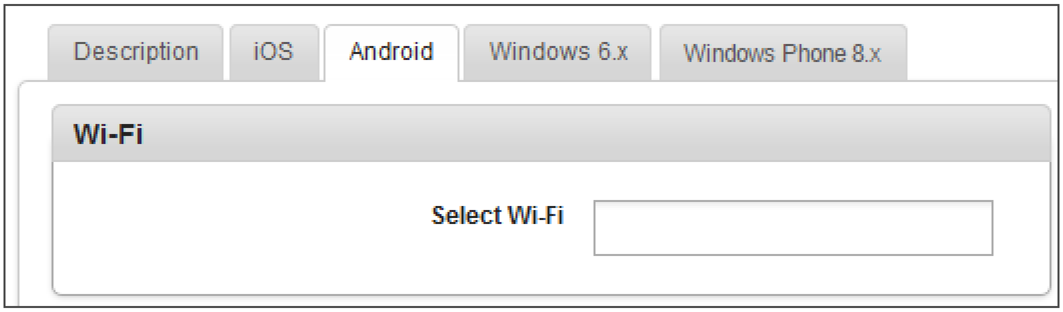
11. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

Set Network Policy for Android

To specify network policy for the Android platform, follow these steps:

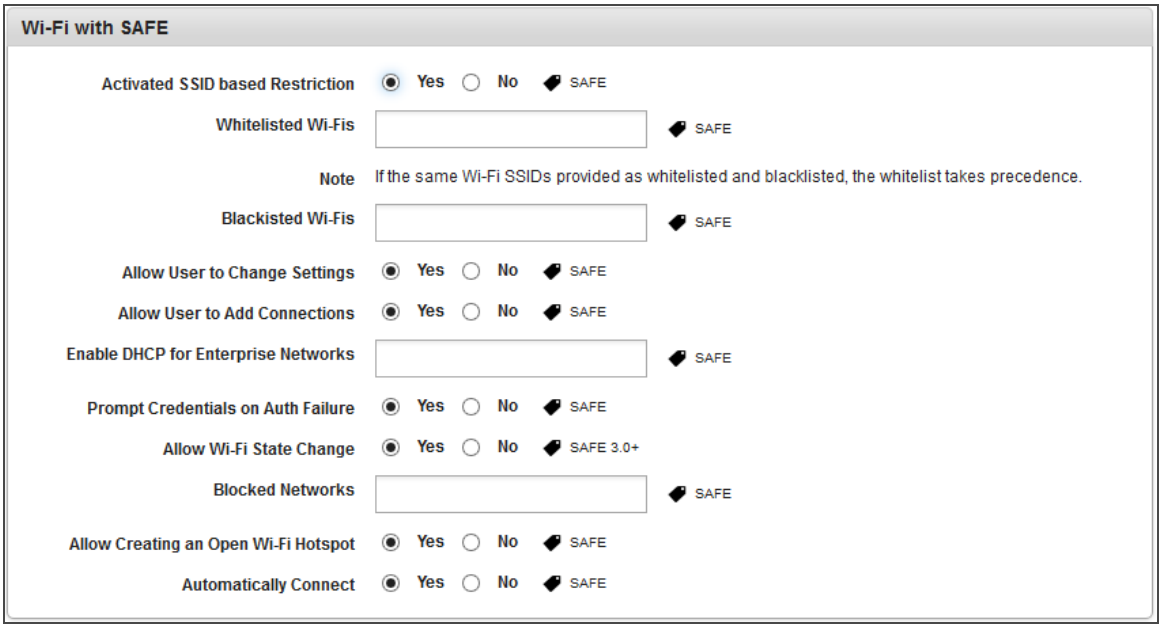
1. In **Wi-Fi**, enter the name of the Wi-Fi you want to use. Ensure that this is one of the Wi-Fis configured in **Enterprise Resources** > **Wi-Fi**.



Wi-Fi

Select Wi-Fi

2. In **Wi-Fi with SAFE**, complete the following fields:



Wi-Fi with SAFE

Activated SSID based Restriction	● Yes ○ No	SAFE
Whitelisted Wi-Fis		SAFE
Note	If the same Wi-Fi SSIDs provided as whitelisted and blacklisted, the whitelist takes precedence.	
Blackisted Wi-Fis		SAFE
Allow User to Change Settings	● Yes ○ No	SAFE
Allow User to Add Connections	● Yes ○ No	SAFE
Enable DHCP for Enterprise Networks		SAFE
Prompt Credentials on Auth Failure	● Yes ○ No	SAFE
Allow Wi-Fi State Change	● Yes ○ No	SAFE 3.0+
Blocked Networks		SAFE
Allow Creating an Open Wi-Fi Hotspot	● Yes ○ No	SAFE
Automatically Connect	● Yes ○ No	SAFE

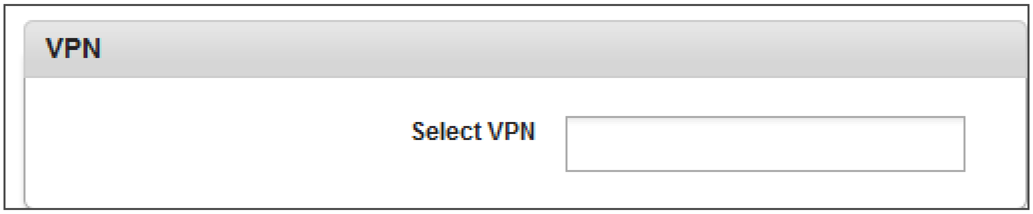
- **Activated SSID based Restriction**: By default this option is set to Yes. You can modify it to No.

  Only when the Activated SSID based Restriction is set to Yes are the following options active:

  - **Whitelisted Wi-Fis**: Select one of the whitelisted Wi-Fis.
  - **Blacklisted Wi-Fis**: Select one of the blacklisted Wi-Fis.
- **Allow User to Change Settings**: By default this option is set to No. You can modify it to Yes.
- **Allow User to Add Connections**: By default this option is set to No. You can modify it to Yes.
- **Enable DHCP for Enterprise Networks**: Select the DHCP for enterprise networks.
- **Prompt Credentials on Auth Failure**: By default this option is set to Yes. You can modify it to No.
- **Allow Wi-Fi State Change**: By default this option is set to Yes. You can modify it to No.
- **Blocked Networks**: Select the desired SSIDs to be blocked, which prevents the user from connecting to the SSID. The blocked network still appears in the Access Point list but is disabled. A network is considered blocked if any administrator has it in a blacklist.
- **Allow Creating an Open Wi-Fi Hotspot**: By default this option is set to Yes. You can modify it to No.
- **Automatically Connect**: By default this option is set to Yes. You can modify it to No. If it is No, a user must manually connect to the designated Wi-Fi

> *Important:* The Hidden Network functionality is not supported for Android.

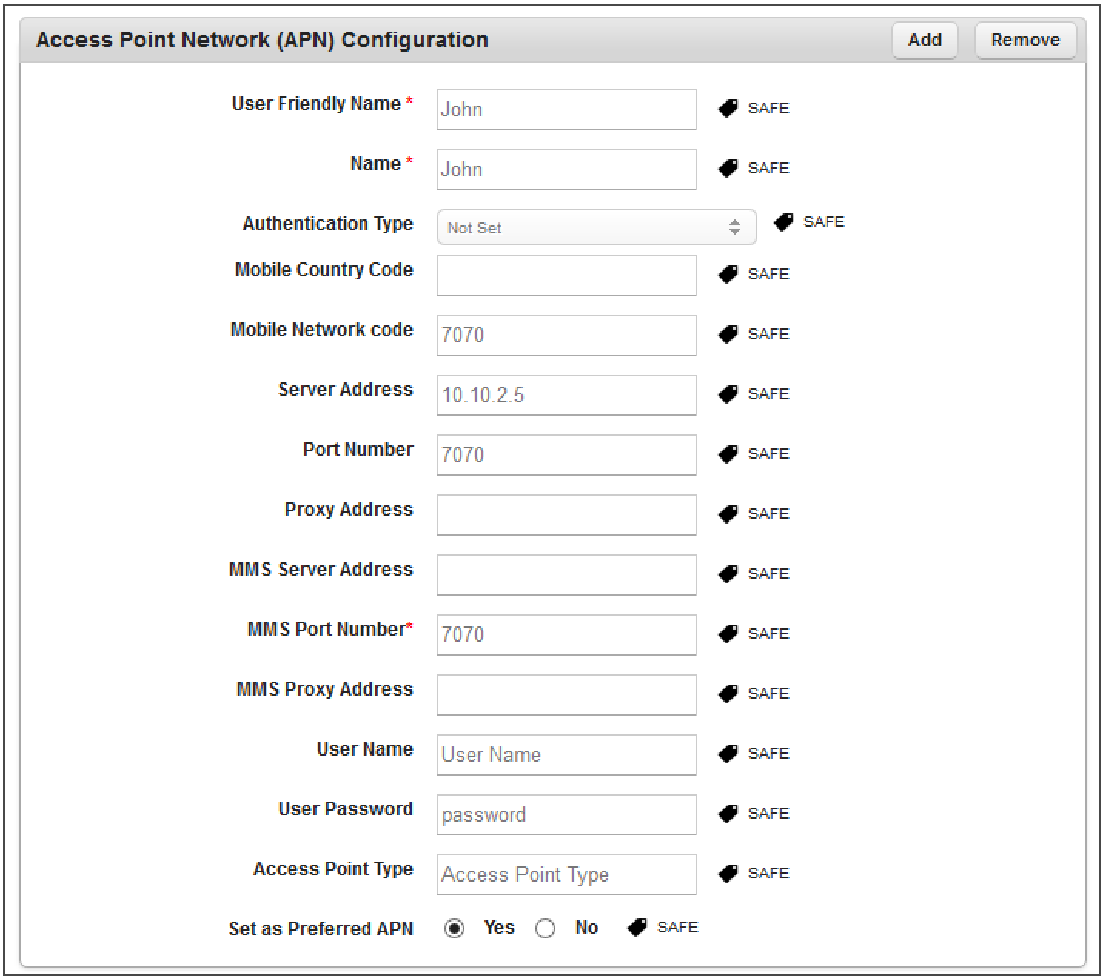
3. In the **VPN**, select one of the VPNs that are configured in the **Enterprise Resources** > **VPN** section.



VPN

Select VPN	

4. In **Access Point Network (APN) Configuration**, follow these steps:



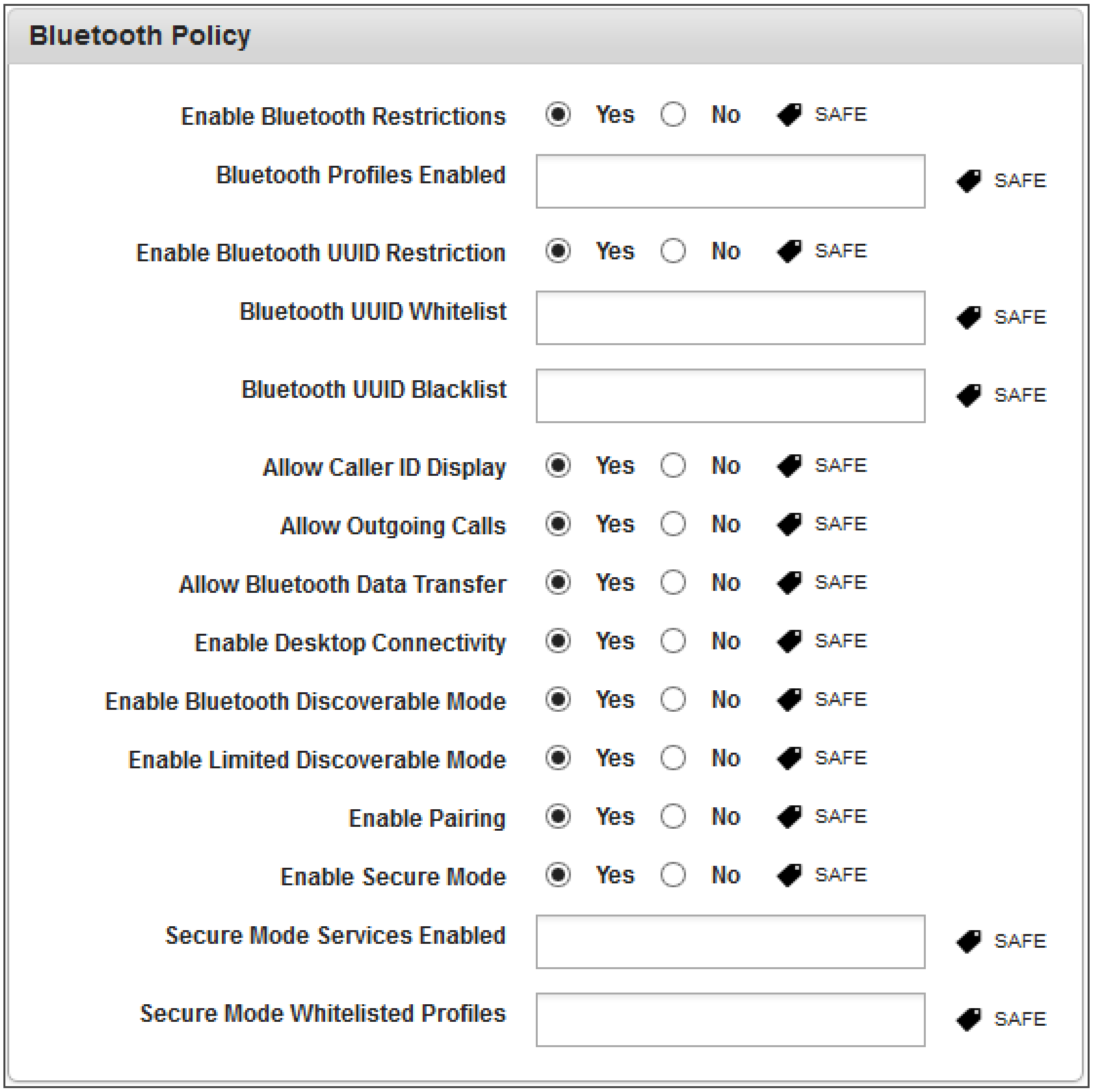
Access Point Network (APN) Configuration

User Friendly Name *	John	SAFE
Name *	John	SAFE
Authentication Type	Not Set	SAFE
Mobile Country Code		SAFE
Mobile Network code	7070	SAFE
Server Address	10.10.2.5	SAFE
Port Number	7070	SAFE
Proxy Address		SAFE
MMS Server Address		SAFE
MMS Port Number*	7070	SAFE
MMS Proxy Address		SAFE
User Name	User Name	SAFE
User Password	password	SAFE
Access Point Type	Access Point Type	SAFE
Set as Preferred APN	● Yes ○ No	SAFE

- **User Friendly Name ***: Enter a name for your APN.
- **Name ***: Enter the APN name that received from your network provider.

- **Authentication Type**: Select one of the options from the drop-down list.
- **Mobile Country Code**: Enter your mobile country code, such as 1 for the United States or 91 for India.
- **Mobile Network Code**: Enter your mobile network code. If you do not have it, please provide your network provider for the same.
- **Server Address**: Enter the server address of the APN.
- **Port Number**: Enter the port number.
- **Proxy Address**: Enter the proxy server address.
- **MMS Server Address**: Enter the MMS server address.
- **MMS Port Number ***: Enter the MMS port number.
- **MMS Proxy Address**: Enter the MMS proxy.
- **User Name**: Enter the user authentication name.
- **User Password**: Enter the password.
- **Access Point Type**: Enter the type of access point. For example, *default, mms, or supl*. If you do not enter any value, this field is populated with these values *"default,mms,supl"* on the user device.
- **Set as Preferred APN**: By default this option is set to Yes. You can modify it to No. If you set this as Yes, all your APN communications pass through this APN settings.

5. For thee **Bluetooth Policy**, complete the following fields:



Bluetooth Policy

Enable Bluetooth Restrictions	● Yes ○ No	SAFE
Bluetooth Profiles Enabled		SAFE
Enable Bluetooth UUID Restriction	● Yes ○ No	SAFE
Bluetooth UUID Whitelist		SAFE
Bluetooth UUID Blacklist		SAFE
Allow Caller ID Display	● Yes ○ No	SAFE
Allow Outgoing Calls	● Yes ○ No	SAFE
Allow Bluetooth Data Transfer	● Yes ○ No	SAFE
Enable Desktop Connectivity	● Yes ○ No	SAFE
Enable Bluetooth Discoverable Mode	● Yes ○ No	SAFE
Enable Limited Discoverable Mode	● Yes ○ No	SAFE
Enable Pairing	● Yes ○ No	SAFE
Enable Secure Mode	● Yes ○ No	SAFE
Secure Mode Services Enabled		SAFE
Secure Mode Whitelisted Profiles		SAFE

- **Enable Bluetooth Restrictions**: By default this option is set to No. You can modify it to Yes. If it is Yes, only then the below options are displayed.
  - **Bluetooth Profiles Enabled**: Select the profiles from the list.
- **Enable Bluetooth UUID Restriction**: By default this option is set to No. If you modify it to Yes, the following fields are active:

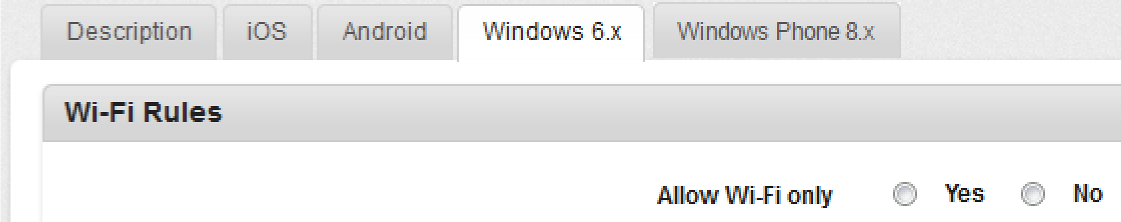
    - **Bluetooth UUID Whitelist**: Select the UUIDs from the list.
    - **Bluetooth UUID Blacklist**: Select the UUIDs from the list.
- **Allow Caller ID Display**: By default, this option is set to Yes. You can modify it to No.
- **Allow Outgoing Calls**: By default, this option is set to Yes. You can modify it to No.
- **Allow Bluetooth Data Transfer**: By default, this option is set to Yes. You can modify it to No.
- **Enable Desktop Connectivity**: By default, this option is set to Yes. You can modify it to No.
- **Enable Bluetooth Discoverable Mode**: By default, this option is set to Yes. You can modify it to No.
- **Enable Limited Discoverable Mode**: By default, this option is set to Yes. You can modify it to No.
- **Enable Pairing**: By default, this option is set to Yes. You can modify it to No.
- **Enable Secure Mode**: By default, this option is set to No. If you modify it to Yes, the following fields are active:
    - **Secure Mode Services Enabled**: Select the services from the list.
    - **Secure Mode Whitelisted Profiles**: Select the profiles from the list.

6. Click **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
7. Click **Save and Continue** button to stay on the same page and perform other updates on policy.

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

Set Network Policy for Windows 6.x

1. To specify Network policy for Windows 6.x platform, follow these steps:



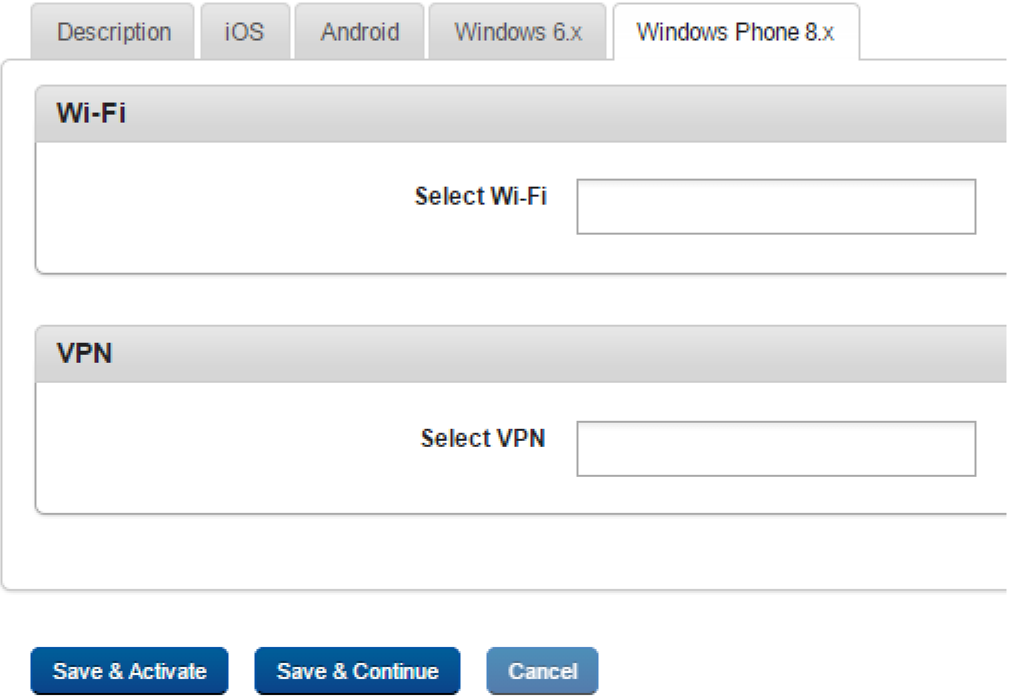
2. **Allow Wifi Only**: By default, this option is set to No. You can modify it to Yes.
3. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
4. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

> *Note:* To apply Network Policy, Passcode policy must be there and device should have a passcode.

Set Network Policy for Windows Phone 8X

1. To specify network policy for Windows 8.X platform, follow these steps:



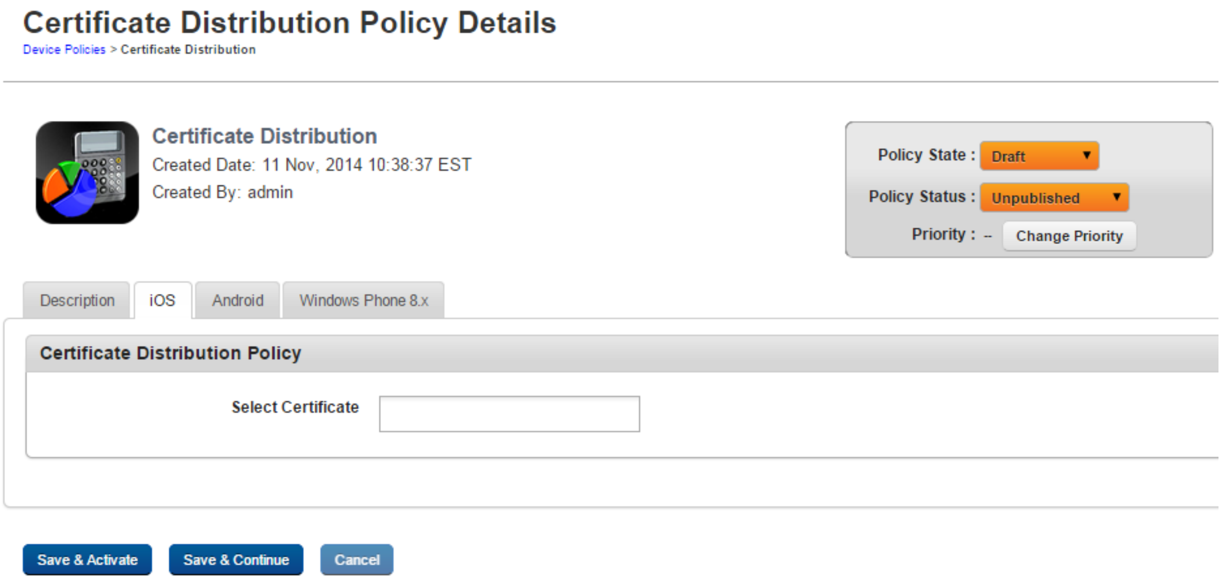
2. **Wi- Fi:** Select one Wi-Fi from the enterprise resources list.

3. **VPN**: Select one VPN from the enterprise resources list.

4. Click **Save and Continue** to stay on the same page and perform other policy updates. Or **Click Save and Activate**.

10.4.6 Certificate Distribution Policy

The primary purpose of the Certificate Distribution policy is to ensure that appropriate certificates are uploaded so the users can access the required data securely.



Certificate Distribution Policy Details

Device Policies > Certificate Distribution

Certificate Distribution
Created Date: 11 Nov, 2014 10:38:37 EST
Created By: admin

Policy State : Draft
Policy Status : Unpublished
Priority : – Change Priority

Certificate Distribution Policy

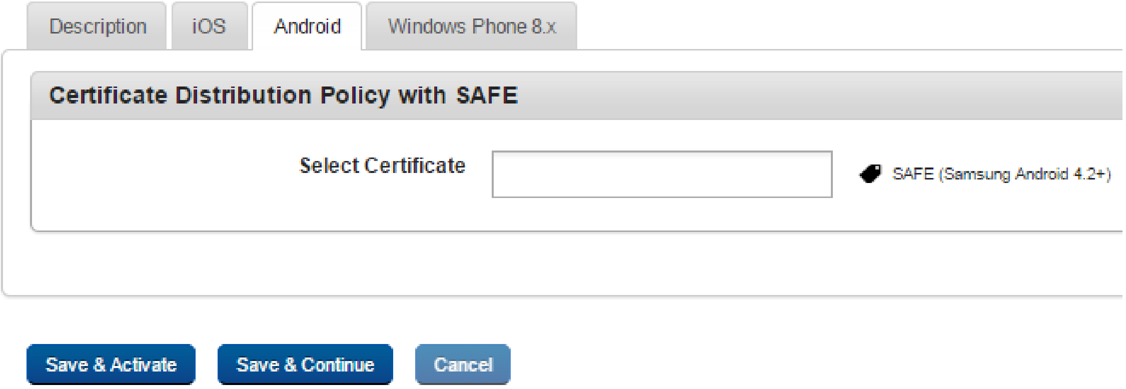
Select Certificate

To set Certificate Distribution policy for iOS, follow these steps:

1. **Description**: By default, this tab is set to Active. Enter the appropriate description for the Certificate Distribution policy.
2. Click the iOS tab to open Certificate Distribution Policy section. You can add more certificates at Enterprise Resources > Certificates.
3. Select the required certificate from the **Select Certificate** list.
4. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
5. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

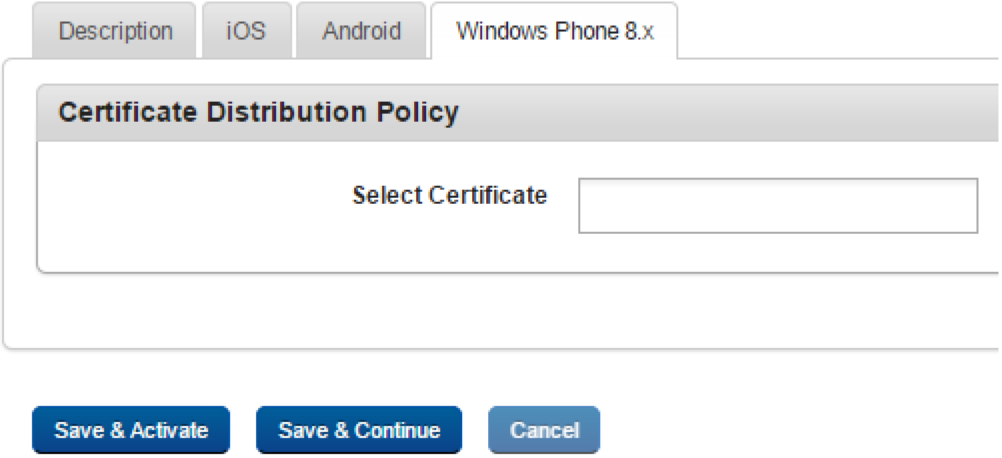
To set Certificate Distribution policy for Android, follow these steps:



1. Click the Android tab to open Certificate Distribution Policy section.
2. Select the required certificate from the **Selected Certificate** list. You can add more certificates at Enterprise Resources > Certificates.
3. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
4. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

To set Certificate Distribution policy for Windows Phone 8.x, follow these steps:

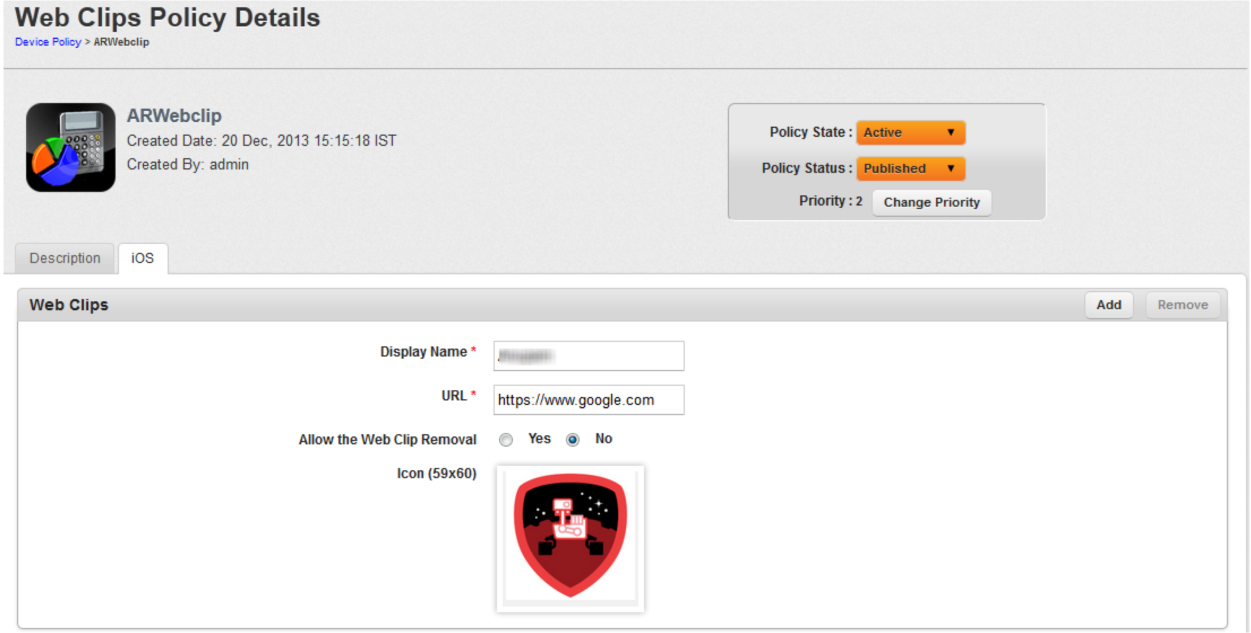


1. Click **Windows Phone 8.x** tab to open Certificate Distribution Policy section.
2. Select the required certificate from the **Selected Certificate** list. You can add more certificates at Enterprise Resources > Certificates.
3. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.
4. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.4.7 Webclips Policy

The primary purpose of the Webclips policy is to specify an icon that conveys the essence of your web application.



Web Clips Policy Details

Device Policy > ARWebclip

ARWebclip
Created Date: 20 Dec, 2013 15:15:18 IST
Created By: admin

Policy State : Active ▾
Policy Status : Published ▾
Priority : 2

Display Name * [redacted]

URL * https://www.google.com

Allow the Web Clip Removal ○ Yes ● No

Icon (59x60)

To specify an icon to represent your web application or webpage on iOS, follow these steps:

1. **Device Policy Description**: Enter a brief description of the Webclips policy, which explains its objective.

   By default, Description tab is set to active.

   Click the **iOS** tab. **Web Clips pane** appears. Enter details into following fields.

2. **Display Name**: Enter an appropriate name for the webclip which signifies its utility. This name is displayed on a device

3. **URL**: Enter the Web application address that is accessed by the webclip icon.

4. **Allow the Web Clip Removal**: By default, this option is set to Yes. You can modify it to No.

5. **Icon(59x60):** Click the Browse button to select the icon from its location to upload.

6. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

7. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

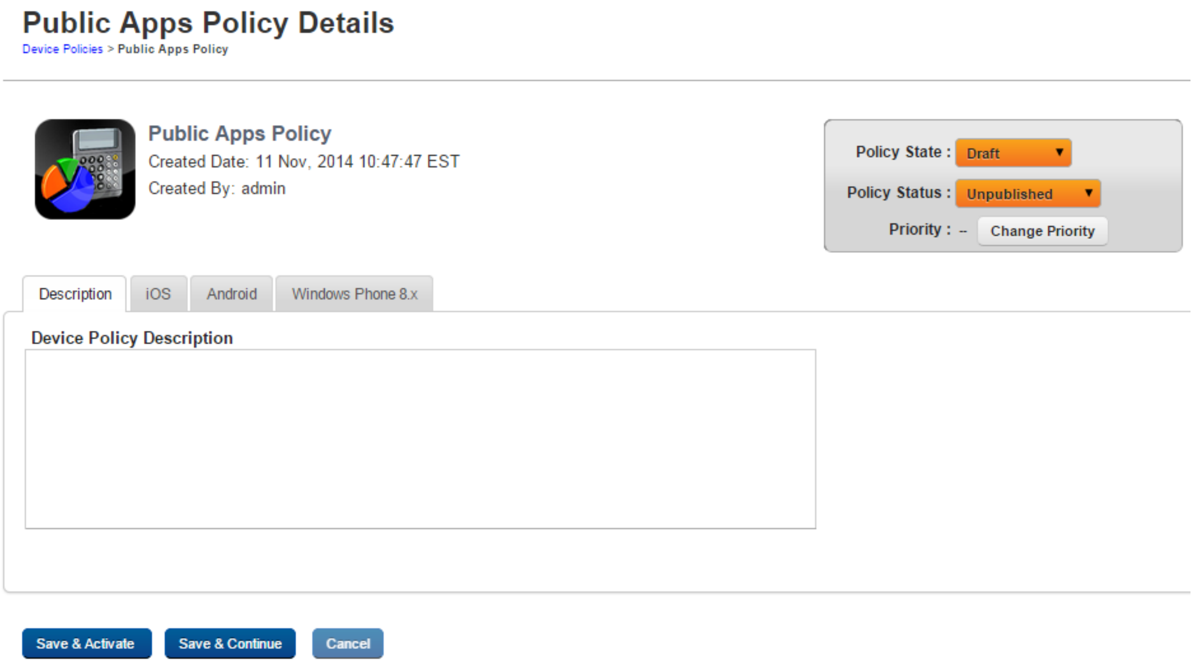
   Click the **Cancel** button to close the window.

   > ***Note:*** (For iOS) The webclip icon pushed from the server is replaced by the icon of the website once the website loads completely on the browser.

If you face any issues with Internet Explorer 9, refer to Annexure.

10.4.8 Public App Policy

The primary purpose of the Public App policy is to have complete control over devices and ensure data security based on existing business rules.


Public Apps Policy Details
Device Policies > Public Apps Policy
Public Apps Policy
Created Date: 11 Nov, 2014 10:47:47 EST
Created By: admin
Policy State : Draft
Policy Status : Unpublished
Priority : -- Change Priority
Description
iOS
Android
Windows Phone 8.x
Device Policy Description
Save & Activate
Save & Continue
Cancel

You can set public app policies for the following operating systems.

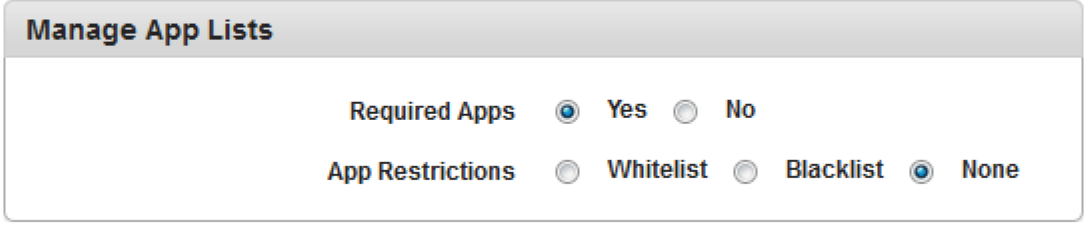
> *Important:* For a public app policy to work for iOS and Android devices, you must have the **Enforce App policy** feature of the Compliance policy to be set to **Yes**. For more information, see Compliance policy.

- Set Public App Policy for iOS
- Set Public App Policy for Android
- Set Public App Policy for Windows Phone 8.x

10.4.8.1 Set Public App Policy for iOS

To set the App Policy for iOS, follow these steps:

1. Click **iOS** tab to open.
2. In the Manage App Lists, do the following:



Manage App Lists

Required Apps ● Yes ○ No

App Restrictions ○ Whitelist ○ Blacklist ● None

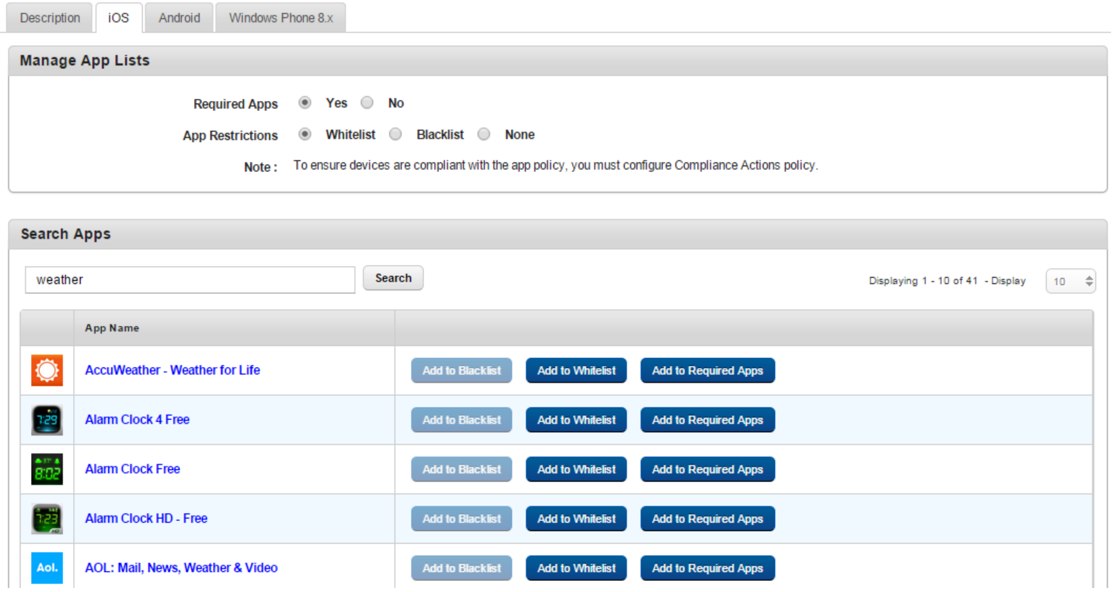
a. **Required Apps**: By default, this option is set to **Yes**. You can modify it to **No**.

   If this option is set to **Yes**, the Add to Required Apps button is active in the Search Apps section.

b. **App Restrictions**: By default, this option is set to **None**. You can modify it to Whitelist Apps or Blacklist Apps.

   Based on the option selected, one of the following buttons will be active in the Search Apps section:

   - Add to Whitelist Apps
   - Add to Blacklist Apps



Manage App Lists

Required Apps ● Yes ○ No

App Restrictions ● Whitelist ○ Blacklist ○ None

Note : To ensure devices are compliant with the app policy, you must configure Compliance Actions policy.

Search Apps

weather

Displaying 1 - 10 of 41 - Display 10

	App Name	
	AccuWeather - Weather for Life	Add to Blacklist · Add to Whitelist · Add to Required Apps
	Alarm Clock 4 Free	Add to Blacklist · Add to Whitelist · Add to Required Apps
	Alarm Clock Free	Add to Blacklist · Add to Whitelist · Add to Required Apps
	Alarm Clock HD - Free	Add to Blacklist · Add to Whitelist · Add to Required Apps
Aol.	AOL: Mail, News, Weather & Video	Add to Blacklist · Add to Whitelist · Add to Required Apps

3. In the **Search** text box under the **Search Apps** section, enter your text for the app, and click the **Search** button. The system displays apps from Apple App Store and Google Play. The selected apps appear in the list view with **App Name**, **Source** and manage app options. When you search for an app, unrelated apps are displayed as a result in list view. You can create either Blacklist apps or Whitelist apps but not both.

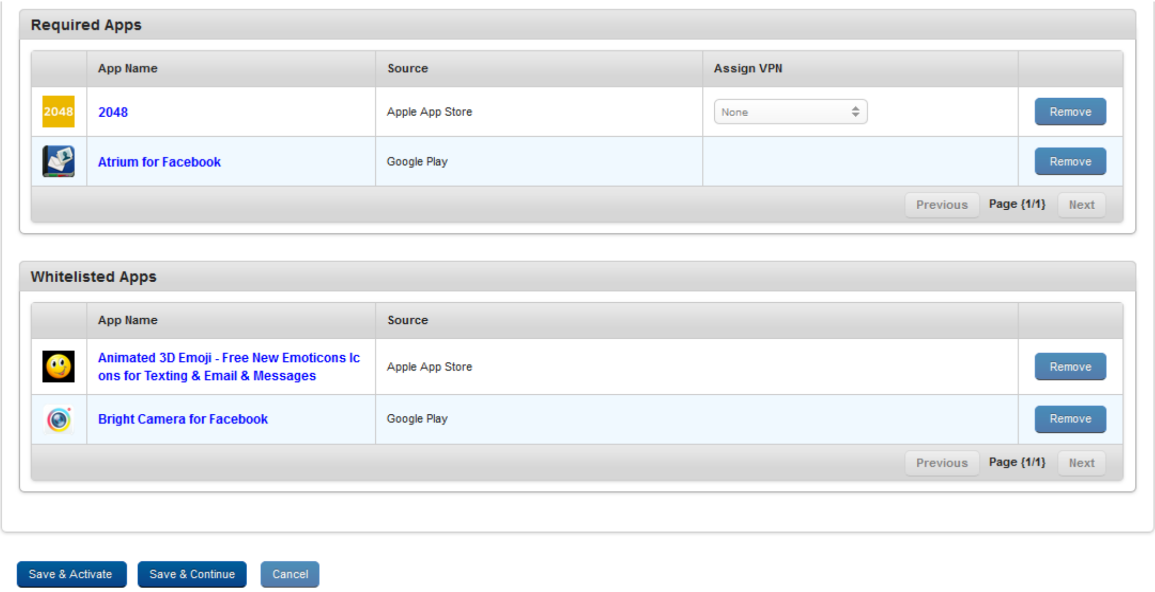
   Based on the options selected in the **Manage App Lists** section, you can add the apps to Blacklist, Whitelist, or Required list.

4. Click the buttons to add apps into the requited category as follows:

   - **Add to Required Apps**
     Required apps must be installed on devices. For iOS, these apps are installed automatically.
   - **Add to Whitelist**
     A Whitelist is a list of apps that you choose whether to install it.
   - **Add to Blacklist**

     A Blacklist is a list of apps that are not allowed to be installed on devices.

   According to the selected category, the system displays apps in various sections with details. For example, the Required Apps section has the **App Name**, **Source** and **Assign VPN** columns.



Required Apps

	App Name	Source	Assign VPN	
2048	2048	Apple App Store	None	Remove
	Atrium for Facebook	Google Play		Remove

Previous Page (1/1) Next

Whitelisted Apps

	App Name	Source	
	Animated 3D Emoji - Free New Emoticons Icons for Texting & Email & Messages	Apple App Store	Remove
	Bright Camera for Facebook	Google Play	Remove

Previous Page (1/1) Next

Whitelisted apps are installed by a user from the Apple App Store. They are considered as Personal apps as they are not pushed by the EMM Server.

> ***Note:*** When app policy alone is pushed along with compliance policy (no other policies are pushed apart from app policy and compliance policy), the view policy pop-up does not display applied policies under server resolved and device acknowledged policy columns. You can check the status of policy delivery in event log.

5. Select one of the VPNs from the **Per App VPN** drop-down list, and assign it for the desired app.

   Only VPNs enabled to be Per App VPN are displayed in the **Per App VPN** drop-down list. For more details, refer Assigning Per App VPN for iOS.

   You can remove any app from the Required or Whitelisted or Blacklisted Apps list by clicking the **Remove** button.

6. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

7. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

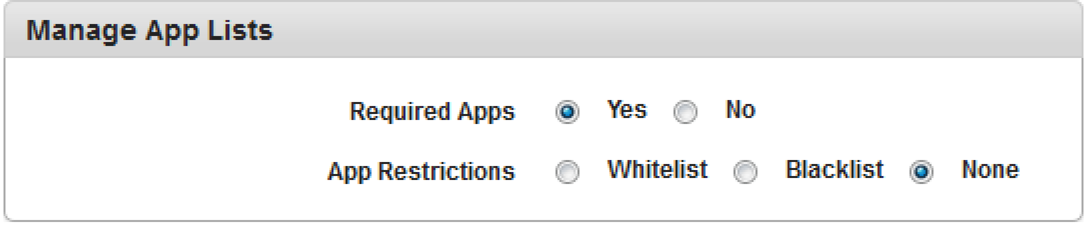
   Click the **Cancel** button to close the window.

   > ***Note:*** On iOS 7.0, whenever a mandatory app is upgraded, the app is installed on device silently.

10.4.8.2 Public App Policy for Android

To set the App Policy for Android, follow these steps:

1. Click **Android** tab.
2. In the Manage App Lists, do the following:



Manage App Lists

Required Apps ● Yes ○ No

App Restrictions ○ Whitelist ○ Blacklist ● None

   a. **Required Apps**: By default this option is set to **Yes**. You can modify it to **No**.

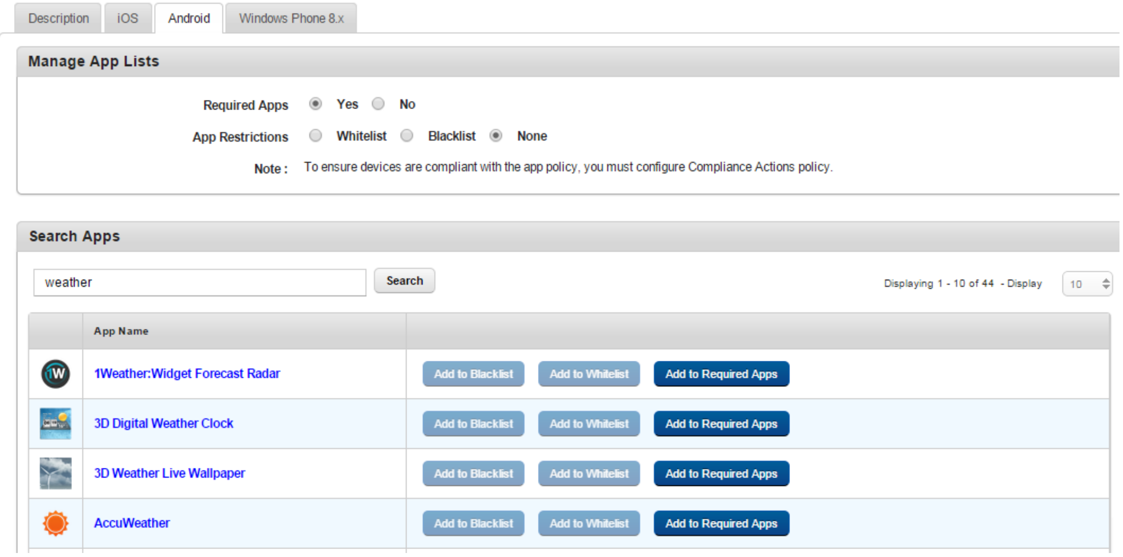
      If this option is set to **Yes**, the Add to Required Apps button is active in the Search Apps section.

   b. **App Restrictions**: By default this option is set to **None**. You can modify it to Whitelist or Blacklist.

> ***Note:*** To ensure devices are compliant with the app policy, you must configure Compliance Actions policy.
> System applications cannot be managed using App Policy.
> Some Carriers /OEMs /Vendors might pre-install Public applications as System Applications. Such applications will not be managed with App Policy.

Based on the option selected, one of the following buttons will be active in the Search Apps section.

- Add to Whitelist Apps
- Add to Blacklist Apps



Manage App Lists

Required Apps ● Yes ○ No

App Restrictions ○ Whitelist ○ Blacklist ● None

Note : To ensure devices are compliant with the app policy, you must configure Compliance Actions policy.

Search Apps

weather [Search]

Displaying 1 - 10 of 44 - Display 10

	App Name	
	1Weather:Widget Forecast Radar	Add to Blacklist · Add to Whitelist · Add to Required Apps
	3D Digital Weather Clock	Add to Blacklist · Add to Whitelist · Add to Required Apps
	3D Weather Live Wallpaper	Add to Blacklist · Add to Whitelist · Add to Required Apps
	AccuWeather	Add to Blacklist · Add to Whitelist · Add to Required Apps

3. Under **Search Apps** section, enter your text for the app in the text field, and click the **Search** button. The system displays apps from Apple App Store and Google Play. The selected apps appear in the list view with **App Name**, **Source** and manage app options. When you search for an app, unrelated apps are displayed as a result in list view. You can create either Blacklist or Whitelist apps but not both.

   Based on the options selected in the **Manage App Lists** section, you can add the apps to Blacklist, Whitelist, or Required list.

4. Click the buttons to add apps into the requited category as follows:

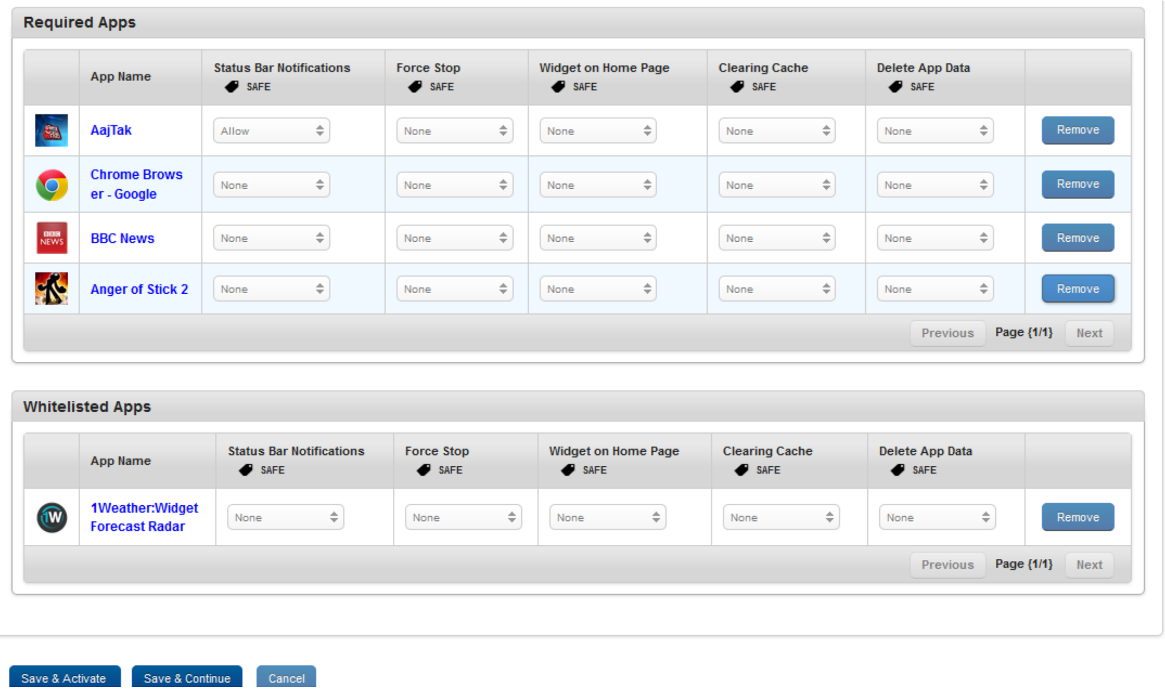
   - **Add to Required Apps**
     Required apps are must be installed on devices. For iOS these apps are installed automatically.

   - **Add to Whitelist**
     A Whitelist is a list of apps that are allowed for you to choose whether to install it.

   - **Add to Blacklist**

     A Blacklist is the list of apps that are not allowed to install on devices.

As per the selected category, the system displays apps in various sections with details. For example, Required Apps section has the **App Name**, **Status Bar Notifications, Force Stop, Widget on Home Page, Clearing Cache,** and **Delete App Data** columns.



Required Apps

	App Name	Status Bar Notifications SAFE	Force Stop SAFE	Widget on Home Page SAFE	Clearing Cache SAFE	Delete App Data SAFE	
	AajTak	Allow	None	None	None	None	Remove
	Chrome Browser - Google	None	None	None	None	None	Remove
	BBC News	None	None	None	None	None	Remove
	Anger of Stick 2	None	None	None	None	None	Remove

Whitelisted Apps

	App Name	Status Bar Notifications SAFE	Force Stop SAFE	Widget on Home Page SAFE	Clearing Cache SAFE	Delete App Data SAFE	
	1Weather:Widget Forecast Radar	None	None	None	None	None	Remove

Whitelisted apps are installed by a User from the Google Play Store. They are considered as Personal apps as they are not pushed by the EMM Server.

> ***Note:*** When App policy alone is pushed along with Compliance policy (no other policies are pushed apart from app policy and compliance policy), the View Policy pop-up does not display applied policies under Server resolved and Device acknowledged policy columns. You can check the status of policy delivery in event log.

5. Configure SAFE for Required or Whitelisted or Blacklisted Apps if required:

   a. **Status Bar Notifications**: By default, this option is set to None You can modify it to Allow or Block.
   The Admin can specify whether messages received by the app can be shown in the status bar or not by selecting Allow.
   If Block is selected, any messages received by the app are not shown in the status bar.

   b. **Force Stop**: By default, this option is set to None You can modify it to Allow or Block.

   The Admin can specify whether the User has the ability to Force Stop an app by selecting Allow.

   If Blocked is selected, the user cannot Force Stop the app.

   c. **Widget on Home Page**: By default, this option is set to None. You can modify it to Allow or Block.
   The Admin can specify whether the widgets of an app are allowed to become a widget on the device home page by selecting Allow.
   If Block is selected, the user cannot add widgets of that app to the home page.

   d. **Clearing Cache**: By default, this option is set to None You can modify it to Allow or Block.

   e. **Delete App Data**: By default, this option is set to None You can modify it to Allow or Block.

You can remove any app from the Required or Whitelisted or Blacklisted Apps list by clicking the **Remove** button.

6. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

7. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

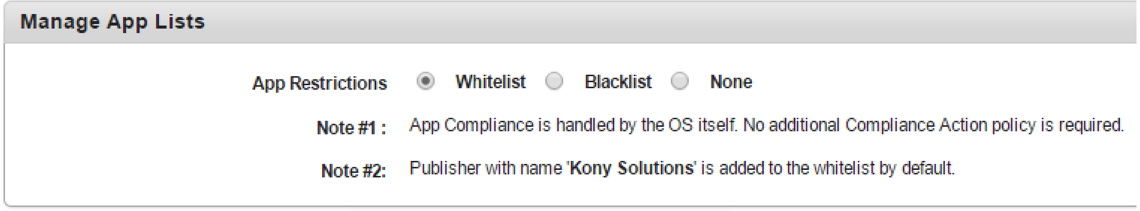
   Click the **Cancel** button to close the window.

10.4.8.3 Public App Policy for Windows Phone 8.X

To set the App Policy for Windows Phone 8X,

1. Click **Windows Phone 8.x** tab.

2. Navigate to Manage App Lists. By default, the App Restrictions option is set to **None**. You can modify it to Whitelist or Blacklist.



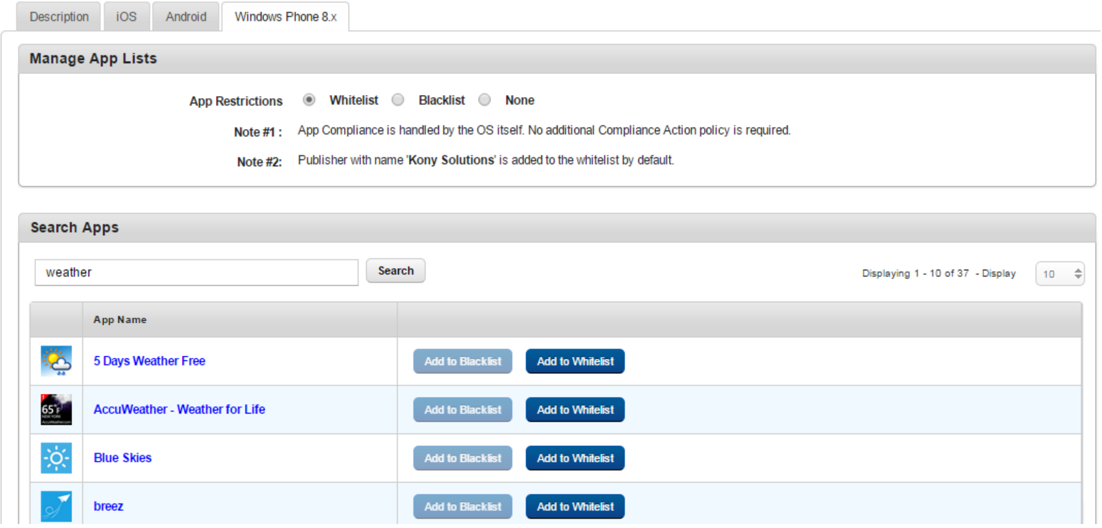
Manage App Lists

App Restrictions ● Whitelist ○ Blacklist ○ None

Note #1 : App Compliance is handled by the OS itself. No additional Compliance Action policy is required.

Note #2: Publisher with name '**Kony Solutions**' is added to the whitelist by default.

- Add to Whitelist
- Add to Blacklist



Manage App Lists

App Restrictions ● Whitelist ○ Blacklist ○ None

Note #1 : App Compliance is handled by the OS itself. No additional Compliance Action policy is required.

Note #2: Publisher with name '**Kony Solutions**' is added to the whitelist by default.

Search Apps

weather

Displaying 1 - 10 of 37 - Display 10

	App Name	
	5 Days Weather Free	Add to Blacklist Add to Whitelist
	AccuWeather - Weather for Life	Add to Blacklist Add to Whitelist
	Blue Skies	Add to Blacklist Add to Whitelist
	breez	Add to Blacklist Add to Whitelist

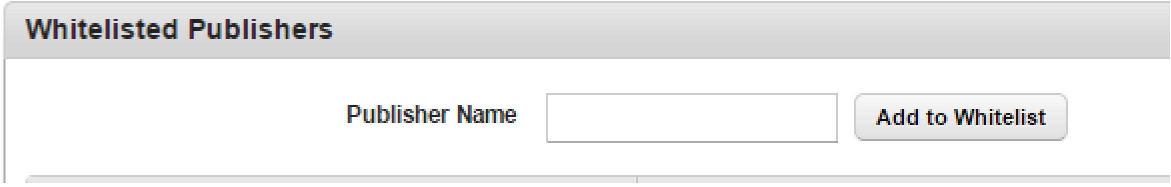
3. Under **Search Apps** section, enter your text for the app in the text field, and click the **Search** button. The system displays apps from the Windows App Store. The selected apps appear in the list view with **App Name**, and **Add to Black List and Add to Whitelist** options. You can create either Blacklist or Whitelist apps but not both.

4. Based on selections in Manage App Lists, click **Add to Whitelist** or **Add to Blacklist** to add apps to the required category.

5. You can remove any app from the Whitelisted or Blacklisted Apps list by clicking the **Remove** button.

6. You can add a publisher to the Whitelist or a Blacklist.

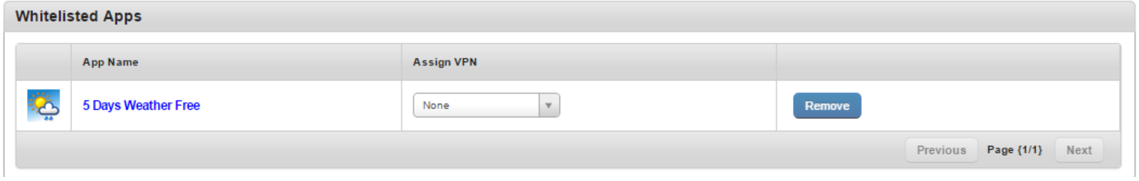
    a. To add a publisher, from the **Whitelisted Publishers** section, enter the publisher name in the **Publisher** text box and click **Add to Whitelist**. You can search and download apps from a whitelisted publisher.


Whitelisted Publishers

Publisher Name

b. To add a publisher, from the **Blacklisted Publishers** section, enter the publisher name in **Publisher** text box and click **Add to Blacklist**. The publisher is added to Blacklist. You cannot search and download apps from a Blacklisted publisher.

7. Remove a publisher from the Whitelisted or Blacklisted Apps list by clicking the **Remove** button.



Whitelisted Apps

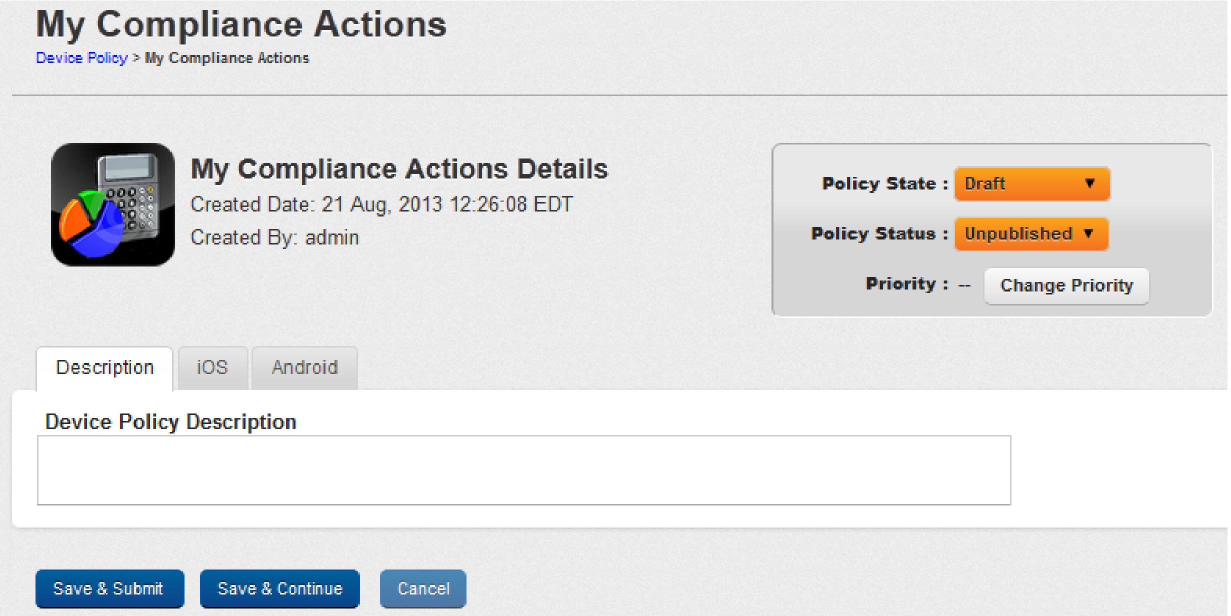
	App Name	Assign VPN	
	5 Days Weather Free	None	Remove

8. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

9. Click the **Save and Continue** button to stay on the same page and perform other updates on policy. To close the window. click **Cancel**.

10.4.9 Compliance Actions Policy

The primary purpose of the Compliance Actions policy is to restrict the device usage if they do not adhere to the policy and trigger appropriate action depending upon the business rules.



My Compliance Actions

Device Policy > My Compliance Actions

My Compliance Actions Details

Created Date: 21 Aug, 2013 12:26:08 EDT

Created By: admin

Policy State : Draft

Policy Status : Unpublished

Priority : --

Device Policy Description

10.4.9.1 Enforcement Actions

Enforcement actions allow the Admin to define a bunch of compliance actions against devices that violate the Policy applicable. When a device performs a compliance violation act, an enforcement action is triggered within a specified time frame with respect to the event occurrence.

The Admin can perform the following Enforcement Actions:

Enforcement Actions	Description
Alert Administrator	In case of non-compliance of the policies alert the Admin immediately.
Alert User and Administrator	In case of non-compliance of the policies alert the Admin and User immediately.
Reset Passcode and Lock	This action is only available for Android devices. The device's passcode can be changed automatically and locked. This locks users out of their own non-compliant devices. The User must contact Admin to gain access to the device again.
Block Email	Block Email blocks access to the Exchange ActiveSync. The user shall not be able to view emails from Exchange server again.
Enterprise Wipe	Enterprise wipe selectively erases only those device settings, user data, applications and application data that were previously installed by Kony EMM.
Complete Wipe	When a device is Completely Wiped, the future enrollment rule is by default set to Never Enroll. Complete Wipe erases complete data including Enterprise settings and user-installed public applications, data or device settings configured by the user. For an Employee-Owned device, when a Complete Wipe is sent as an Enforcement Action, the state should be suspended with Enterprise Wipe

Enforcement Actions	Description
Remove App Data	This action removes app data from the device. Remove App Data is only applicable to Enterprise Apps pushed through EMM and not side-loaded apps.

If a device is non-compliant, with every heartbeat, the chosen compliance action is executed on it until the device comes back into compliance. Automatically mails are also triggered intimating the users and the Administrators about the action. If a device changes compliance state after a policy acknowledgment, you need to wait until next heart beat for corresponding violation actions.

When a device is Completely Wiped, the future enrollment rule is by default set to Never Enroll.

> *Important:*
> **(For Employee owned Devices only)**
> If you select Complete Wipe as Enforcement Action, then Enterprise Wipe with deactivated state is sent to the device.
>
> **(For Corporate and Shared Devices)**
> If you select Complete Wipe as Enforcement Action, then Complete Wipe occurs but future enrollment of the device is not possible.

Compliance actions can be defined in one of the following two modes, or both:

- Simple Compliance
- Conditional Compliance

An administrator can define both kinds of compliance actions for each platform and both set of rules must be applied to devices.

Simple Compliance

In the case of simple compliance, the current method is applied. There is no change in the simple compliance section.

Conditional Compliance Actions

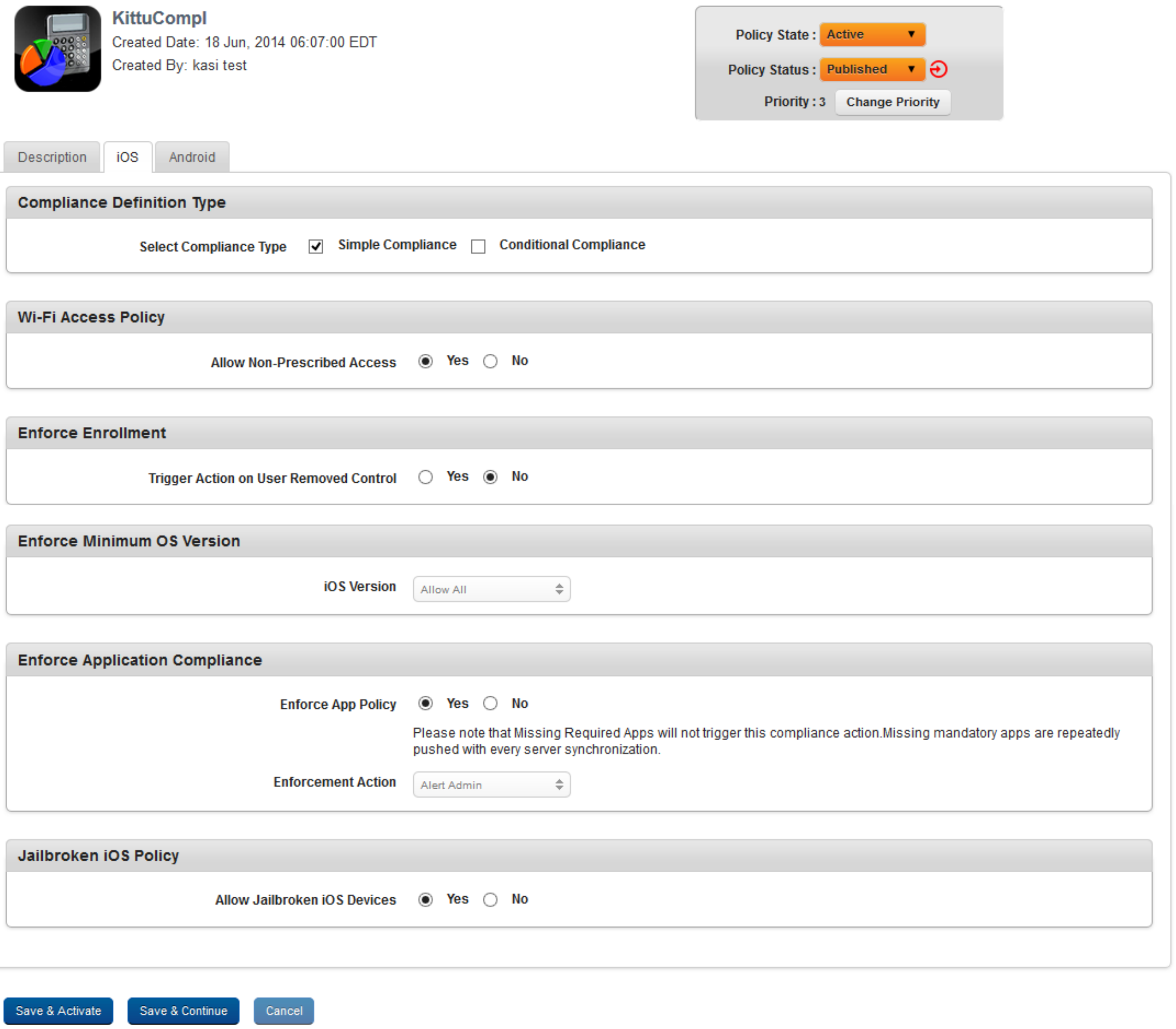
An administrator can also define composite compliance rules. This includes conditions for several compliance parameters and rules for a combined compliance conditions. Enforcement actions can be assigned for each rule definition. The same set of actions as in Simple compliance can be performed here.

The following is an example of a compliance rule: If a device is out of Wi-Fi compliance and app compliance, then block email.

You can set Compliance Actions Policy for the following operating systems:

- Set Compliance Action Policy for iOS
- Set Compliance Action Policy for Android

10.4.9.2 Set Compliance Action Policy for iOS



KittuCompl
Created Date: 18 Jun, 2014 06:07:00 EDT
Created By: kasi test

Policy State : Active
Policy Status : Published
Priority : 3

Compliance Definition Type

Select Compliance Type ☑ Simple Compliance □ Conditional Compliance

Wi-Fi Access Policy

Allow Non-Prescribed Access ● Yes ○ No

Enforce Enrollment

Trigger Action on User Removed Control ○ Yes ● No

Enforce Minimum OS Version

iOS Version: Allow All

Enforce Application Compliance

Enforce App Policy ● Yes ○ No

Please note that Missing Required Apps will not trigger this compliance action.Missing mandatory apps are repeatedly pushed with every server synchronization.

Enforcement Action: Alert Admin

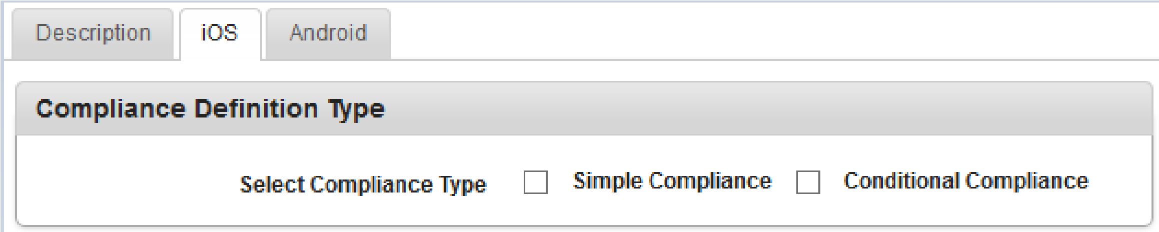
Jailbroken iOS Policy

Allow Jailbroken iOS Devices ● Yes ○ No

To set Compliance Action settings for iOS, follow these steps:

1. Enter a brief and appropriate description of the policy in the **Device Policy Description** text box.

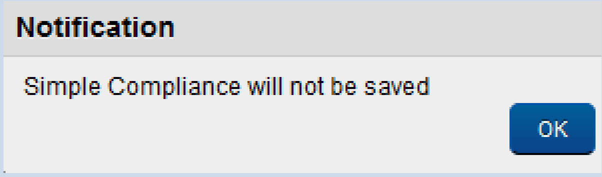
2. Click the **iOS** tab. The system displays the iOS tab with the **Compliance Definition Type** section by default. The Compliance Definition Type section has two checkboxes:



Compliance Definition Type

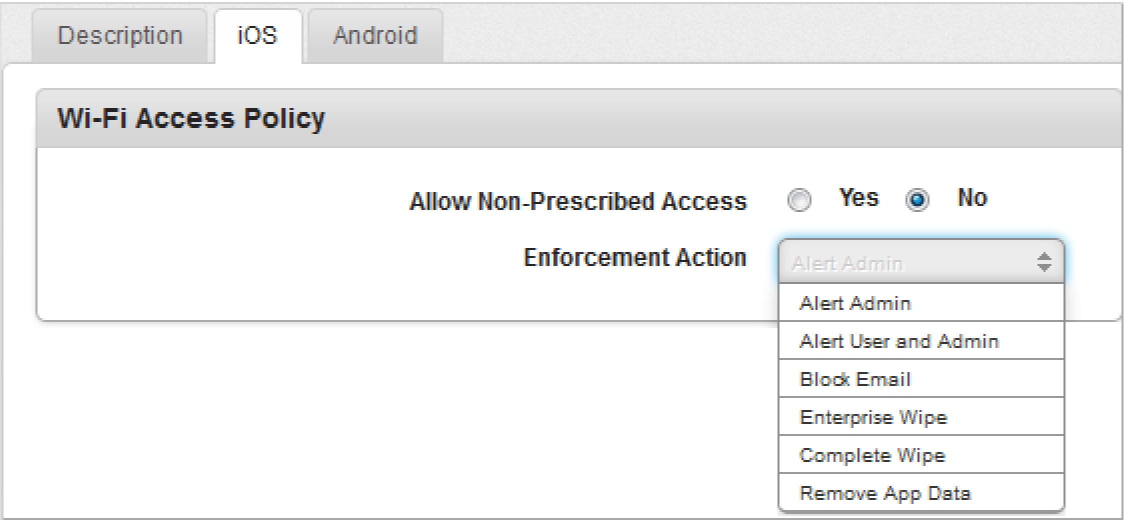
Select Compliance Type □ Simple Compliance □ Conditional Compliance

- Select Compliance Type as Simple Compliance
- Select Compliance Type as Conditional Compliance

> *Important:* If the check box is cleared without saving details, the system displays the following message "Simple Compliance will not be saved." or "Conditional Compliance will not be saved." Click **OK** to confirm.
>
> 
>
> Notification
>
> Simple Compliance will not be saved
>
>
>
> To prevent data loss, ensure that you save the details if required.

3. In the **Compliance Definition Type** section, select the **Simple Compliance** checkbox to configure simple compliance actions.

4. Enter details for the simple compliance actions:

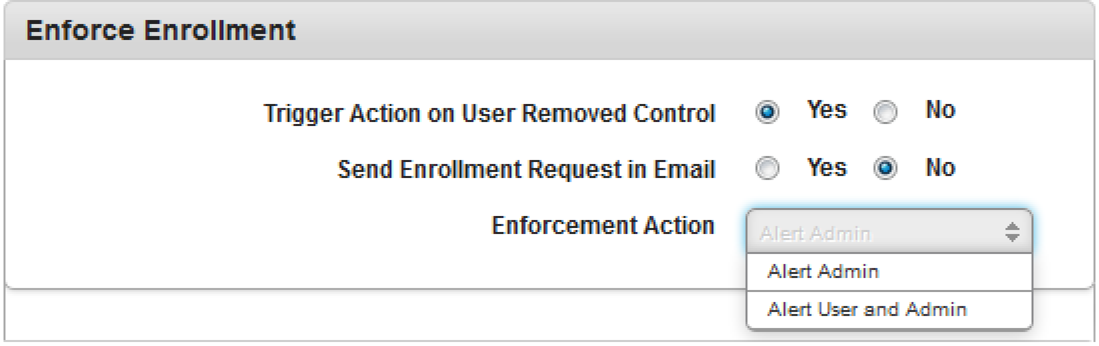


Wi-Fi Access Policy

Allow Non-Prescribed Access ○ Yes ● No

Enforcement Action: Alert Admin

a. **Wifi Access Policy**: This setting allows the Admin to create an alert for using or creating Wi-Fi connections not prescribed as part of the Policy. By default, **Allow Non-Prescribed Access** option is set to Yes. If you select this option as No, Enforcement Action drop-down menu appears. If required, select the required action from the dropdown list.



Enforce Enrollment

Trigger Action on User Removed Control ● Yes ○ No

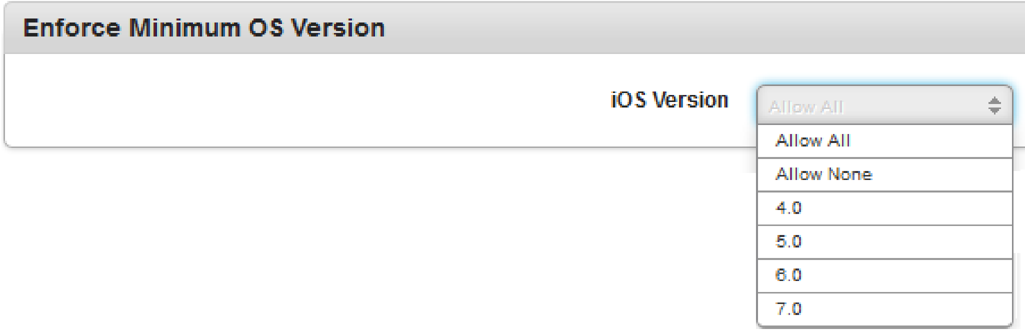
Send Enrollment Request in Email ○ Yes ● No

Enforcement Action: Alert Admin

b. **Enforce Enrollment**:

This setting allows the Admin to enforce enrollment of the device. By default, the **Trigger Action on User Removed Control** option is set to No. If you select this option as Yes, the **Send Enrollment Request in Email** option appears.

By default, **Send Enrollment Request in Email** option is set to No. You can select this option as Yes. If required, select the Enforcement Action - Alert Admin or Alert User and Admin from the drop-down list.

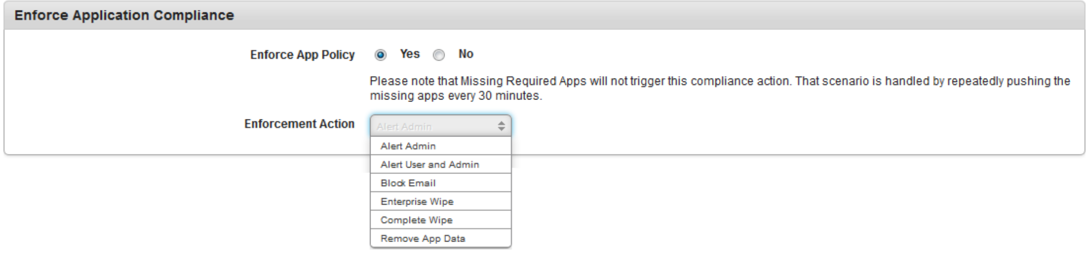


Enforce Minimum OS Version

iOS Version: Allow All

c. **Enforce Minimum OS Version**

This setting allows the administrator to set iOS version. By default, the **iOS Version** option is set to Allow All. You can select the desired iOS version from the above drop-down list.



Enforce Application Compliance

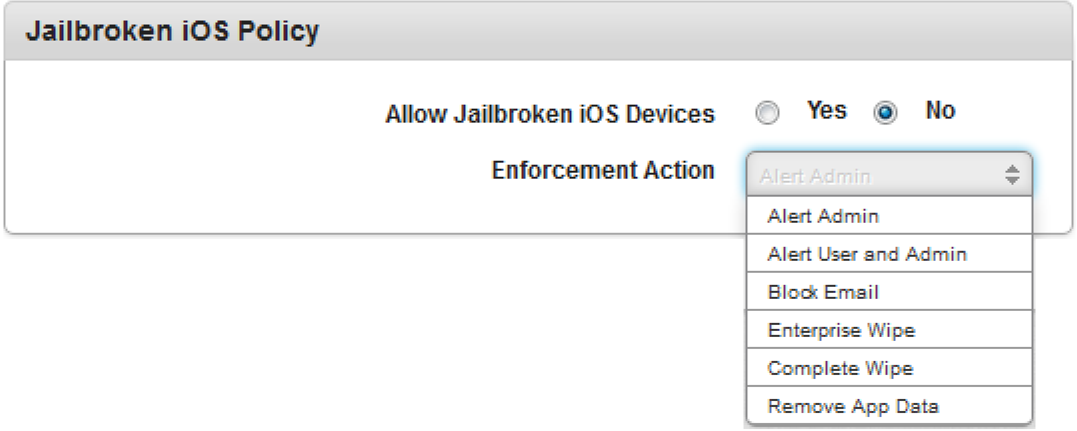
Enforce App Policy: ● Yes ○ No

Please note that Missing Required Apps will not trigger this compliance action. That scenario is handled by repeatedly pushing the missing apps every 30 minutes.

Enforcement Action: Alert Admin

d. **Enforce Application Compliance**

By default, **Enforce App Policy** option is set to Yes. If you select this option as No, the Enforcement Action drop-down list is removed from the screen. If required, select the required action from the dropdown list.



Jailbroken iOS Policy

Allow Jailbroken iOS Devices ○ Yes ● No

Enforcement Action: Alert Admin

e. **Jailbroken iOS Policy**

This setting defines if Jailbroken devices are allowed or not allowed. If Jailbroken devices are allowed, then no enforcement actions are defined. By default, Allow Jailbroken iOS Devices option is set to No. If you select the option as Yes, Enforcement Action drop-down list is removed from the screen.

f. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

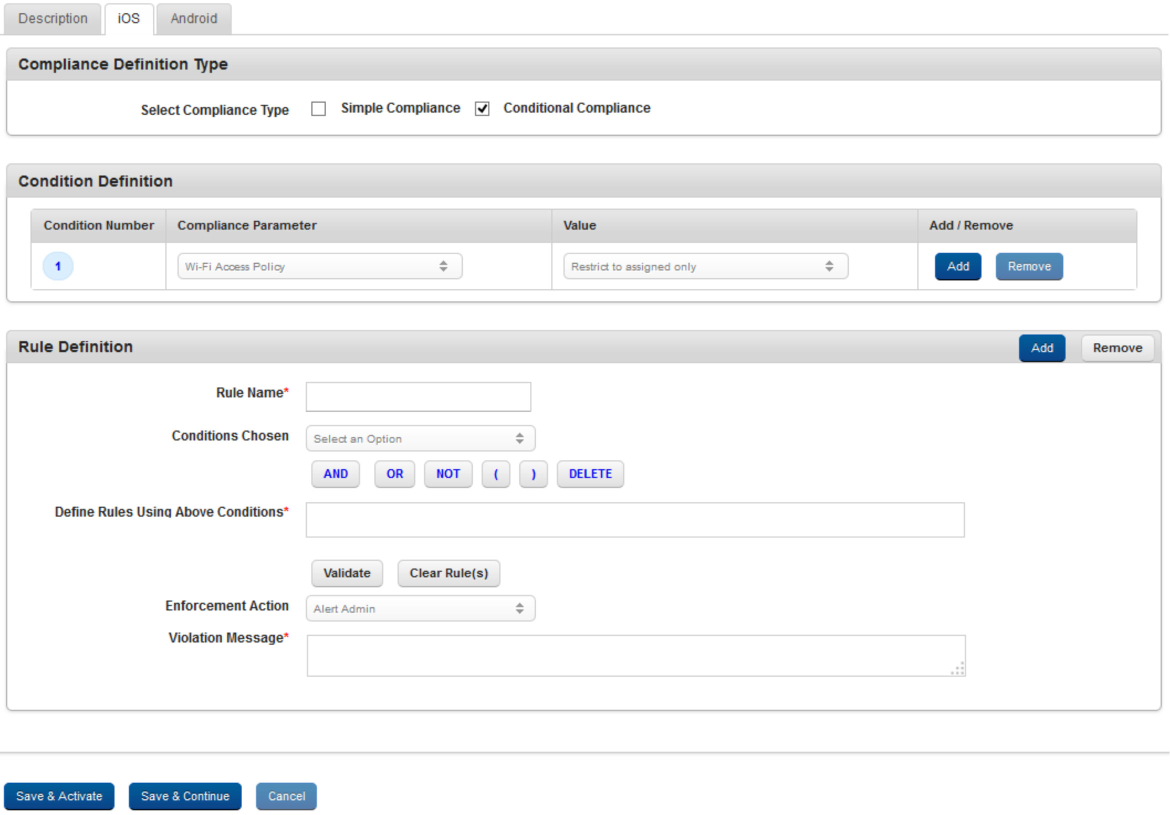
g. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.
Click the **Cancel** button to close the window.

5. In the **Compliance Definition Type** section, select the **Composite Compliance** check box to configure composite compliance actions.

6. Enter details for composite compliance actions:

By default, the Condition Definition section has the first row added with the Condition Number.

> ***Note:*** The Condition Number is the reference to entire row of the added compliance parameter in the grid that helps you use them to define different combined conditions in the Define Rules Using Above Conditions area.



Compliance Definition Type

Select Compliance Type □ Simple Compliance ☑ Conditional Compliance

Condition Definition

Condition Number	Compliance Parameter	Value	Add / Remove
1	Wi-Fi Access Policy	Restrict to assigned only	Add Remove

Rule Definition

Rule Name*

Conditions Chosen: Select an Option

Define Rules Using Above Conditions*

Enforcement Action: Alert Admin

Violation Message*

a. Under the **Compliance Parameter** column, select the parameter from the drop-down list. Based on the compliance parameter selected, the **Value** column is updated with options as required.

b. Select the value from the **Value** column drop-down list.

   You can add a new row in the Condition Definition section. To add a new row, click the **ADD** button under Add/Remove column.
   At least one condition must be exist. You can delete added rows. To delete a row, click the **Remove** button.

Once you are done with defining conditions, do the following in the **Rule Definition** section:

c. In **Rule Name**, enter the name for the rule definition.
   You can add new rule definitions. To add a rule definition, click the **ADD** button in the **Rule Definition** section.
   At least one rule definition must be exist. You can delete added rule definitions. To delete a rule definition, click the **Remove** button.

d. Select a condition from the **Conditions Chosen** drop-down list. The drop-down list is loaded with the conditions that you defined.

> ***Note:*** The system validates whether the rule definition follows BODMAS, a rule which specifies the order of operations in a mathematical expression. BODMAS stands for brackets, orders, division and multiplication, and addition and subtraction.

e. Click the logic button to apply the conditional logic. The system inserts the logic button next to the condition number in the Define Rules Using Above Conditions area. You can click any one of the six logic buttons as required, required - and, or, not, left parenthesis, right parenthesis, or delete.

   Repeat the step d through step e to complete your rule definition if required.

f. Click the **Validate** button. The system validates whether the rule definition follows the BODMAS (Brackets Of Division Multiplication Addition Subtraction) rule of selection. If the created rule syntax is correct, the system displays a message "*Syntax of the Rule is valid.*", else displays "*Syntax of the Rule is invalid. Please fix the same.*"

   Click the **Clear Rule** button if you want to clear all the rule definition details.

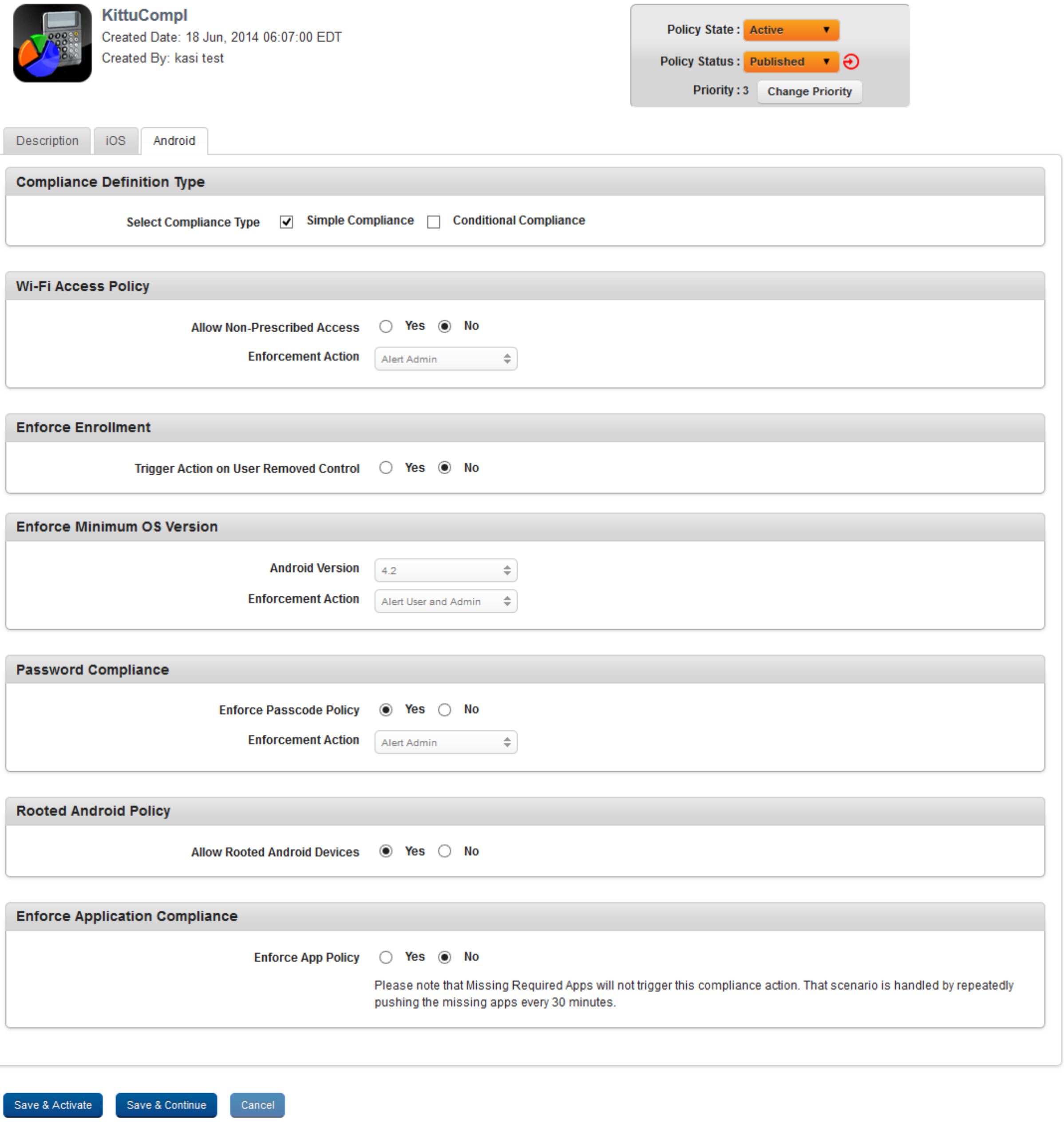
g. Select one of the actions from the **Enforcement Action** drop-down list for the above rule. Scroll down to the Violation Message text box, and enter a message. The message is displayed to users when an action in a rule definition is triggered.

h. Enter a message in the **Violation Message** text box. The message is displayed to users when an action in a Rule Definition is triggered.

i. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

j. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.
Click the **Cancel** button to close the window.

10.4.9.3 Set Compliance Action Policy for Android



KittuCompl
Created Date: 18 Jun, 2014 06:07:00 EDT
Created By: kasi test

Policy State : Active
Policy Status : Published
Priority : 3

Compliance Definition Type

Select Compliance Type ☑ Simple Compliance ☐ Conditional Compliance

Wi-Fi Access Policy

Allow Non-Prescribed Access ○ Yes ● No
Enforcement Action: Alert Admin

Enforce Enrollment

Trigger Action on User Removed Control ○ Yes ● No

Enforce Minimum OS Version

Android Version: 4.2
Enforcement Action: Alert User and Admin

Password Compliance

Enforce Passcode Policy ● Yes ○ No
Enforcement Action: Alert Admin

Rooted Android Policy

Allow Rooted Android Devices ● Yes ○ No

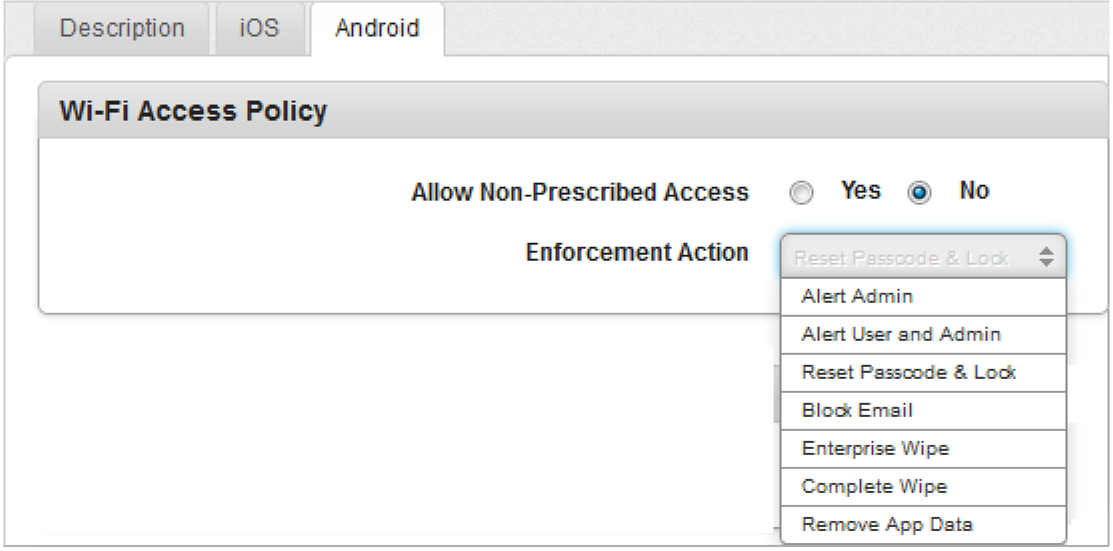
Enforce Application Compliance

Enforce App Policy ○ Yes ● No

Please note that Missing Required Apps will not trigger this compliance action. That scenario is handled by repeatedly pushing the missing apps every 30 minutes.

To set Compliance Action settings for Android, follow these steps:

1. Enter a brief description of the policy in Device Policy Description text box.
2. Click the **Android** tab. The system displays the Android tab with the Compliance Definition Type section by default. The Compliance Definition Type section has two check boxes:
   - Select Compliance Type as Simple Compliance
   - Select Compliance Type as Conditional Compliance
3. In the **Compliance Definition Type** section, select the **Simple Compliance** check box to configure simple compliance actions. The system displays the following:
4. Enter details for the simple compliance actions:



Description | iOS | Android

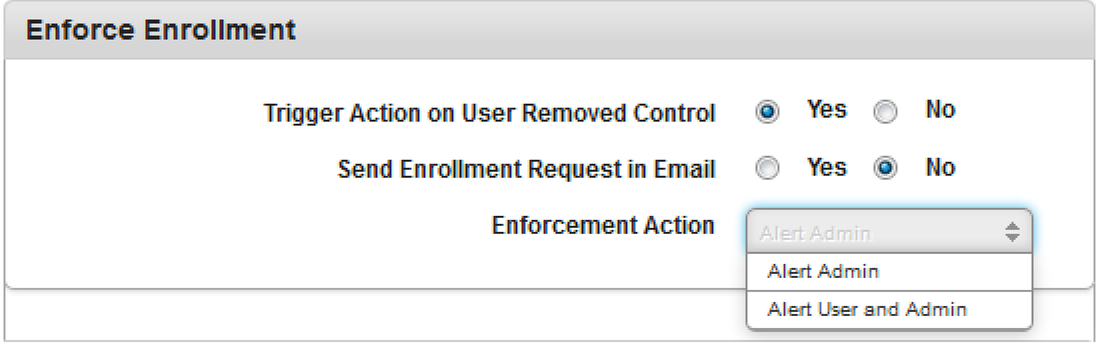
Wi-Fi Access Policy

Allow Non-Prescribed Access ○ Yes ● No

Enforcement Action: Reset Passcode & Lock

   a. **Wi-Fi Access Policy:**

      This setting allows the administrator to create an alert for using or creating Wi-Fi connections not prescribed as part of the policy. By default, the **Allow Non-Prescribed Access** option is set to Yes. If you select this option as No, Enforcement Action drop-down list appears. If required, select the required action from the drop-down list.



Enforce Enrollment

Trigger Action on User Removed Control ● Yes ○ No

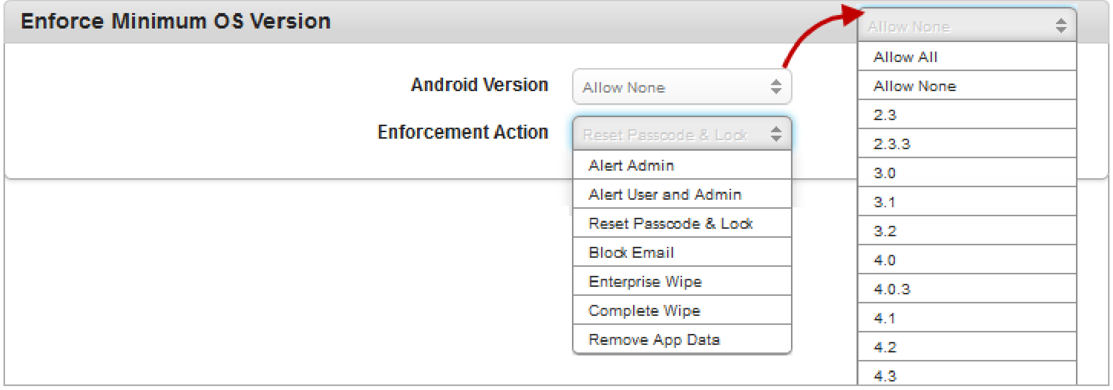
Send Enrollment Request in Email ○ Yes ● No

Enforcement Action: Alert Admin

b. **Enforce Enrollment**:

This setting allows the Admin to enforce enrollment of the device. By default the **Trigger Action on User Removed Control** option is set to No. If you select this option as Yes, the **Send Enrollment Request in Email** option appears.

By default, the **Send Enrollment Request in Email** option is set to No. If you select this option as Yes, the Enforcement Action drop-down list appears, as shown above. If required, select the required action from the dropdown list.



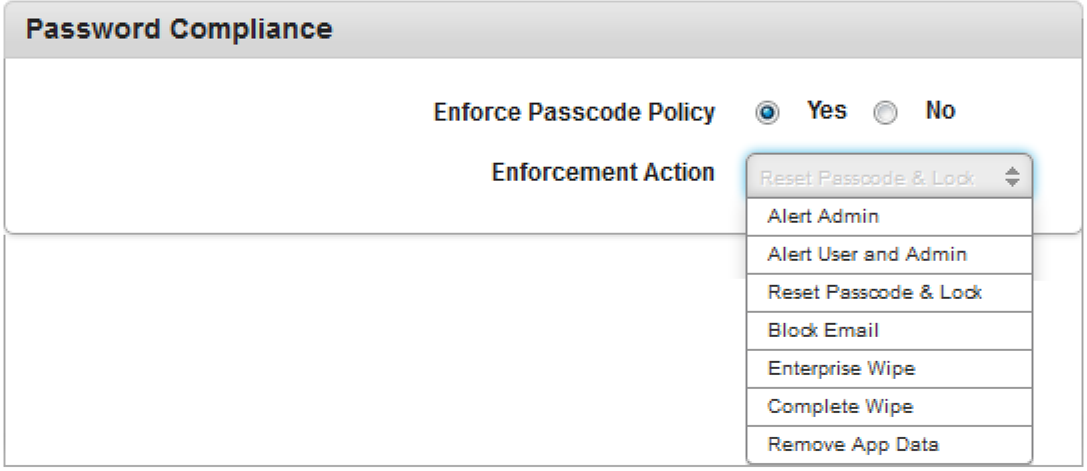
Enforce Minimum OS Version

Android Version: Allow None

Enforcement Action: Reset Passcode & Lock

c. **Enforce Minimum OS Version**

This setting allows the administrator to set Android version. By default, the Android Version option is set to Allow All. You can select the desired Android version from the drop-down list. If required, select the required action from the drop-down list.



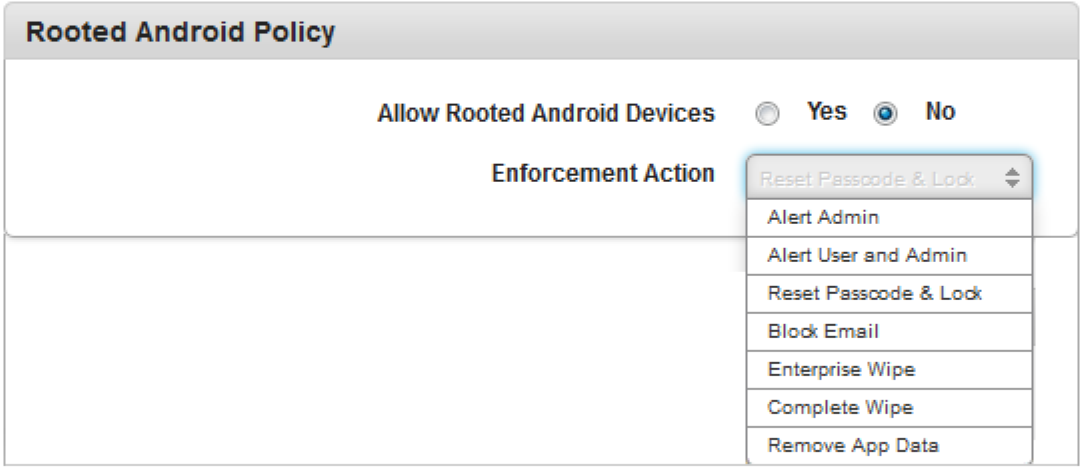
Password Compliance

Enforce Passcode Policy ● Yes ○ No

Enforcement Action: Reset Passcode & Lock

d. **Password Compliance**:

This setting allows the administrator to set Passcode policy on device. By default, the Password Compliance option is set to No. If you select this option as Yes, then the Enforcement Action drop-down list appears. If required, select the required action from the drop-down list.



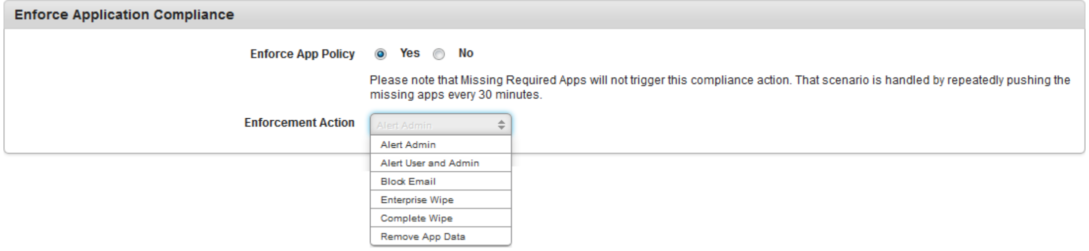
Rooted Android Policy

Allow Rooted Android Devices ○ Yes ● No

Enforcement Action: Reset Passcode & Lock

e. **Rooted Android**:

By default, the Allow Rooted Android Devices option is set to Yes. If you select this option as No, the Enforcement Action dropdown list appears. If required, select the required action from the dropdown list.



Enforce Application Compliance

Enforce App Policy ● Yes ○ No

Please note that Missing Required Apps will not trigger this compliance action. That scenario is handled by repeatedly pushing the missing apps every 30 minutes.

Enforcement Action: Alert Admin

f. **Enforce Application Compliance**

By default, **Enforce App Policy** option is set to Yes. If you select this option as No, Enforcement Action dropdown list is removed from the screen. If required, select the required action from the drop-down list.

5. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

6. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

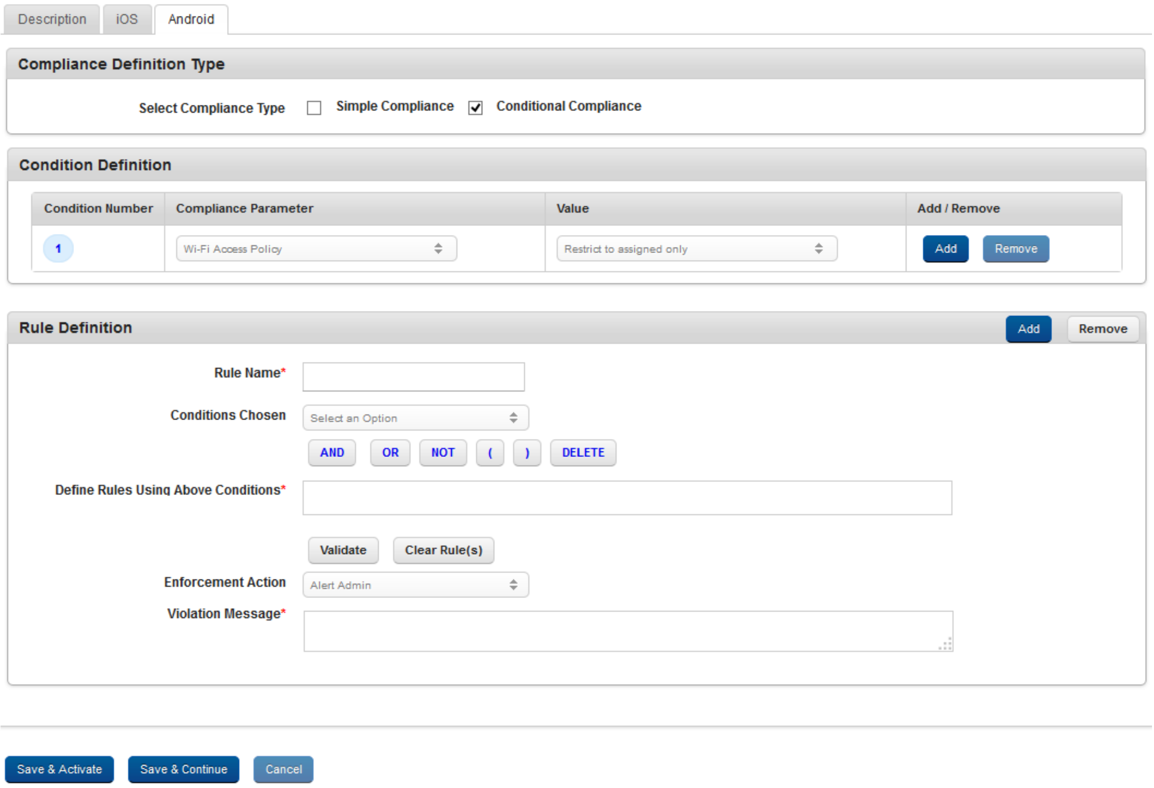
   Click the **Cancel** button to close the window.

7. In the **Compliance Definition Type** section, select the **Composite Compliance** check box to configure composite compliance actions.

8. Enter details for Composite compliance actions:

   By default, the Condition Definition section has first row added with the Condition Number.

> *Note:* The Condition Number is the reference to entire row of the added compliance parameter in the grid that helps you use them to define different combined conditions in the Define Rules Using Above Conditions area.



Compliance Definition Type

Select Compliance Type ☐ Simple Compliance ☑ Conditional Compliance

Condition Definition

Condition Number	Compliance Parameter	Value	Add / Remove
1	Wi-Fi Access Policy	Restrict to assigned only	Add Remove

Rule Definition

Rule Name*

Conditions Chosen: Select an Option

Define Rules Using Above Conditions*

Enforcement Action: Alert Admin

Violation Message*

a. Under the **Compliance Parameter** column, select the parameter from drop-down list. Based on the compliance parameter selected, the **Value** column is updated with options as required.

b. Select the value from the **Value** column drop-down list.

   You can add a new row in the Condition Definition section. To add a new row, click the **ADD** button under Add/Remove column.
   At least one condition must be exist.

When finished defining conditions, scroll to the **Rule Definition** section.

c. In **Rule Name** field, enter the name for the rule definition. To delete a rule definition, click the Remove button.
   You can add new rule definitions. To add a rule definition, click the **ADD** button in the **Rule Definition** section.
   At least one rule definition must exist.

d. Select a condition from the **Conditions Chosen** drop-down list. The drop-down list is loaded with the number of conditions that you defined.

e. Click the logic button to apply the conditional logic. The system inserts the logic button next to the condition number in the Define Rules Using Above Conditions area. You can click any one of the six logic buttons as required - and, or, not, left parenthesis, right parenthesis, and delete.

   Repeat the step d through step e to complete your rule definition if required.

f. Click the **Validate** button. If the created rule syntax is correct, the system displays a message "*Syntax of the Rule is valid.*", else displays "*Syntax of the Rule is invalid. Please fix the same.*"

   Click the **Clear Rule** button to clear all the rule definition details.

g. Select one of the actions from the **Enforcement Action** drop-down list for the above rule.

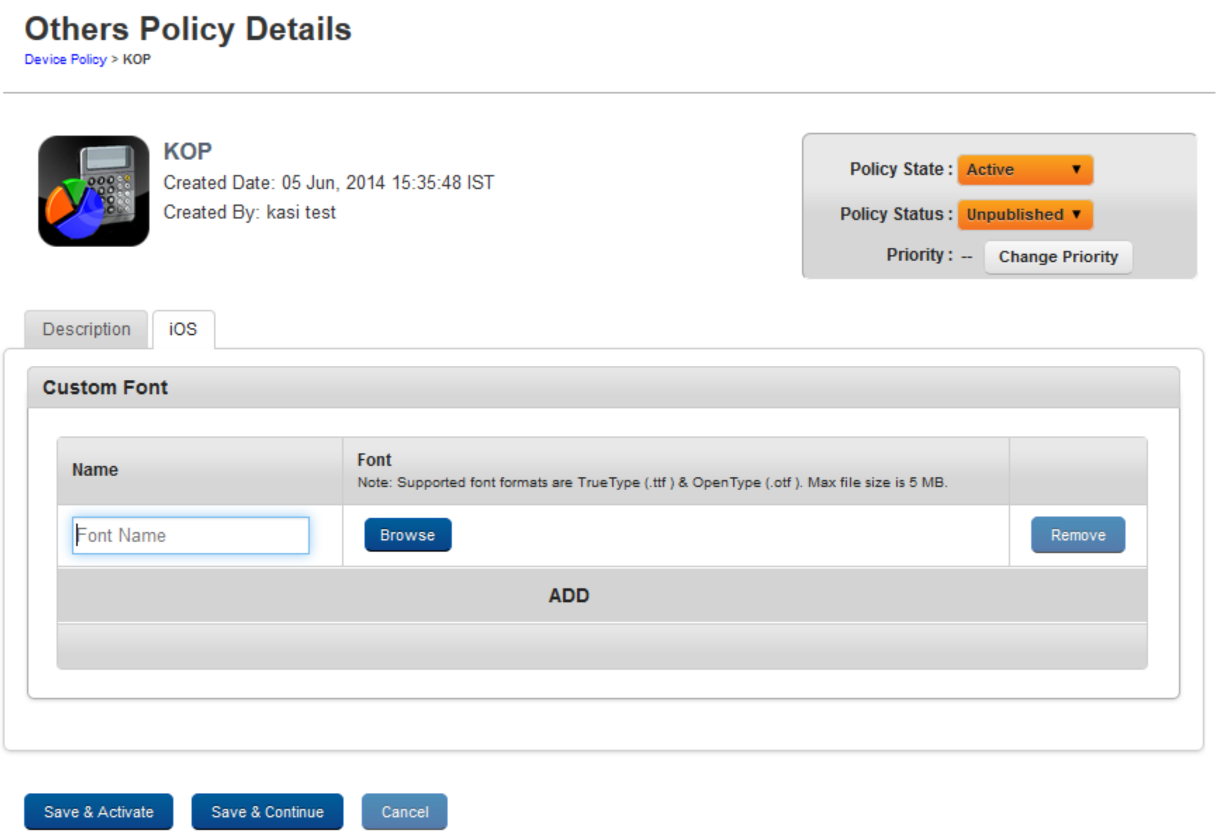
h. Scroll down to the Violation Message textbox, and enter a message. The message is displayed to users when an action in a Rule Definition is triggered.

i. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

j. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.
   Click the **Cancel** button to close the window.

10.4.10 Others Policy

The administrator can push fonts (.TTF or .OTF) files to iOS device. Once these fonts are configure on the device, the OS recognizes the fonts properly and supplies them to the app on the device.



Others Policy Details

Device Policy > KOP

KOP

Created Date: 05 Jun, 2014 15:35:48 IST

Created By: kasi test

Policy State : Active

Policy Status : Unpublished

Priority : --

Custom Font

Name	Font Note: Supported font formats are TrueType (.ttf) & OpenType (.otf). Max file size is 5 MB.	
Font Name	Browse	Remove

1. Click the **ADD** button to add new rows. You can remove added rows by clicking the **Remove** button.

2. In **Name**, enter a font name .

3. In **Font**, click the **Browse** button to navigate to your local folder and select the font file.

4. Click the **Save and Activate** button to save the data and exit the window. The updated policy details appear in the list view.

5. Click the **Save and Continue** button to stay on the same page and perform other updates on policy.

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

10.5 Devices

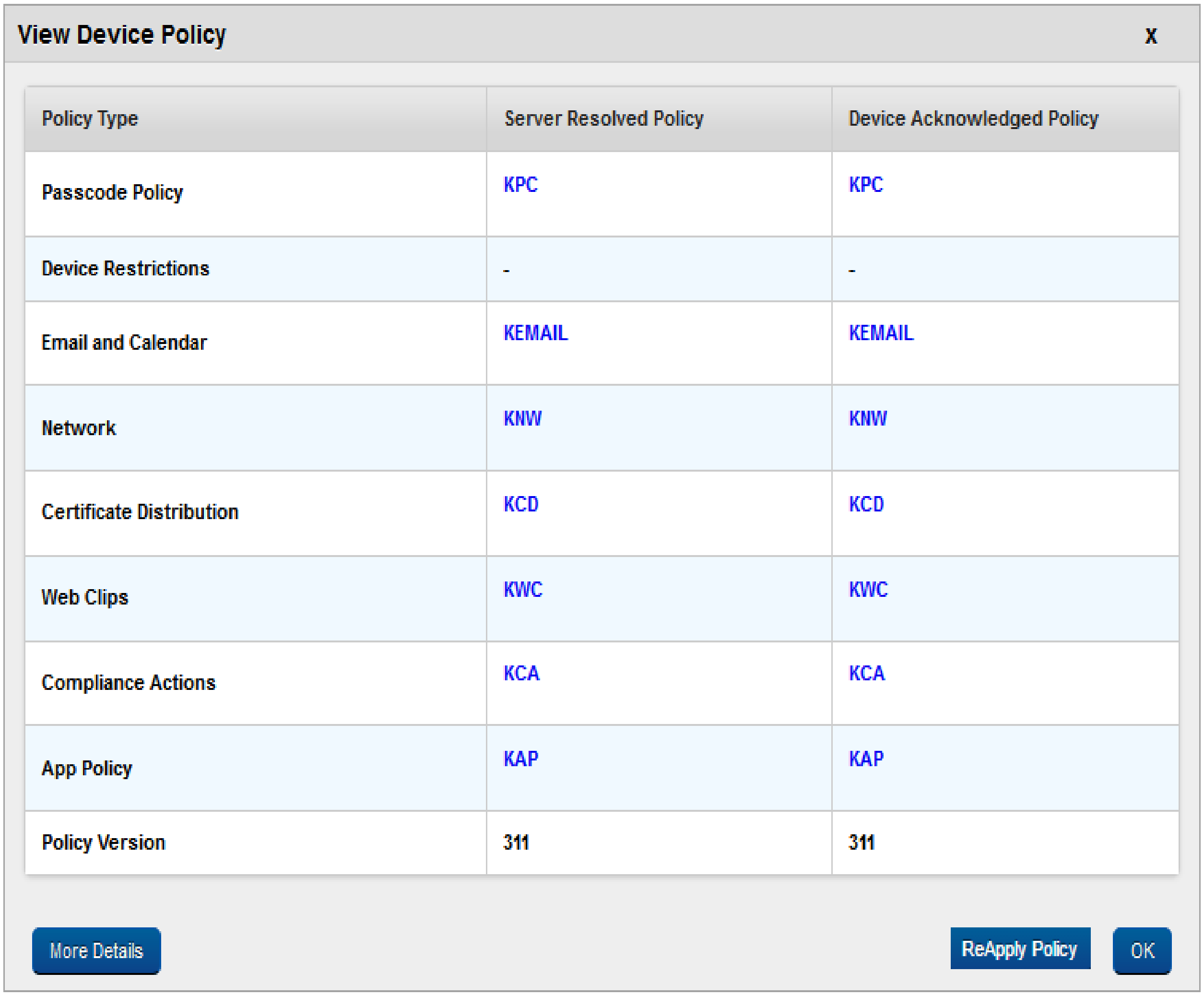
The primary purpose of Devices page is to provide all the information about devices and perform different activities to manage them efficiently.

From the **Device Management** section, click the **Devices** from the left panel. The Devices page appears with a list of the enrolled 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	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: • **Device name** • **IMEI** • **Serial number** • **SIM ID** You can also search for a device based on the device name, IMEI number, serial number, and SIM ID.

Columns	Description
Status	Displays the current status of the device. Devices Statuses are as follows: • **Enrolled:** The Device is registered with EMM Console. • **Deactivated:** The Device status is changed from active to inactive. • **Retired**: The Device has stopped working. • **Control Removed:** Enforced security policies are removed from the Device. • **Suspended**:The device is still enrolled and the EMM Server has full control over the device. • **Device Lost**: If a device cannot be recovered.
Device Owner	Displays the name of User with whom the Device is enrolled.
Ownership	Displays the ownership of the device. Options are Corporate, Employee, and Shared.
Compliance	Displays the compliance status of the device.
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.
Policy Applied	Click **View Policy** button to see applied policy details.



View Device Policy

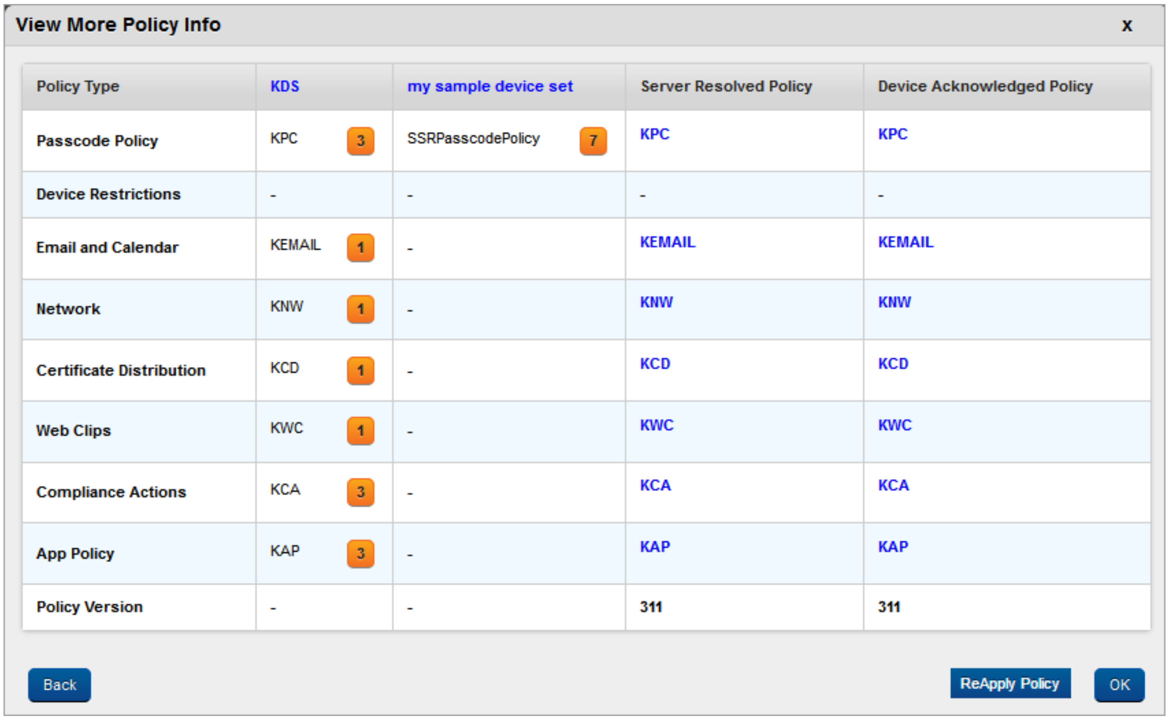
Policy Type	Server Resolved Policy	Device Acknowledged Policy
Passcode Policy	KPC	KPC
Device Restrictions	-	-
Email and Calendar	KEMAIL	KEMAIL
Network	KNW	KNW
Certificate Distribution	KCD	KCD
Web Clips	KWC	KWC
Compliance Actions	KCA	KCA
App Policy	KAP	KAP
Policy Version	311	311

1. Policy Applied: Click the **View Policy** button to see the applied policy details. **View Policy** window appears with the following column headers.

   The View displays the following columns:

Columns	Description
Policy Name	This column shows all the policy types that are applied to devices.
Server Resolved Policy	Server Resolved Policies are the latest policies that should be pushed to the device.
Device Acknowledged Policy	Based on the acknowledgment from the device, policies are displayed.

2. Click the **More Details** button to view the additional details.



View More Policy Info

Policy Type	KDS	my sample device set	Server Resolved Policy	Device Acknowledged Policy
Passcode Policy	KPC 3	SSRPasscodePolicy 7	KPC	KPC
Device Restrictions	-	-	-	-
Email and Calendar	KEMAIL 1	-	KEMAIL	KEMAIL
Network	KNW 1	-	KNW	KNW
Certificate Distribution	KCD 1	-	KCD	KCD
Web Clips	KWC 1	-	KWC	KWC
Compliance Actions	KCA 3	-	KCA	KCA
App Policy	KAP 3	-	KAP	KAP
Policy Version	-	-	311	311

The **View More Policy** Info window appears with complete details of the policy.

3. Click **ReApply Policy** to apply the policy again on the device.

4. Click the **OK** button to close the window.

Important: When the server resolved policy and the device acknowledged policy are different, a red flag will appear next to the policy name in the Server Resolved Policy column. The policies might differ if the Server Resolved policy is modified and those modifications are yet to be applied on the device (the device is offline or not reachable by the server). The red flag will disappear when the device comes online and acknowledges the policy.

Important: If Admin initiates wipe and if the device is offline, then the status of the device is first moved to suspended and once the device comes online, changes the status to deactivated. Even for online devices, the deactivated status for device moves to suspended state first followed by Deactivated. However, it may not be noticed because it happens with in no time.

10.5.1 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.
- **Retired**: The device is not enrolled to EMM. It is recommended to use the status if you do not want this device to be enrolled again.
- **Suspended**:The device is still enrolled and the EMM Server has full control over the device. This is the default status the device goes into when it is enterprise wiped through compliance actions. While doing a manual enterprise wipe, this status is chosen if the admin still wants to retain control over the device. To bring the device out of suspension, the admin can invoke the **Resume** action. For more details, refer to Resume Device.
- **Device Lost**: The device is not enrolled to EMM. It is recommended to use this status if a device is lost and cannot be recovered. Typically one would mark the device *"No"* for allow future enrollment.

- **Control Removed:** This status occurs when control over the device is manually removed by the user.
    - **iOS:** In iOS this status is set if the user removes all profiles. When a device goes into Control Removed status, all policies and apps are automatically removed.
    - **Android:** In Android this status is set if the Admin privileges are revoked for enterprise store. All policies are automatically removed and the user is prompted to remove all managed apps including enterprise apps. In case the user deletes enterprise store before all apps are deleted, an email is sent to the admin with the list of apps still present on the device at the time of enterprise store deletion.

    > ***Note:*** To re-enroll a control removed device, enterprise store must be deleted and the enrollment process should be performed again.
    >
    > If the device is control removed, and enterprise store app data is removed, and then you try to re-enroll same app, this may result in unexpected behavior. It is recommended that you delete enterprise store app before trying to re-enroll into EMM.

    In case of SAFE even if control is removed, SAFE licenses and polices are still active on the device. The user must delete enterprise store also to remove the SAFE license on the device. Even after this is done, some settings still reside on the device such as:

    - SAFE email policy
    - APN Settings

10.5.2 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?

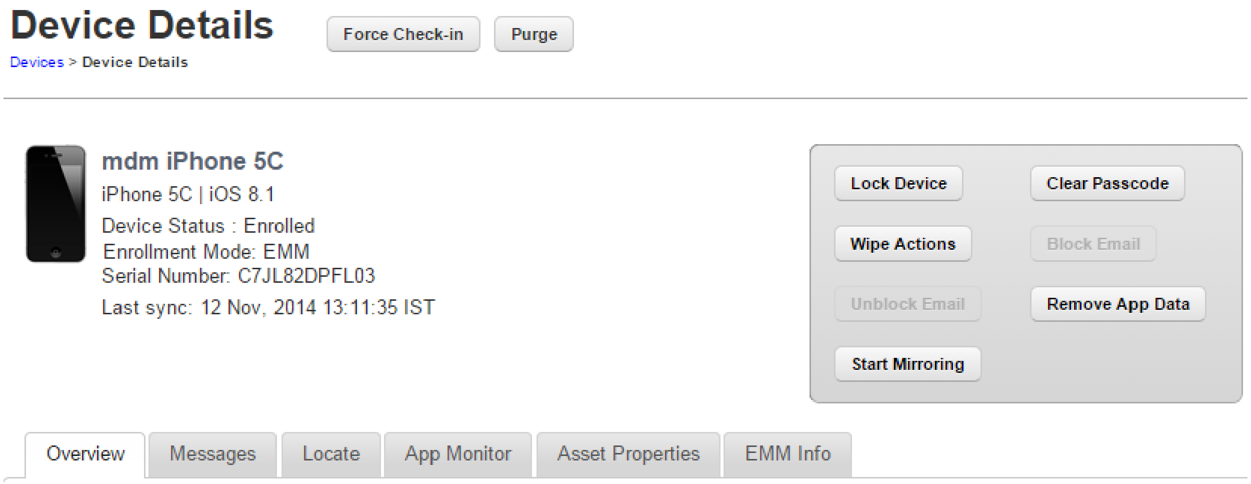
3. Click **Yes** to confirm. The selected entry removed.

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**.

10.6 Device Details

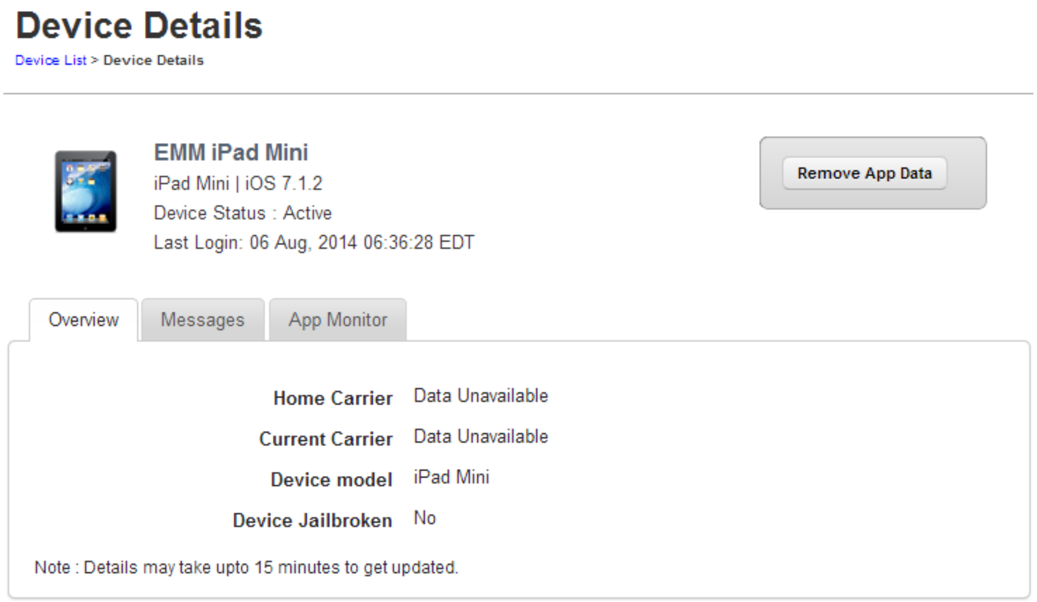
The primary purpose of the Device Details page is to display complete information of a device and manage the device through various actions available.



Device Details

Devices > Device Details

mdm iPhone 5C
iPhone 5C | iOS 8.1
Device Status : Enrolled
Enrollment Mode: EMM
Serial Number: C7JL82DPFL03
Last sync: 12 Nov, 2014 13:11:35 IST



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

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.

Screen Element Properties	Description
Page Title	This is available on extreme right corner on top of the screen, for example, Device Details.
Navigation Link	This link navigates you to main page, for example, click Device List > Device Details link to navigate to Device List main page.
Device Name	Displays the unique identification name of the device.
Device Status	Displays the current status of the device, for example enrolled.
Enrollment Mode	Displays the enrollment mode of the device.
Serial Number	Displays the unique serial number of the device.
Last Sync	Displays the date and time when the device was last synced with the server.

> ***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

10.6.1 Device Details Page Tabs

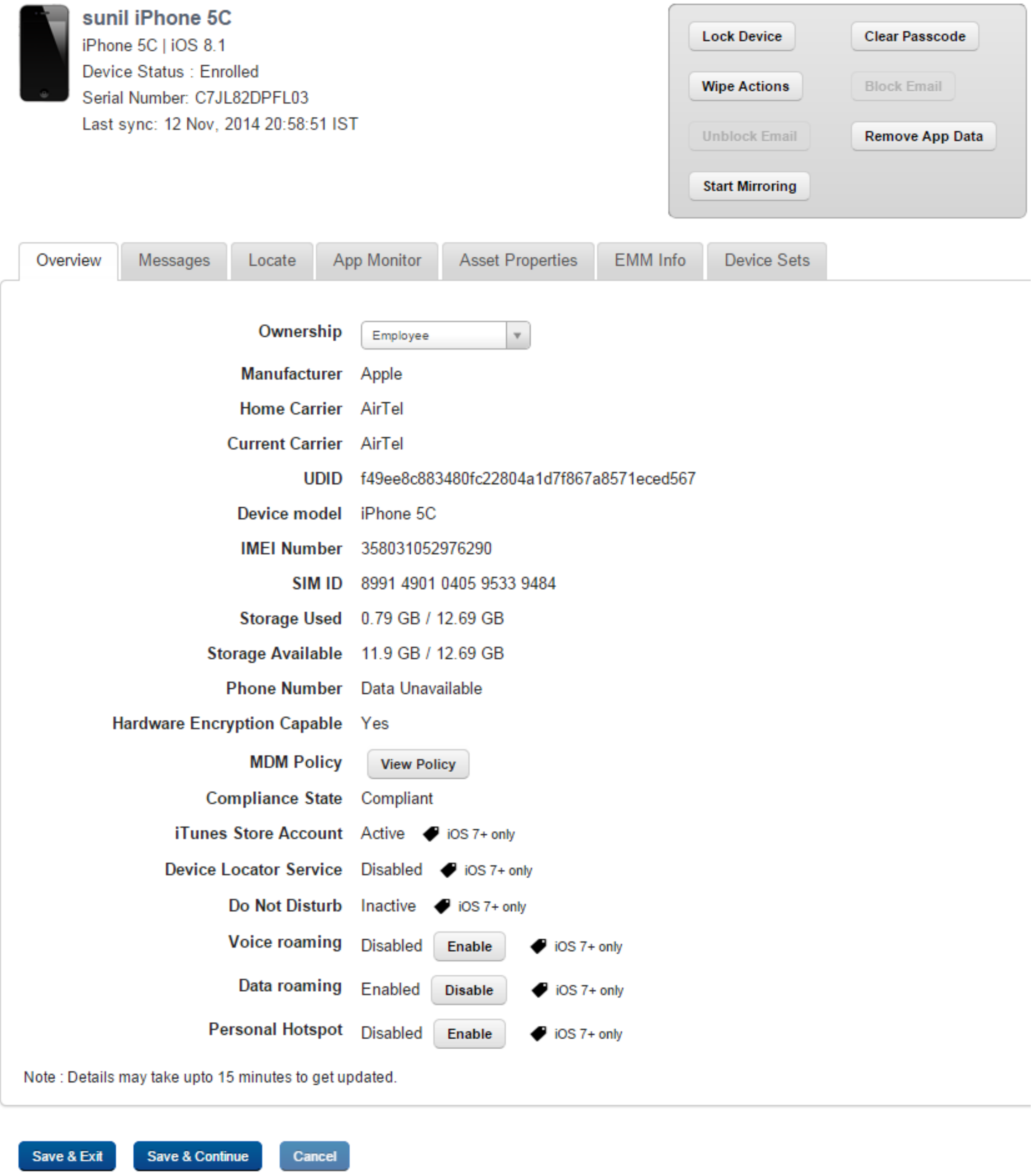
Device details page displays the following tabs:

- Overview
- Messages
- Locate
- App Monitor
- Asset Properties
- EMM Info
- Device Sets

10.6.1.1 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



sunil iPhone 5C
iPhone 5C | iOS 8.1
Device Status : Enrolled
Serial Number: C7JL82DPFL03
Last sync: 12 Nov, 2014 20:58:51 IST

Ownership	Employee
Manufacturer	Apple
Home Carrier	AirTel
Current Carrier	AirTel
UDID	f49ee8c883480fc22804a1d7f867a8571eced567
Device model	iPhone 5C
IMEI Number	358031052976290
SIM ID	8991 4901 0405 9533 9484
Storage Used	0.79 GB / 12.69 GB
Storage Available	11.9 GB / 12.69 GB
Phone Number	Data Unavailable
Hardware Encryption Capable	Yes
MDM Policy	View Policy
Compliance State	Compliant
iTunes Store Account	Active iOS 7+ only
Device Locator Service	Disabled iOS 7+ only
Do Not Disturb	Inactive iOS 7+ only
Voice roaming	Disabled Enable iOS 7+ only
Data roaming	Enabled Disable iOS 7+ only
Personal Hotspot	Disabled Enable iOS 7+ only

Note : Details may take upto 15 minutes to get updated.

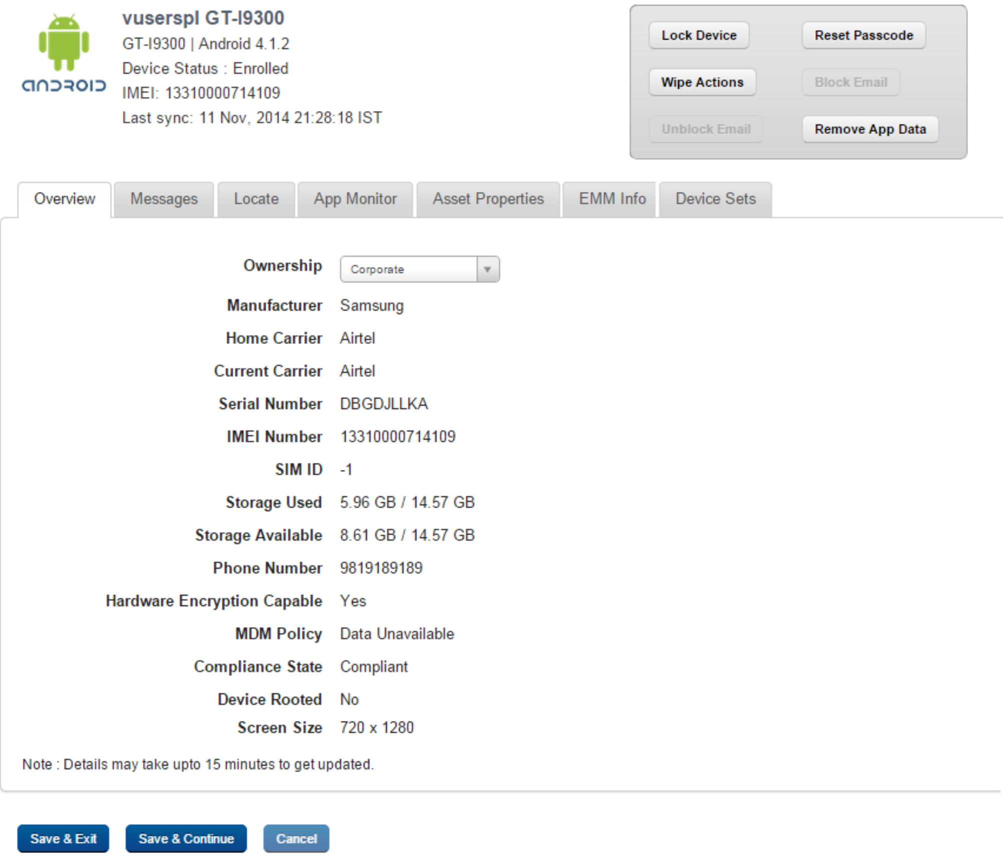
- **Compliance State**: Displays compliance state of the device.

> *Note:* In case of conditional compliance (or both policy and rule), the system displays the policy name and rule name. For example <policy name:rule name>.
>
> In case of simple compliance, the system displays the compliance status.
> For example, <Non Compliant (Min OS Version)>

- **iTunes Store Account Active**: Displays whether an iTunes Store Account is Active.
- **Device Locator service**: Display whether Device Locator service is enabled.
- **Do Not Disturb**: Displays whether Do Not Disturb is in effect.
- **Voice Roaming**: Displays whether Voice Roaming is enabled.

  If you enable Data Roaming, the Voice Roaming is enabled automatically.
- **Data Roaming**: Displays whether Data Roaming is enabled. You can modify it to Disable.
- **Personal Hotspot**: Displays whether Personal Hotspot Enabled. You can modify it to Disable.
- **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.

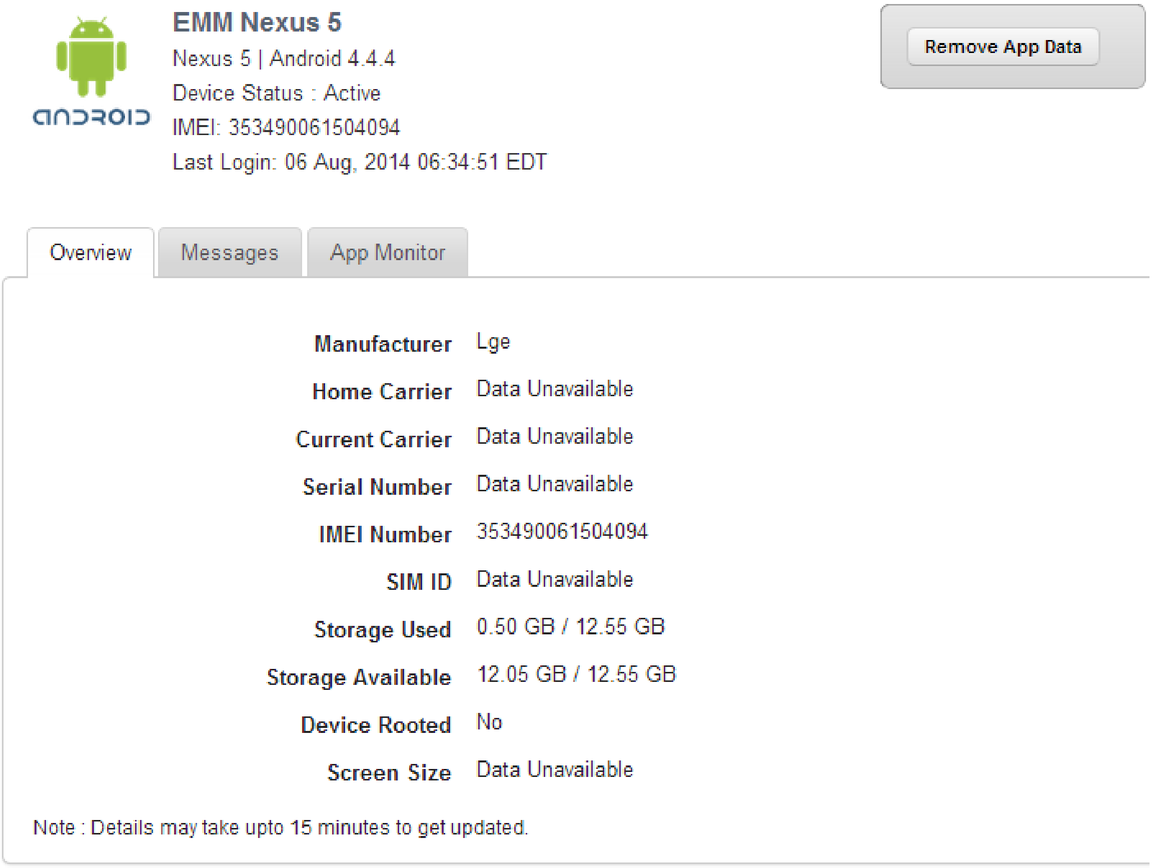
Overview for Android



vuserspl GT-I9300
GT-I9300 | Android 4.1.2
Device Status : Enrolled
IMEI: 13310000714109
Last sync: 11 Nov, 2014 21:28:18 IST

Ownership	Corporate
Manufacturer	Samsung
Home Carrier	Airtel
Current Carrier	Airtel
Serial Number	DBGDJLLKA
IMEI Number	13310000714109
SIM ID	-1
Storage Used	5.96 GB / 14.57 GB
Storage Available	8.61 GB / 14.57 GB
Phone Number	9819189189
Hardware Encryption Capable	Yes
MDM Policy	Data Unavailable
Compliance State	Compliant
Device Rooted	No
Screen Size	720 x 1280

Note : Details may take upto 15 minutes to get updated.



EMM Nexus 5
Nexus 5 | Android 4.4.4
Device Status : Active
IMEI: 353490061504094
Last Login: 06 Aug, 2014 06:34:51 EDT

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.

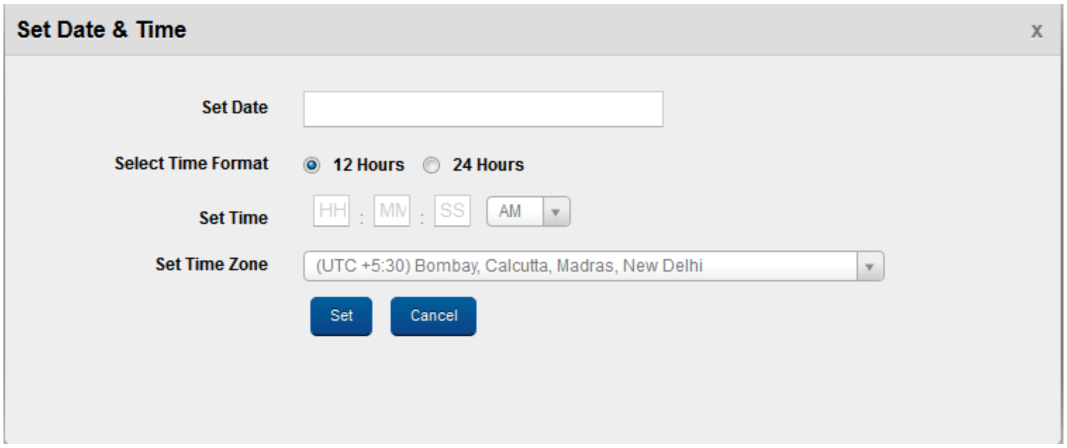
Manufacturer:

- **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 Date & Time**: Displays date and time of the device.
  Date: Displays date of the device.
  Time: Displays time in HH/MM/SS format (12 hour or 24 hour set on device)
  Timezone: Displays timezone of the device.

  The Admin can modify the date and time settings if permissions are granted in the Device Restrictions policy.

  a. Click the **Modify** button if you wish to change the settings.



Set Date & Time

Set Date

Select Time Format ● 12 Hours ○ 24 Hours

Set Time HH : MM : SS AM

Set Time Zone (UTC +5:30) Bombay, Calcutta, Madras, New Delhi

  b. In the **Set Date & Time** dialog, enter the details and click **Set**.

- **Compliance State**: Displays compliance state of the device.

> ***Note:*** In case of conditional compliance (or both policy and rule), the system displays the policy name and rule name. For example <policy name:rule name>.
>
> In case of simple compliance, the system displays the compliance status.
> For example, <Non Compliant (Min OS Version)>

- **Device Rooted**: Displays whether device root access is enabled.

- **Screen Size**: Displays the screen size of the device.

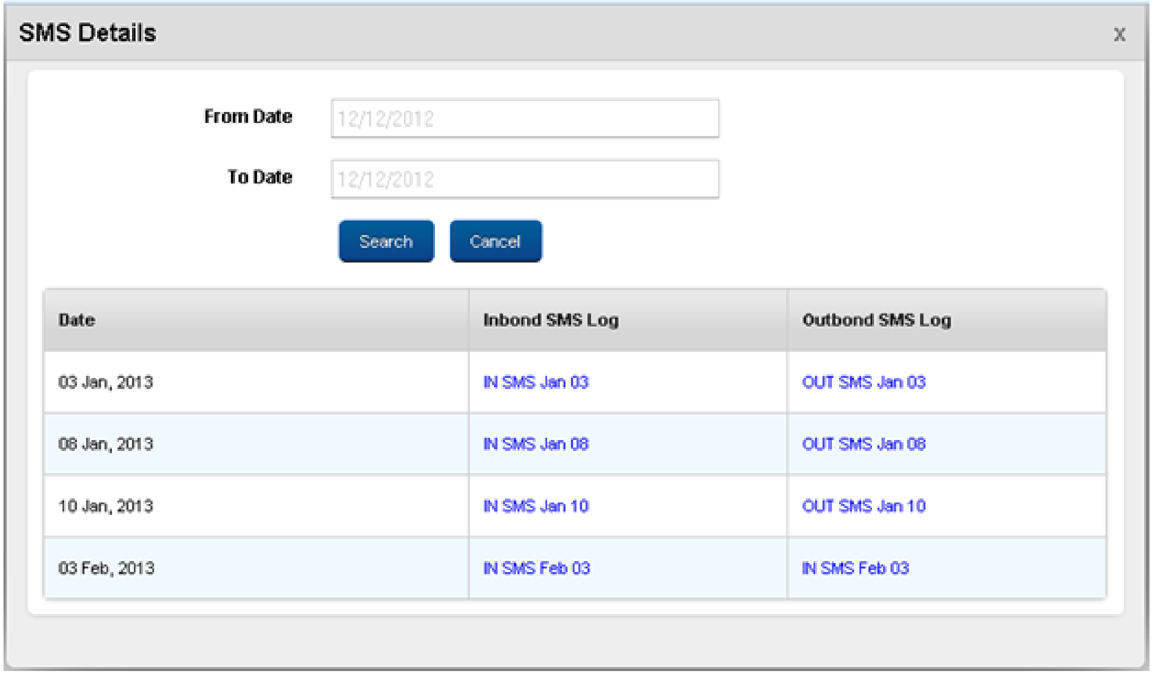
- Certificates (Android SAFE): Displays certificates installed on the device.
  The administrator can remove all of these certificates if required. When the administrator attempts to delete certificates, the system displays a confirmation message "*Do you want to remove all certificates from the credential store?*"
  Click **Yes** to confirm to delete certificates.

- **Block MMS with Storage(Android SAFE)**
  When MMS is blocked, all the MMSes received are stored on the device, but not shown to the User. The administrator can choose to Unblock MMS by clicking the same. Once unblocked, the MMSes are delivered to the User.

- **Block SMS with Storage (Android SAFE)**
  When SMS is blocked, all the SMSs received by the device are stored on the device but not shown to the User. The Admin can choose to Unblock SMS by invoking the same. Once unblocked, the stored SMSs are delivered to the device.

  The Admin can also choose to clear the stored SMS messages by click on the Clear Stored SMS button. If cleared stored SMSs, the SMSs are never delivered. This may need to be done if a device is non-compliant and the Block Action was taken. But the device then must be deactivated. Then instead of delivering the SMSs, the admin choose to clear them.

- **Calls and SMS Stats Capture (Android SAFE)**



From Date 12/12/2012

To Date 12/12/2012

Date	Inbond SMS Log	Outbond SMS Log
03 Jan, 2013	IN SMS Jan 03	OUT SMS Jan 03
08 Jan, 2013	IN SMS Jan 08	OUT SMS Jan 08
10 Jan, 2013	IN SMS Jan 10	OUT SMS Jan 10
03 Feb, 2013	IN SMS Feb 03	IN SMS Feb 03

Through Restrictions Policy, both Calls and SMS stats capture can be enabled. This allows the Admin to get logs of all Call and SMS data.

Daily logs are maintained separately for Incoming and Outgoing Calls and SMSes. The Admin can access these from the Device Overview. These logs are stored in .CSV format. They can be downloaded when the User clicks to see Details. The Admin can specify the date range for which to show logs and all the logs are shown.

The max limit of logs allowed per device is 1 MB. If the logs go above that, they are automatically purged in a first in first out manner.

- **Reset SMS Count (Android SAFE)**
  This resets the number of SMS to 0. User can send SMSes again until they reach the limit as specified in the Device Restrictions policy.

- **Reset Calls Count (Android SAFE)**
  This resets the number of Calls to 0 (zero). User can send Calls again until they reach the limit as specified in the Device Restrictions policy.

- Click the **Save and Exit** button. In the confirmation message that appears, click OK to return to the device list page.

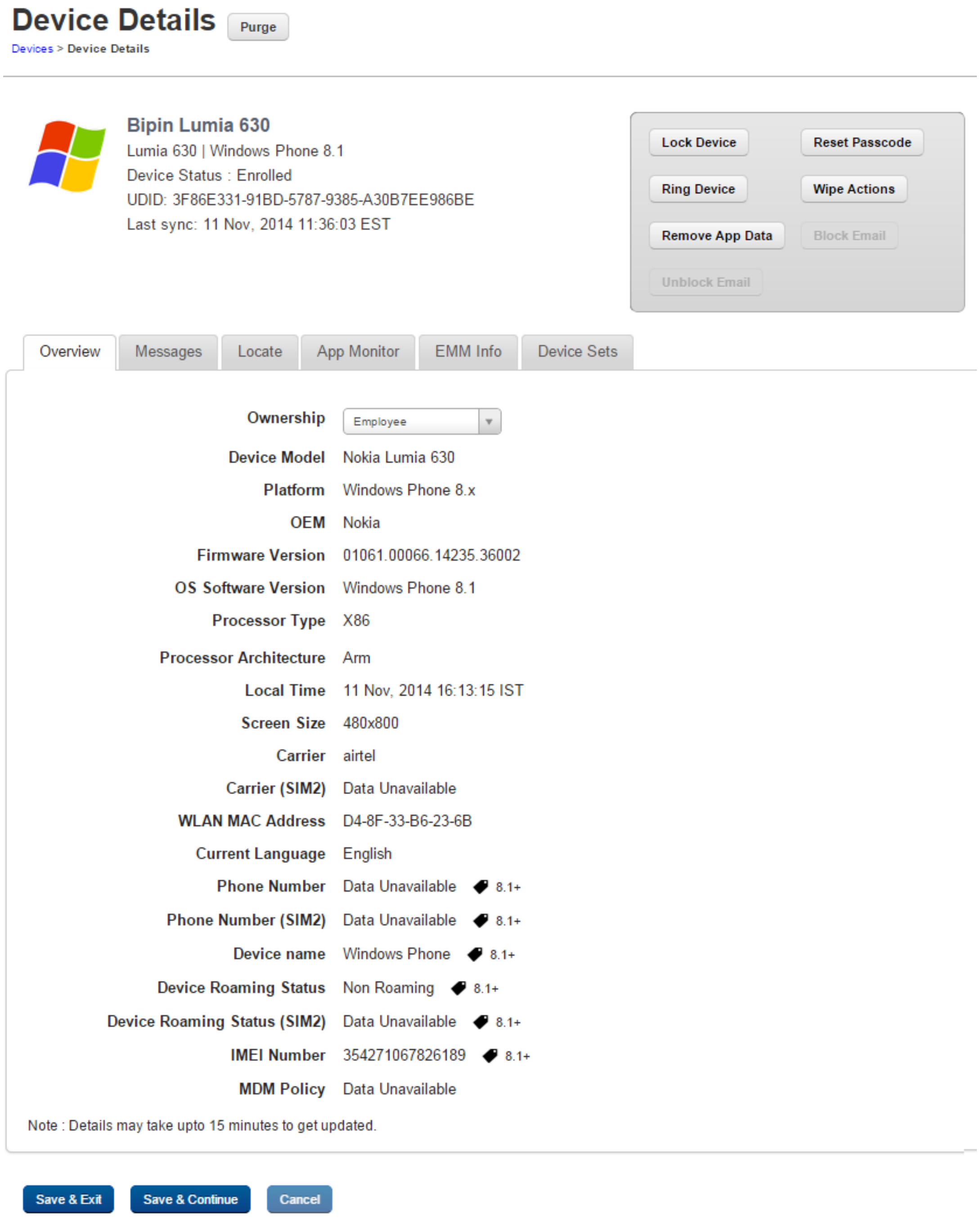
  OR

  To remain on the same page to do other changes immediately, click the **Save and Continue** button.In the confirmation message that appears, click OK to continue.

- Click the **MDM Policy** button to view the policies applied to the device.For more details, refer Device List

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

Overview - Windows Phone 8.x



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

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

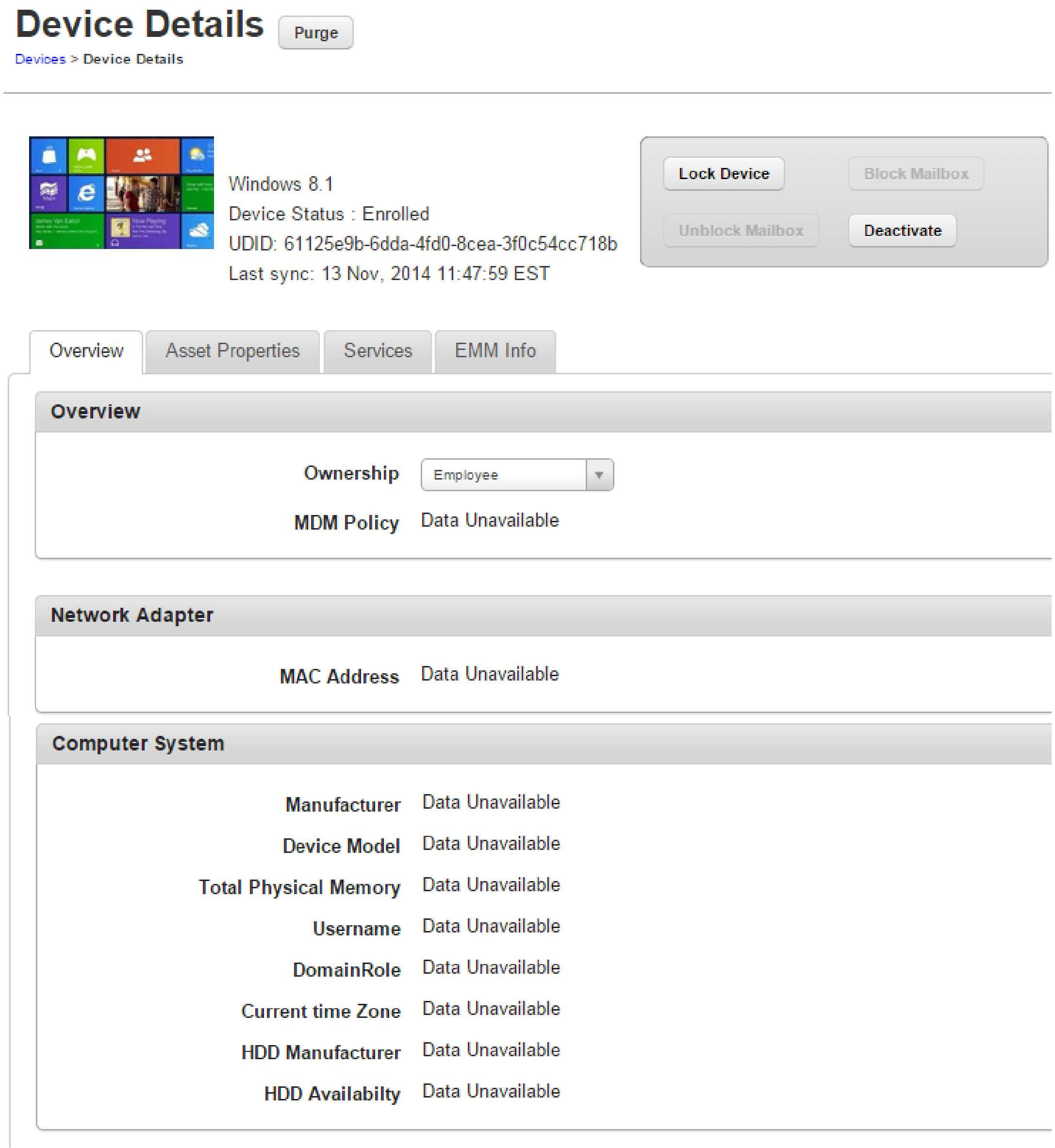
Note : Details may take upto 15 minutes to get updated.

Overview:

- **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.

Overview - Windows 8.1



Device Details

Windows 8.1
Device Status : Enrolled
UDID: 61125e9b-6dda-4fd0-8cea-3f0c54cc718b
Last sync: 13 Nov, 2014 11:47:59 EST

Overview

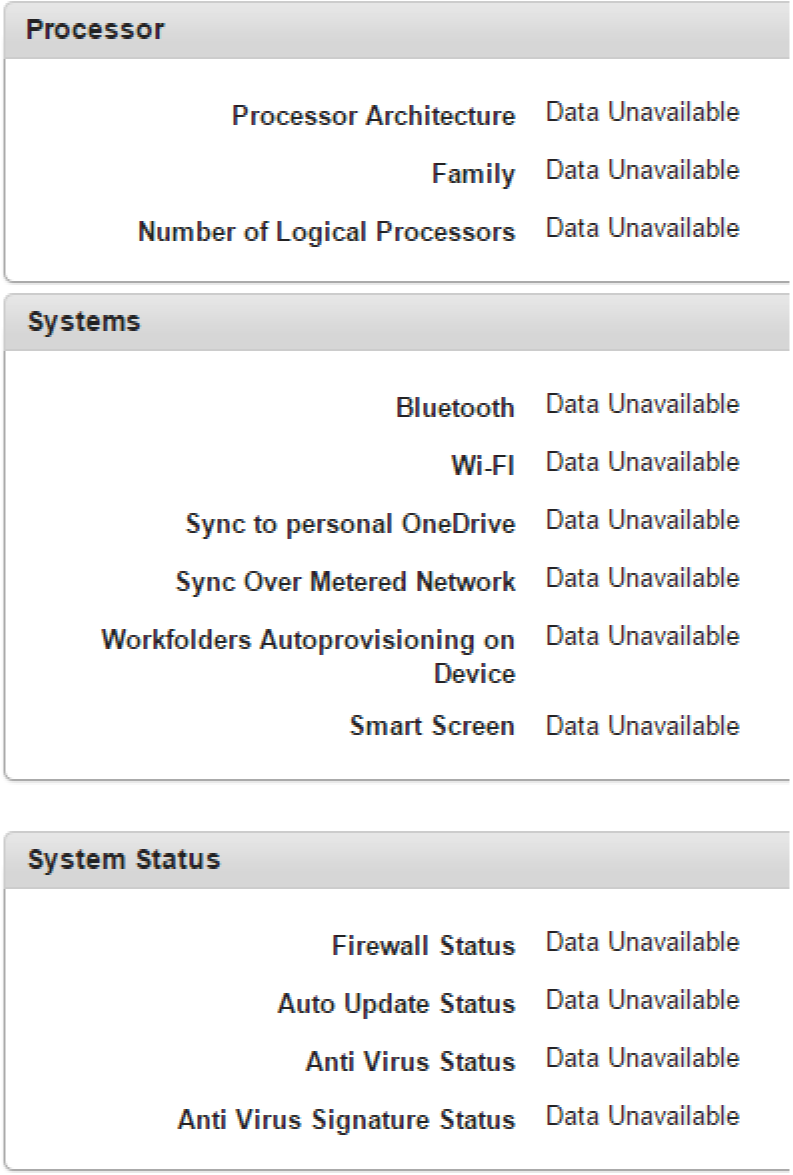
Ownership	Employee
MDM Policy	Data Unavailable

Network Adapter

MAC Address	Data Unavailable

Computer System

Manufacturer	Data Unavailable
Device Model	Data Unavailable
Total Physical Memory	Data Unavailable
Username	Data Unavailable
DomainRole	Data Unavailable
Current time Zone	Data Unavailable
HDD Manufacturer	Data Unavailable
HDD Availabilty	Data Unavailable



Processor

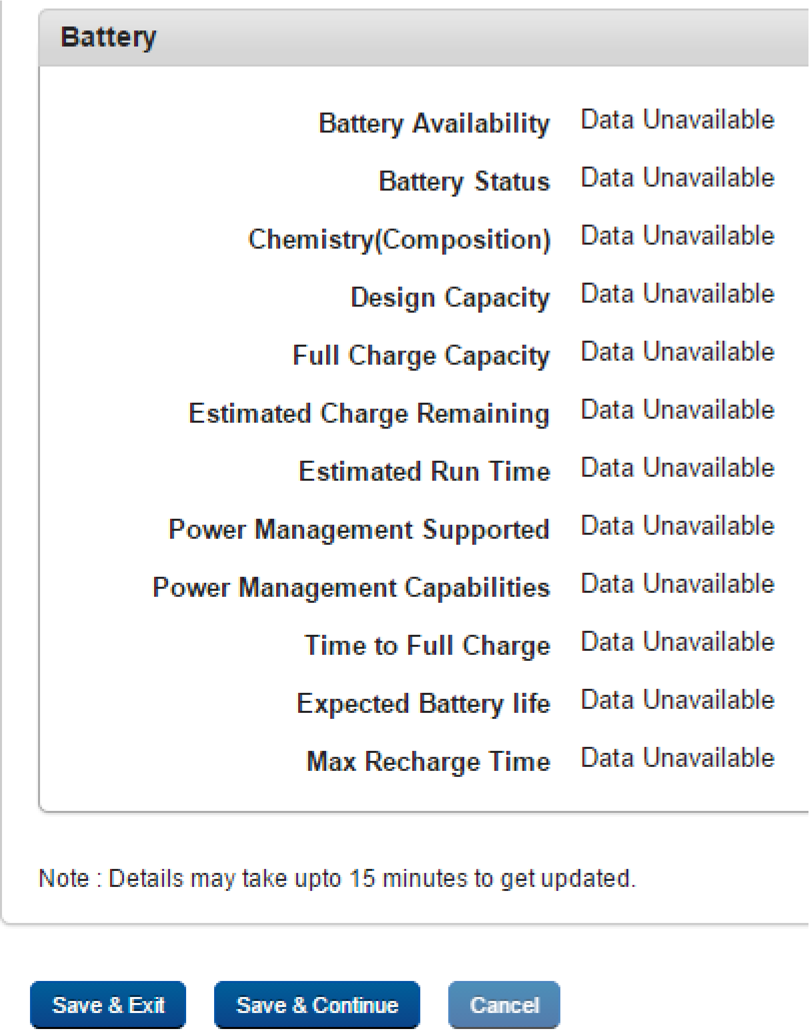
Processor Architecture	Data Unavailable
Family	Data Unavailable
Number of Logical Processors	Data Unavailable

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.

- **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.

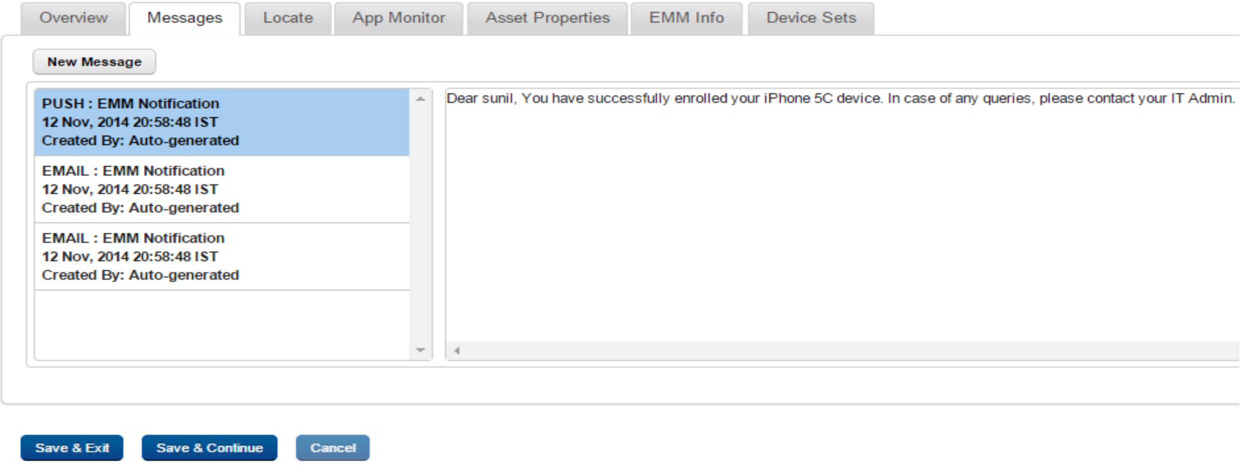
- **Username**: Displays username of the device user.
- **DomainRole**: Displays details of domain role of the device.
- **Current time Zone**: Displays the local time zone details of the device.
- **HDD Manufacturer**: Displays details of the HDD manufacturer.
- **HDD Availability**: Displays details 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 synched 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.

10.6.1.2 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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

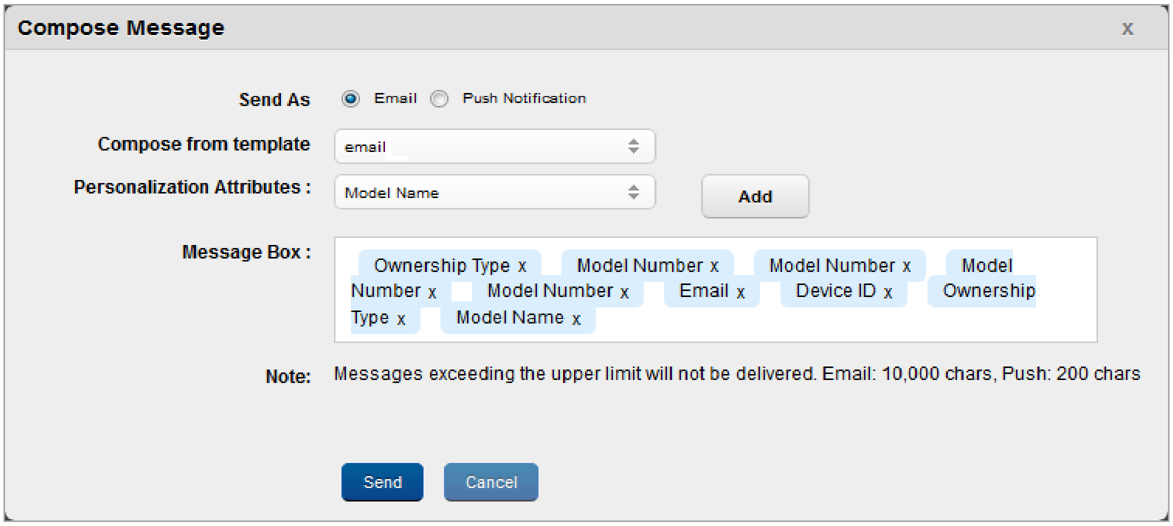
EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

To compose a message, follow these steps:

1. Click the **New Message** button to open the **Compose Message** window. Enter the following details:



Send As ● Email ○ Push Notification

Compose from template: email

Personalization Attributes : Model Name

Message Box : Ownership Type x Model Number x Model Number x Model Number x Model Number x Email x Device ID x Model Ownership Type x Model Name x

Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

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.

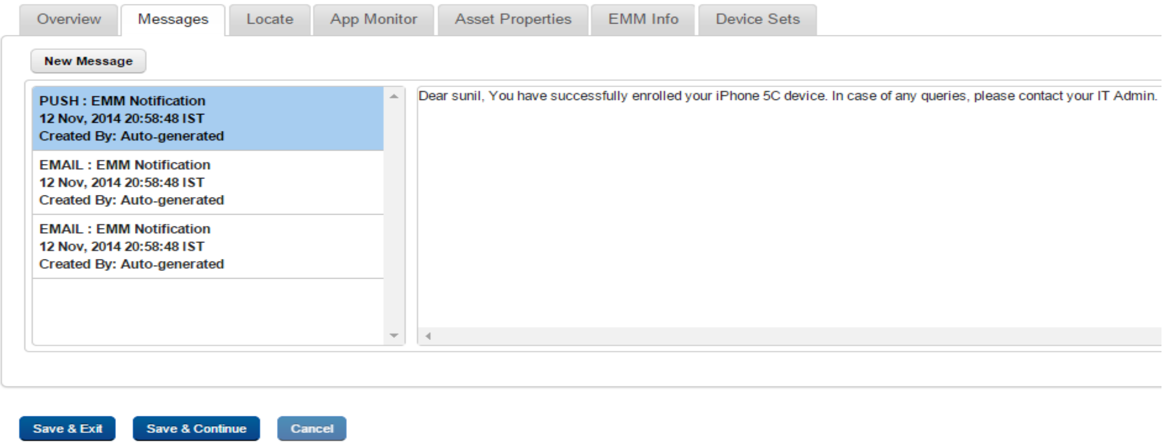
   To automate the work-flow process, you create message templates under Device Settings > Message Templates section. You can access these messages in Compose Message window through Compose from Template dropdown list.

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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

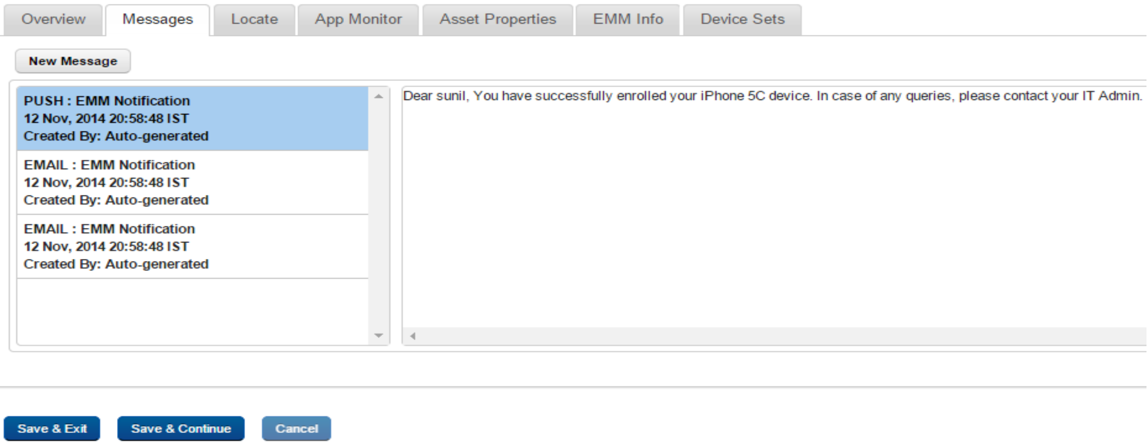
The message appears in the message window

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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

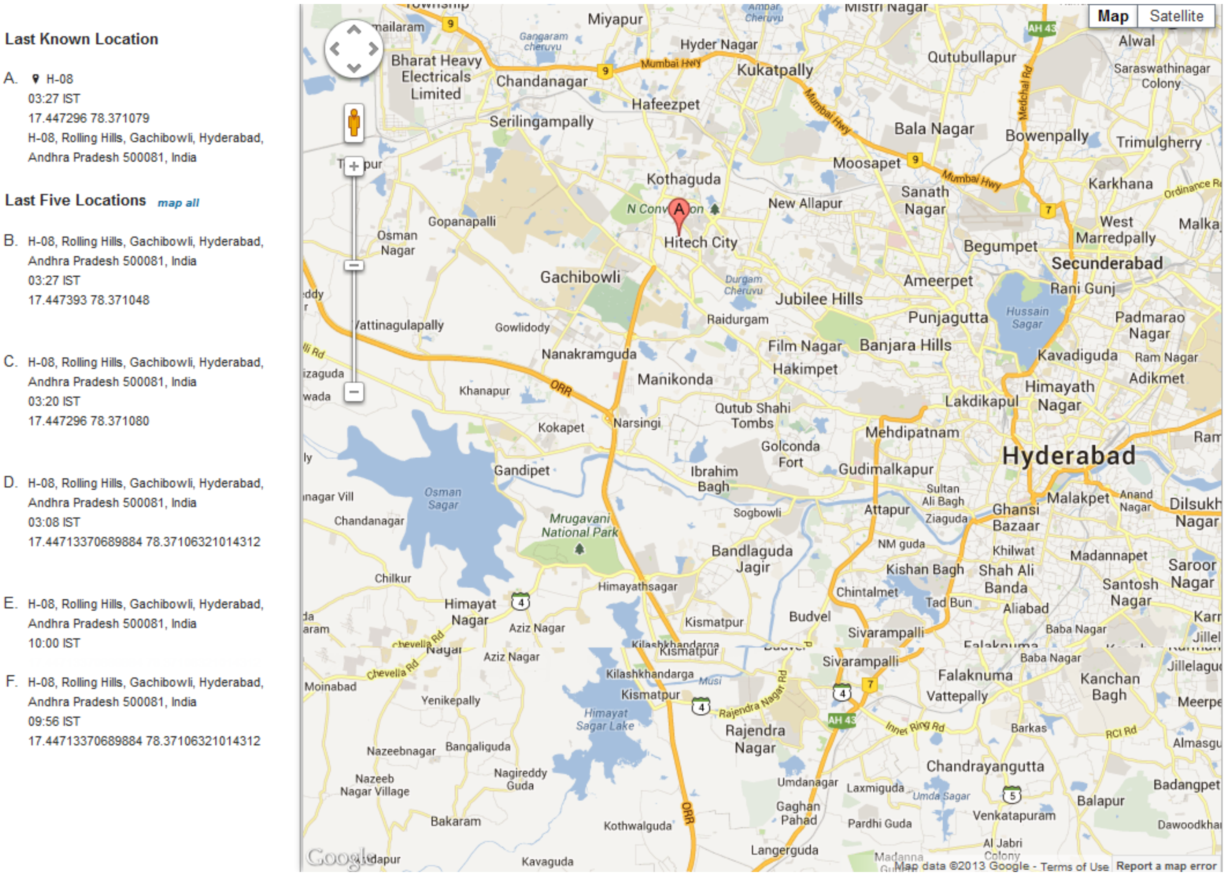
Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

The message appears in the message window.

10.6.1.3 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.

10.6.1.4 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 three types of Apps.

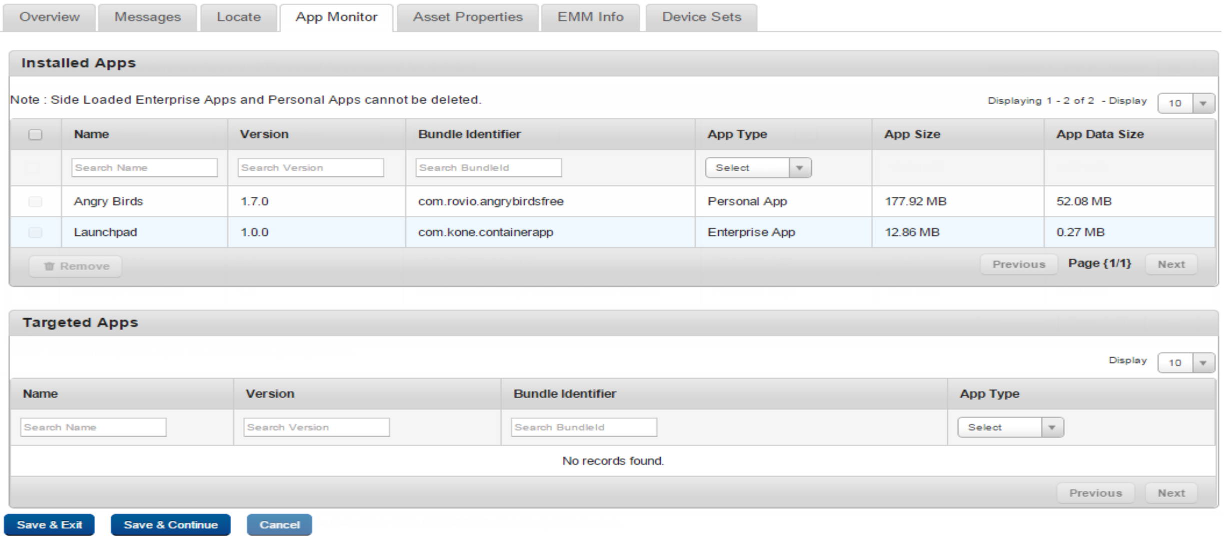
- Enterprise Applications: Apps which are published into Enterprise Store are known as Enterprise Apps. These can be deleted by the Administrator, if they are downloaded through the Enterprise Store. They cannot be deleted in iOS devices if they are side-loaded.

- Personal Applications: Apps which are downloaded through Public Apps store like Apple App Store or Google App Store are considered as Personal Apps. If Whitelisted apps are installed by a User from the Apple App Store or Google Play, they are considered as Personal apps as they are not pushed by the EMM Server. These apps cannot be deleted.

- Managed Apps: Public Apps pushed through EMM are considered as Managed Apps. They can be deleted.

For Windows 6.x devices, none of the apps can be removed remotely.

App Monitor for iOS



Installed Apps

Note : Side Loaded Enterprise Apps and Personal Apps cannot be deleted.

Displaying 1 - 2 of 2 - Display 10

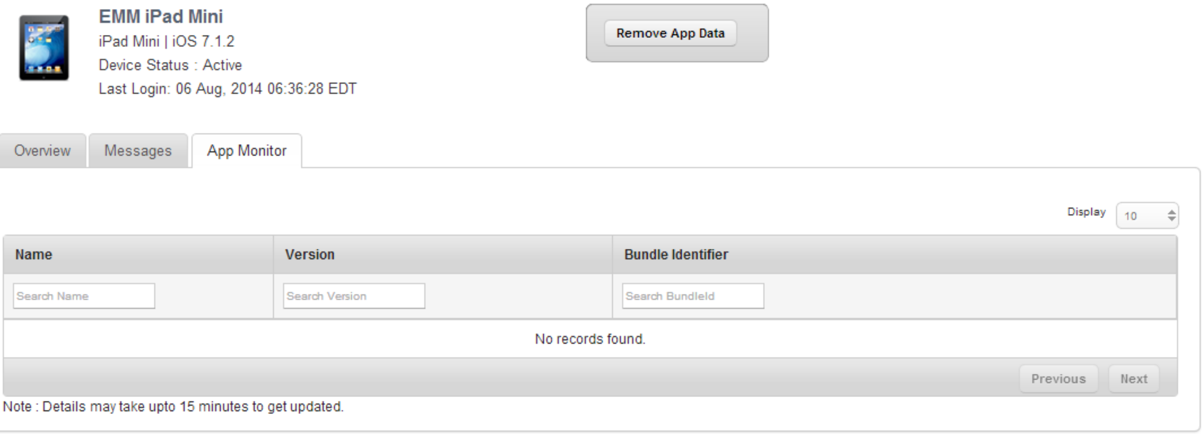
□	Name	Version	Bundle Identifier	App Type	App Size	App Data Size
	Search Name	Search Version	Search BundleId	Select		
□	Angry Birds	1.7.0	com.rovio.angrybirdsfree	Personal App	177.92 MB	52.08 MB
□	Launchpad	1.0.0	com.kone.containerapp	Enterprise App	12.86 MB	0.27 MB

Targeted Apps

Display 10

Name	Version	Bundle Identifier	App Type
Search Name	Search Version	Search BundleId	Select

No records found.


EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Display 10

Name	Version	Bundle Identifier
Search Name	Search Version	Search BundleId

No records found.

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for iOS has the following details:

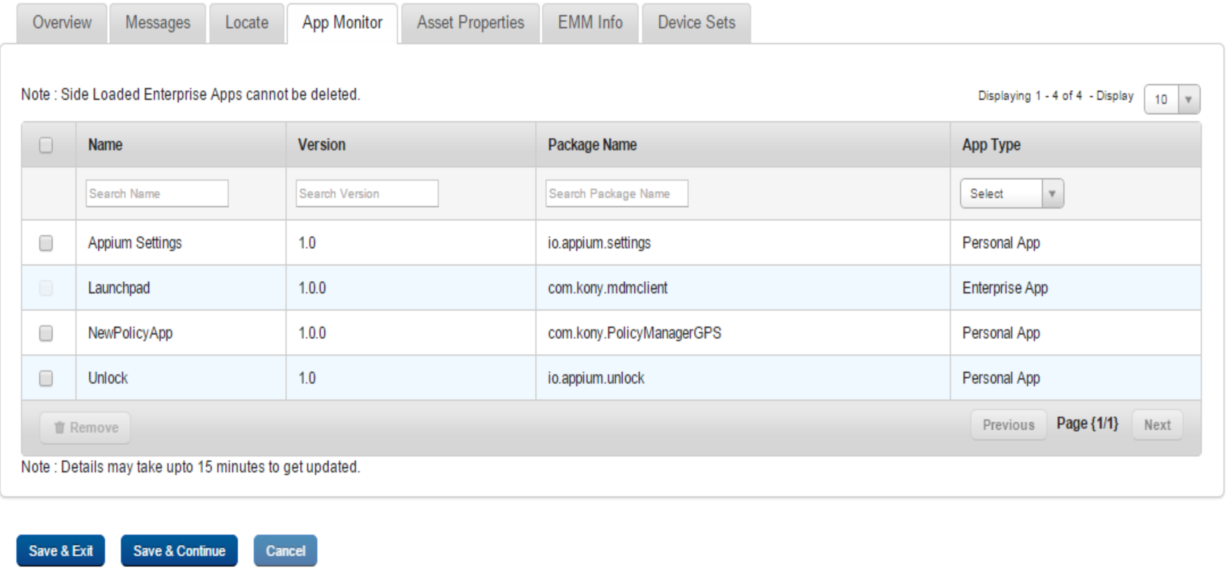
- **Name**: Displays the Name of the application.
- **Version**: Displays the Version of the application.
- **Bundle Identifier**: Displays the bundle ID of the application.

> ***Note:*** In the App Monitor tab for iOS, Publisher has been replaced with Bundle Identifier.

- **App Type**: Displays the type of the application.
- **App Size**: Displays the size of the installed application.
- **App Data Size**: Displays the size of the data in the application.

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.

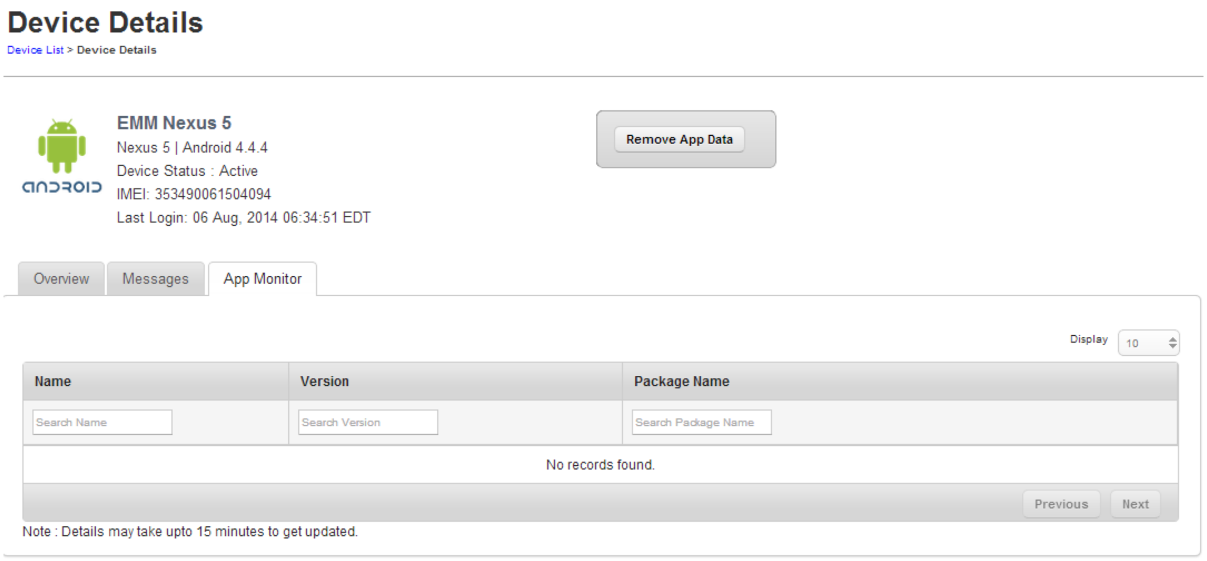


Note : Side Loaded Enterprise Apps cannot be deleted.

Displaying 1 - 4 of 4 - Display 10

□	Name	Version	Package Name	App Type
	Search Name	Search Version	Search Package Name	Select
□	Appium Settings	1.0	io.appium.settings	Personal App
□	Launchpad	1.0.0	com.kony.mdmclient	Enterprise App
□	NewPolicyApp	1.0.0	com.kony.PolicyManagerGPS	Personal App
□	Unlock	1.0	io.appium.unlock	Personal App

Note : Details may take upto 15 minutes to get updated.



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

Name	Version	Package Name
No records found.		

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.

   > ***Note:*** In the App Monitor tab for Android, Publisher has been replaced with Package Name.

4. **App Type**: Displays the type of the application.
5. **App Status**:Displays the status of the application.
6. **App Running**: Displays whether the application is running or not running. The administrator can change App Running status remotely.
7. **App Uninstallation Mode**: Displays whether the uninstallation of the application is allowed or not on the device.
8. **Actions**: An administrator can perform additional tasks available in the drop-down list.

Based on several combinations with App Status, App Running, and App Uninstallation Mode, the actions are shown in the **Actions** drop-down list.

- If App Status is Enabled, the system displays available action as Disable App in the **Actions**. An administrator can disable or enable the app.
- If an app running is running, an administrator can stop the app by selecting the Stop App in the **Actions** drop-down list. An administrator can start or stop an app based on the running status.
- If an app is Not Allowed for uninstallation, an administrator can allow user to uninstall the app by selecting the Allow Uninstallation in the **Actions** drop-down list. An administrator can allow or deny user to uninstall an app based on the uninstallation mode status.

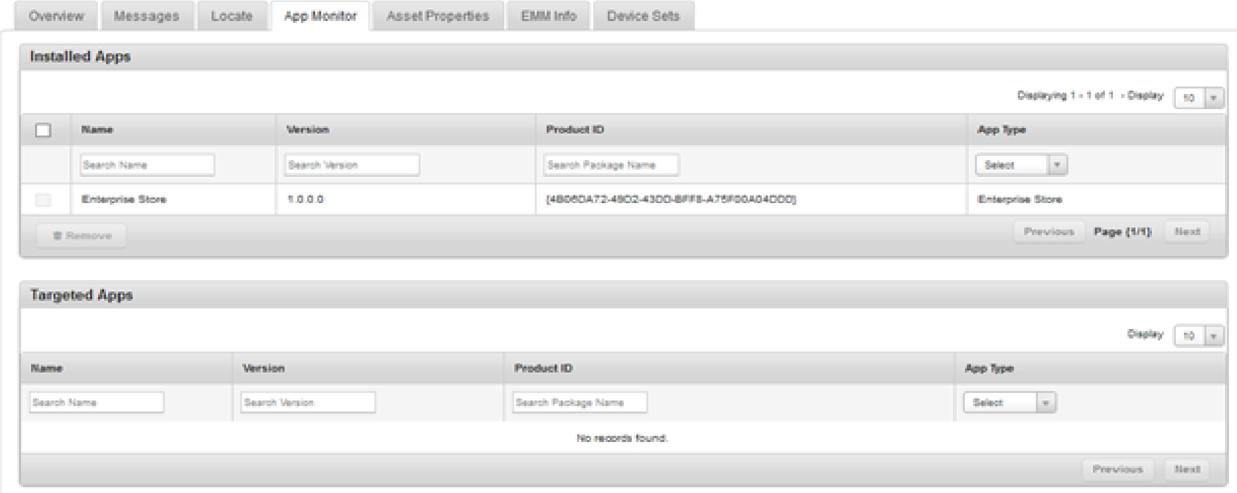
The following table shows the list of actions present with different possible conditions.

If			Then, the system displays the following actions
App Status	App Running	App Uninstallation Mode	
Enabled	Yes	Allowed	• Disable App • Stop App • Disallow Uninstallation
Enabled	No	Not Allowed	• Disable App • Start App • Allow Uninstallation

If			Then, the system displays the following actions
App Status	App Running	App Uninstallation Mode	
Disabled	No	Allowed	• Enable App • Disallow Uninstallation
Disabled	No	Not Allowed	• Enable App • Allow Uninstallation

9. The Admin can get more information of an application. To view more information, hover your mouse on an app under the **Name** column. The system displays the following information shown below:
    - App Cache Size (in MB)
    - App Data Size (in MB)
    - App CPU Usage (in %)
10. According to your search filters criteria, the list view is updated with respective applications details.

App Monitor for Windows Phone 8



Installed Apps

Displaying 1 - 1 of 1 - Display 10

□	Name	Version	Product ID	App Type
	Search Name	Search Version	Search Package Name	Select
□	Enterprise Store	1.0.0.0	{4B06DA72-49D2-43DD-BFF8-A75F00A04DDD}	Enterprise Store

Targeted Apps

Display 10

Name	Version	Product ID	App Type
Search Name	Search Version	Search Package Name	Select

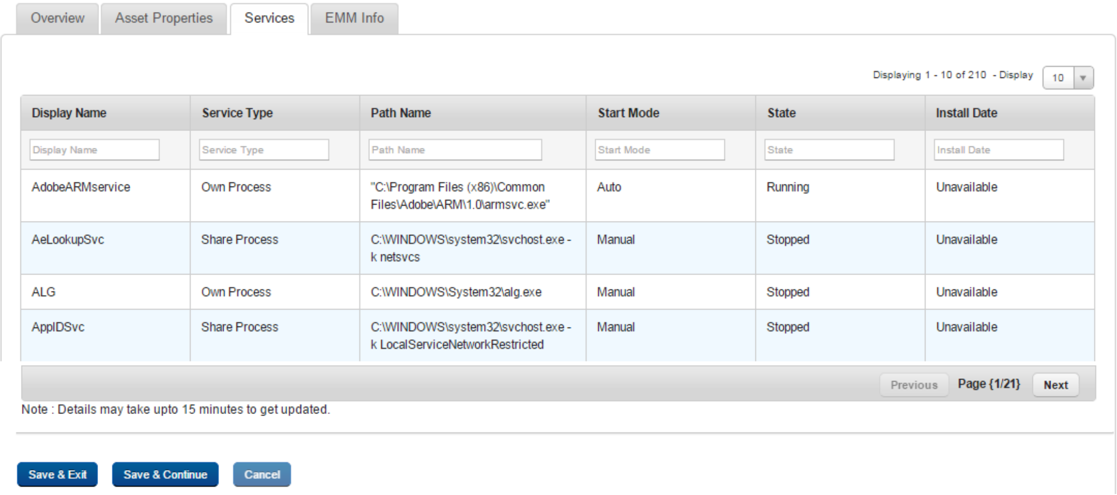
No records found.

The App Monitor list view for Windows Phone 8 has the following details:

- **Name**: Displays the name of the application.
- **Version**: Displays the version of the application.
- **Product ID**: Displays the product ID of the application.
- **App Type**: Displays the type of the application.

Services for Windows 8.1

For Windows 8.1 devices, Asset Properties tab is replaced with Services tab.



Displaying 1 - 10 of 210 - Display 10

Display Name	Service Type	Path Name	Start Mode	State	Install Date
Display Name	Service Type	Path Name	Start Mode	State	Install Date
AdobeARMservice	Own Process	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"	Auto	Running	Unavailable
AeLookupSvc	Share Process	C:\WINDOWS\system32\svchost.exe -k netsvcs	Manual	Stopped	Unavailable
ALG	Own Process	C:\WINDOWS\System32\alg.exe	Manual	Stopped	Unavailable
AppIDSvc	Share Process	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted	Manual	Stopped	Unavailable

Note : Details may take upto 15 minutes to get updated.

The Services list view for Windows 8.1 has the following details:

- **Display Name**: Displays the name of the service.
- **Service Type**: Displays the service type.
- **Path Name**: Displays path name.
- **Start mode**: Displays whether the service starts automatically or manually.
- **State**: Displays details on the running status of the service.
- **Install Date**: Displays the date on that the service is installed.

Removing an App

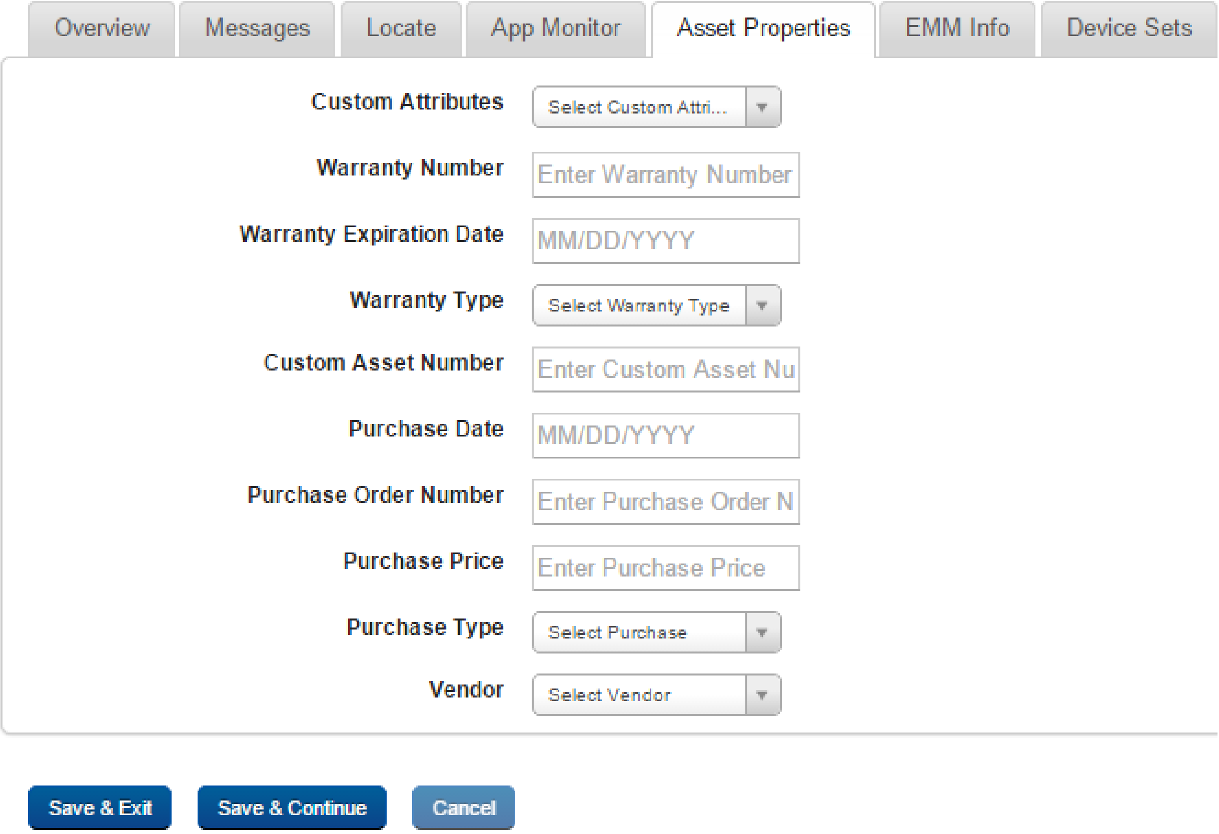
To remove an app, follow these steps:

1. Select the check box next to the app name in the list view.
2. Click the **Remove** button. In the confirmation message **(Remove Application)** that appears, click the **OK** button to return to the details page.
3. Click the **Save and Exit** button.In the confirmation message (**Device details**) that appears, click the **OK** button. The updated device is displayed in the list view.
4. Click the **Save and Continue** button to remain on the same page to update other details.

> ***Note:*** You can not remove any child apps from the devices manually.

10.6.1.5 Asset Properties

You can view and update the Asset Properties as captured during device enrollment. You can update the asset details through Asset Properties tab.

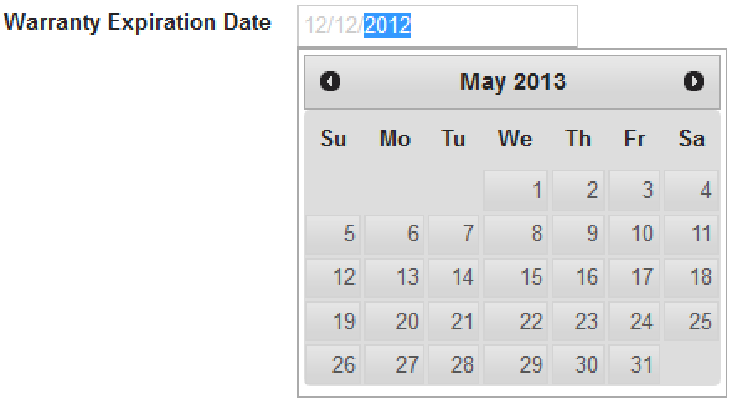


1. To perform the updates, follow these steps:

    a. **Custom Attributes**: Select a custom attribute you want to add from the list.

    b. **Warranty Number**: Enter Warranty Number in the **Enter Warranty Number** text field.

    c. **Warranty Expiration Date**: Click in the field to open the **Calendar window** to select the warranty expiration date.

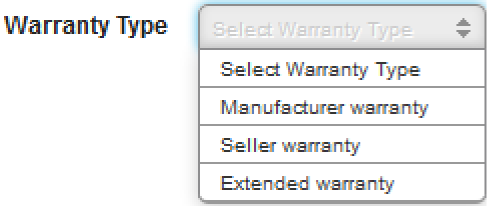


Warranty Expiration Date 12/12/2012

May 2013

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Click the required date in the calendar. The selected date appears in the date field.



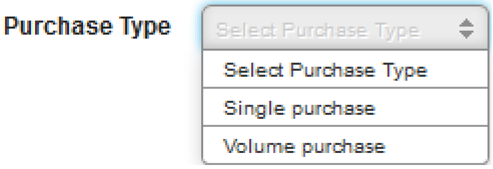
d. **Warranty Type**: Select the required warranty type from the dropdown list.

e. **Custom Asset Number**: Enter the custom asset number in the text field.

f. **Purchase Date**: Click in the field to open **Calendar window** to select the warranty expiration date.

g. **Purchase Order Number**: Enter the purchase order number in the text field.

h. **Purchase Price**: Enter the price of the asset.



i. **Purchase Type:** Select the appropriate purchase type from the dropdown list.

j. **Vendor**: Select the correct vendor from the dropdown list.

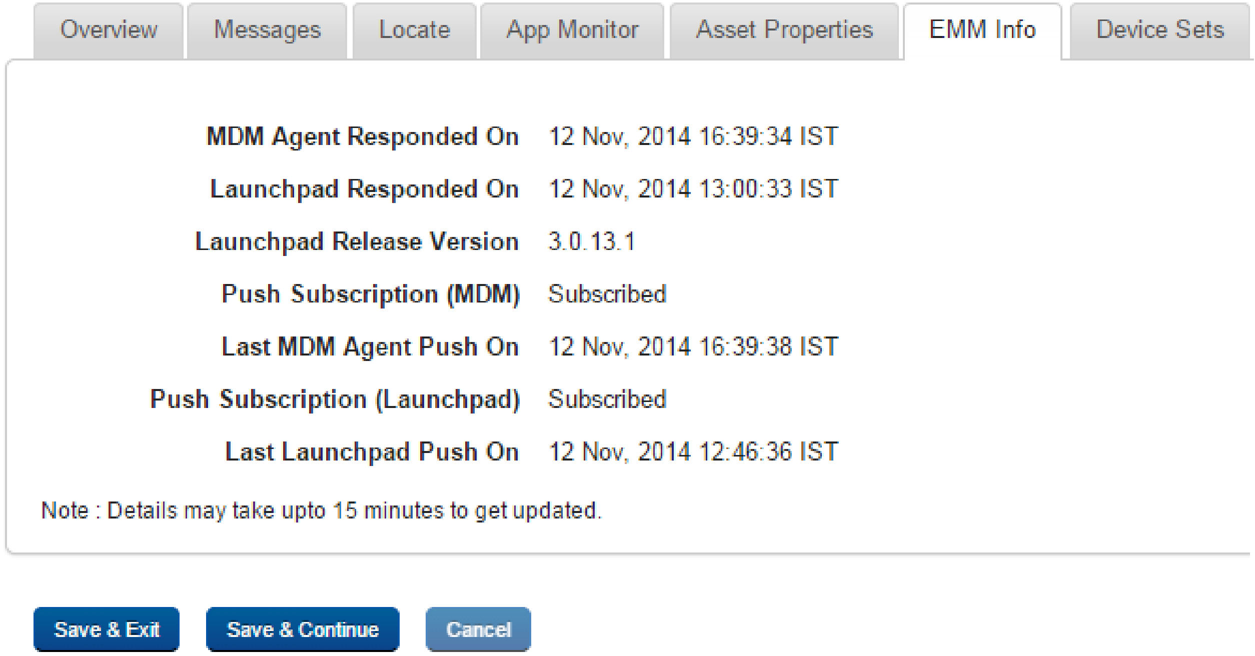
2. Click the **Save and Continue** button. In the confirmation message (Save Device Details - Success)that appears, click OK to continue.

   OR

3. Click the **Save and Exit** button to save the updates and exit the page.

10.6.1.6 EMM Info

You can view EMM Info as captured during device enrollment.



MDM Agent Responded On	12 Nov, 2014 16:39:34 IST
Launchpad Responded On	12 Nov, 2014 13:00:33 IST
Launchpad Release Version	3.0.13.1
Push Subscription (MDM)	Subscribed
Last MDM Agent Push On	12 Nov, 2014 16:39:38 IST
Push Subscription (Launchpad)	Subscribed
Last Launchpad Push On	12 Nov, 2014 12:46:36 IST

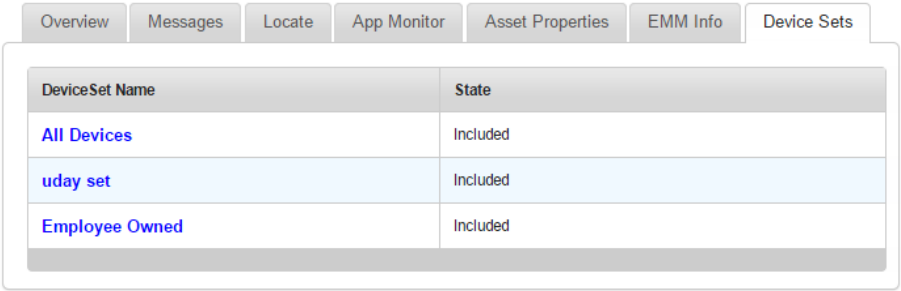
Note : Details may take upto 15 minutes to get updated.

- **MDM Agent Responded On**: Displays details about when the MDM agent responded.
- **Enterprise Store Responded On**: Displays details on when Enterprise Store responded.
- **Enterprise Store Release Version**: Displays Enterprise Store release version number.
- **Push Subscription (MDM)**: Displays whether MDM push is subscribed.
- **Last MDM Agent Push On**: Displays details on when the last MDM agent push occurred.
- **Push Subscription (Enterprise Store)**: Displays whether Enterprise Store push is subscribed.

- **Last Enterprise Store Push On**: Displays details on when the last Enterprise Store push occurred.

10.6.1.7 Device Sets

The Device Sets tab displays device set names the device belongs to.



DeviceSet Name	State
All Devices	Included
uday set	Included
Employee Owned	Included

- **Device Set Name**: Name of the device set.
- **State**: Displays the device state. The state can be included or excluded. The included state denotes that the device adheres to policies of the device set. The excluded state means that the device is excluded from all policies of the device set.

10.6.2 Device Details Page Actions

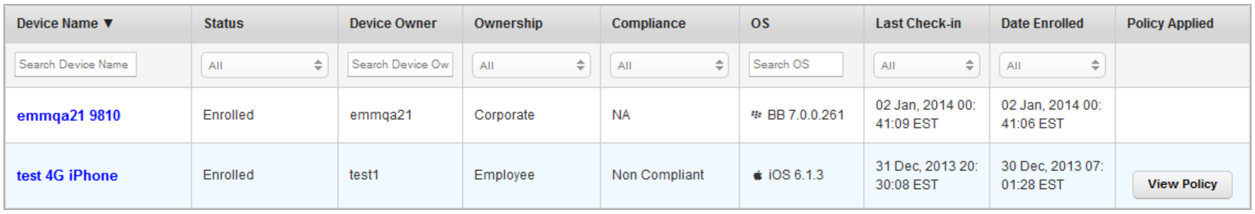
You can perform the following activities from Device List page.

- Searching for Devices
- Updating Device Details
- Locking a Device
- Device Passcode
- Remove App Data
- Block Email Access on Device
- Allow Email Access on Device

- Power Off Device (For Android)
- Disable Sim Pin Lock (For Android)
- Enable Sim Pin Lock (For Android)
- Resume Device
- Start Mirroring
- Stop Mirroring
- Force Check-in
- Purge

10.6.2.1 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 ▼	Status	Device Owner	Ownership	Compliance	OS	Last Check-in	Date Enrolled	Policy Applied
Search Device Name	All	Search Device Ow	All	All	Search OS	All	All	
emmqa21 9810	Enrolled	emmqa21	Corporate	NA	BB 7.0.0.261	02 Jan, 2014 00:41:09 EST	02 Jan, 2014 00:41:06 EST	
test 4G iPhone	Enrolled	test1	Employee	Non Compliant	iOS 6.1.3	31 Dec, 2013 20:30:08 EST	30 Dec, 2013 07:01:28 EST	View Policy

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. **Compliance**: Select the required compliance type from the dropdown list.

f. **OS**: Enter desired operating system version in the **Search OS** text field.

g. **Last Check-in** : Select the date on which the device was last checked-in to EMM from the dropdown list.

h. **Date Enrolled**: Select the date on which the device was enrolled to EMM from the dropdown list.

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.

10.6.2.2 Updating Device Details

The primary purpose to update a device details is to fulfill the requirement of existing business rules. To update a device, click the required device in the list view. Update the details for each tab of the device as required. For more information on this, see Device Details section.

10.6.2.3 Locking a Device

This action is used to lock the selected device in the following circumstances:

- When a Device is thought to be lost or stolen. The device is locked for a duration before the status is decided as Lost.
- The Device is found to be not in compliance with the rules, and can be locked (for Android). The device is locked automatically with the existing passcode.
- If the Device is not issued to any User, the device can be locked.

If Administrator tries to manually take action on the device, Administrator selects a device from the device list and invokes the Lock action.

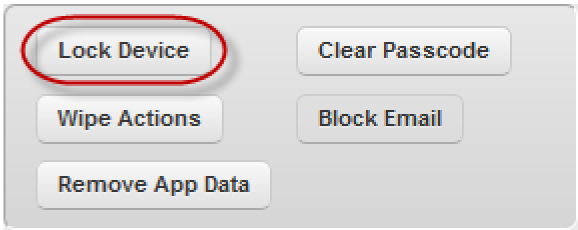
For iOS Devices

In case of iOS devices, the system seeks confirmation from the Administrator about the intention to lock. The Administrator receives a message with options. The administrator has to confirm the action by choosing either to Lock or Cancel the action.

By choosing Lock, the device is locked with the passcode existing on the device.

To lock a device, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.



2. Click the **Lock Device** button next to the Reset Passcode button to open the **Lock Device** window.
   a. **Message**: Enter text that to be appeared on the device.
   b. **Phone Number**: Enter a phone number that to be displayed on the device. Once this number is dialed, your device connects to that number.
3. Click **Lock**. The Lock Device confirmation message appears.
4. Click **OK** to continue .

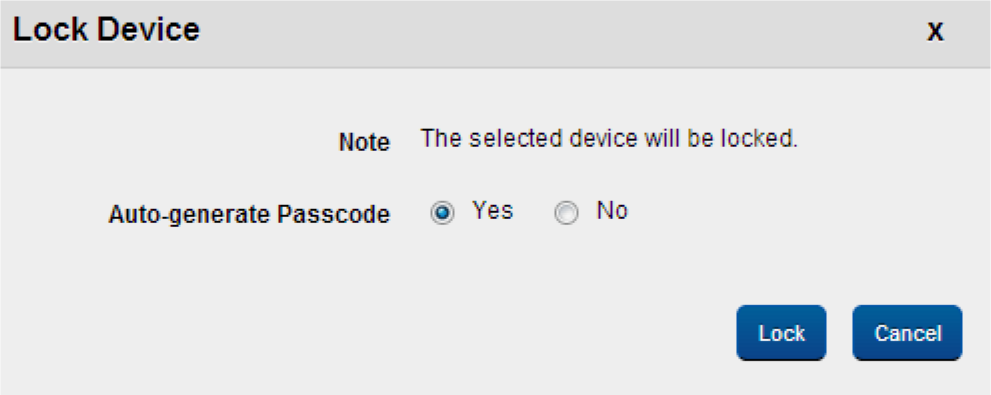
For Android Devices

For Android Devices, the Admin is informed through a message and a choice is provided for the Admin to Auto-Generate the Passcode prior locking the device with the two choices as **Yes** and **No**.

If the Admin chooses to Lock, An automated passcode is generated and applied. The system displays a message confirming that the device has been locked.

If the selected option is No and the Admin chooses to lock, the device is locked with the current passcode. The system displays a message confirming that the device has been locked.

> *Note:* Do not use Auto-generate Passcode if you have any other administrator for the device other than EMM.



Note The selected device will be locked.

Auto-generate Passcode ● Yes ○ No

1. Click the **Lock Device** button next to the Reset Passcode button to open the Lock Device window.

2. The Lock Device window appears with the following options:

3. **Auto-generate Passcode**:Click the Lock button. In the confirmation message (Lock Device) that appears, click OK to continue.

10.6.2.4 Device Passcode

As an Admin, you may require to reset the passcode of a device under following circumstances:

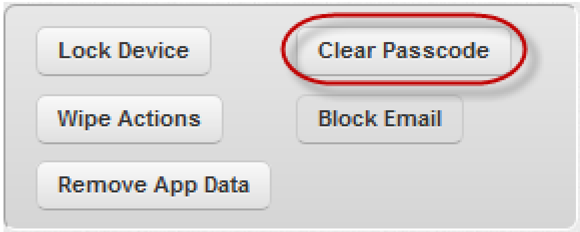
- If the Device User requests it.
- If the Device is missing and yet not declared as Lost.
- If the Device is out of compliance and the administrator wishes to stop any further access to the device temporarily (for Android).
- If the device user is changed.

- If a new Passcode is applied, then the new passcode overrides the existing passcode on the device. The device is automatically locked and you should unlock the device before use it again.
- If the passcode is cleared, no passcode exists on the device for a limited period of time. You need to assign a passcode for the device, which is in compliance with their passcode policy.
- For Android, if you fail to assign a new passcode within the stipulated duration, the system triggers an auto-generated passcode and a lock device command.

Clear Passcode for iOS Devices

To clear the passcode for iOS devices , follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Clear Passcode** button next to Lock Device button.



Clear Passcode window appears with the warning message that if user wishes to clear the passcode, this action will clear the passcode and a new passcode will be generated as per policy.

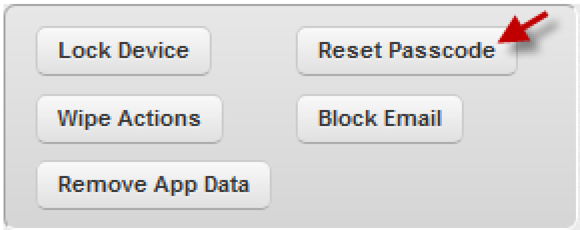
3. Click Yes to continue.
4. In the confirmation message (Reset Passcode) that appears, click OK to return to the main page.

> ***Note:*** (For iOS Platform only) When a user is on Passcode lock screen, and at the same moment Administrator initiates the Clear Passcode; the device hangs and the user needs to restart the device.

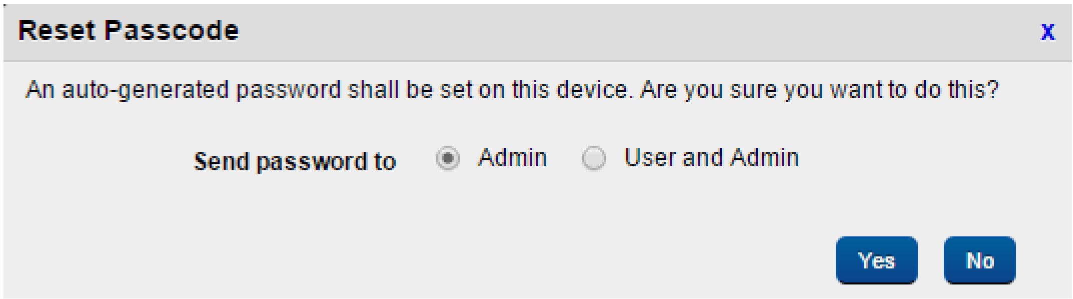
Reset Passcode for Android Devices

To reset the passcode for Android devices, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Reset Passcode** button next to Lock Device button.



Reset Passcode window appears.



Reset Passcode

An auto-generated password shall be set on this device. Are you sure you want to do this?

Send password to ● Admin ○ User and Admin

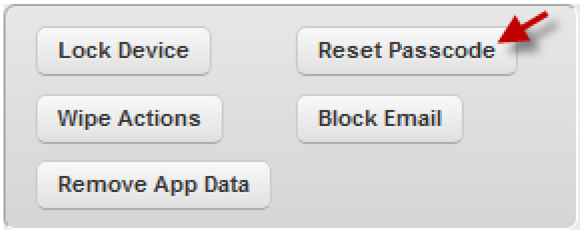
3. **Send password to**: Select where you want to send the reset password. You can choose to end it to the admin alone or to the admin or both admin and the user. By default Send password to is set to **Admin**.
4. Click the **Yes** button. The System displays the confirmation message stating that the request to reset the passcode is successfully submitted and will be executed shortly.
5. Click the **Cancel** button to return to the main page.

Reset Passcode for Windows 8.1 Phone Devices

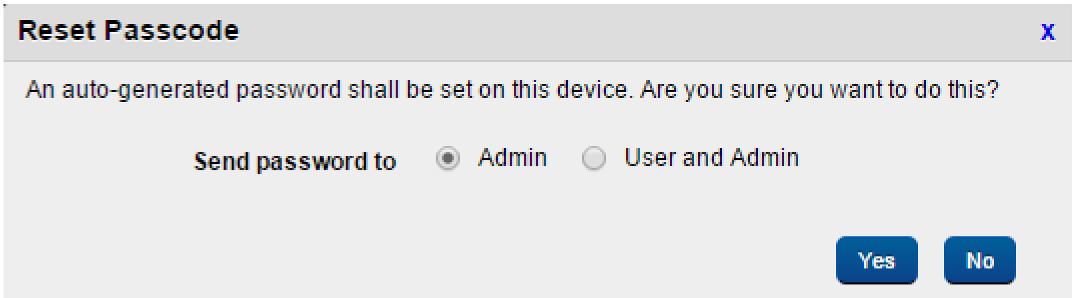
To reset the passcode for Windows 8.1 Phone devices, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.

2. Click the **Reset Passcode** button.



Reset Passcode window appears.



Reset Passcode

An auto-generated password shall be set on this device. Are you sure you want to do this?

Send password to ● Admin ○ User and Admin

3. **Send password to**: Select where you want to send the reset password. You can choose to end it to the admin alone or to the admin or both admin and the user. By default Send password to is set to **Admin**.

4. Click the **Yes** button. The System displays the confirmation message stating that the request to reset the passcode is successfully submitted and will be executed shortly.

5. Click the **Cancel** button to return to the main page.

10.6.2.5 Ring Device for Windows Phone 8.x Devices

You can ring a Windows Phone 8.x device using the Ring Device feature.

To ring a Windows Phone 8.x device,

1. Navigate to the Device Details page of the Windows Phone 8.x device you want to ring.

2. Click **Ring Device**. Ring Device confirmation page appears.

3. Click **Ring**. A confirmation message appears stating that the request is submitted.

4. Click **OK**.

10.6.2.6 Wipe Device

This feature is used to clear the device settings.As an administrator, you may require to wipe the device under several situations:

- If the Device User requests it, for example, the device has become too slow.
- If the Device is missing and yet not declared as Lost.
- The Device is out of compliance and the administrator wishes to stop any further access to the device temporarily.
- If the device user is changed.

The generic process to wipe a device is as follows:

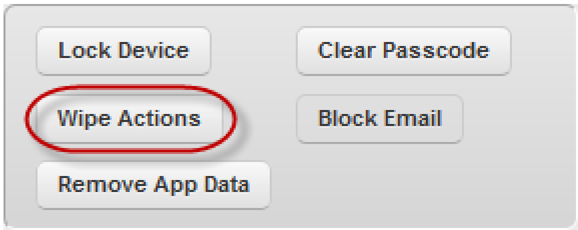
1. The Admin selects a device, which needs to be wiped.
2. The Admin invokes the Wipe action.
    a. For Corporate owned and Shared devices, two options are available: Enterprise Wipe or Complete Wipe.
    b. For Employee owned devices only Enterprise Wipe can be conducted.
3. Admin defines the Status for the completion of Wipe action. The Status can be Deactivated, Retired, Device Lost or Suspended.

> ***Note:*** If a user tries to re-enroll a completely wiped device listed under Enrollment Denied List, the device displays the Terms and Conditions page, in a loop every time a user tries to login. In Enterprise wiped device it works as expected.

To wipe a device follow these steps:

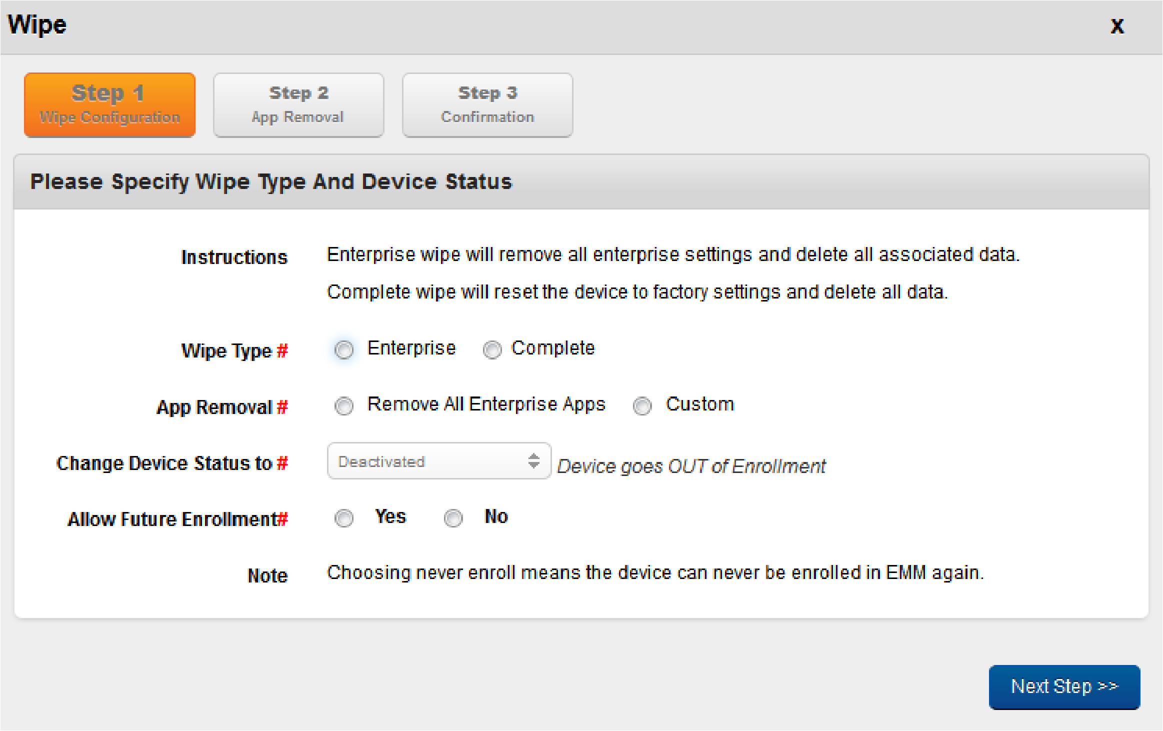
1. Click the required device in the list view. The **Device Details** page appears.

2. To open the Wipe window, click the **Wipe Actions** button next to the Block Email button.



3. The **Wipe Window** appears. The Wipe window includes three steps to wipe a device.

4. **Step One- Wipe Configuration**:Enter the following details:



Please Specify Wipe Type And Device Status

Instructions	Enterprise wipe will remove all enterprise settings and delete all associated data. Complete wipe will reset the device to factory settings and delete all data.
Wipe Type #	○ Enterprise ○ Complete
App Removal #	○ Remove All Enterprise Apps ○ Custom
Change Device Status to #	Deactivated *Device goes OUT of Enrollment*
Allow Future Enrollment#	○ Yes ○ No
Note	Choosing never enroll means the device can never be enrolled in EMM again.

a. **Wipe Type**: Select the Wipe Type as **Enterprise** or **Complete**.

   If Enterprise Wipe is selected then the selected device is un-enrolled and all enterprise data is deleted through EMM profiles, policies and internal applications.The EMM server still holds control over the device. Enterprise Wipe can be applied on all the devices. enterprise store app data is deleted for iOS but not for Android upon Enterprise wipe.

   If the device is completely wiped, the device should be reset to factory settings. All data on the device - enterprise or personal is deleted. Once this wipe is complete, EMM cannot control the device any longer. Complete Wipe can be applied on Corporate and Shared Devices.

   > *Important:*
   > **(For Employee owned Devices only)**
   > If you select Complete Wipe as Enforcement Action, then Enterprise Wipe with deactivated state is sent to the device.
   >
   > **(For Corporate and Shared Devices)**
   > If you select Complete Wipe as Enforcement Action, then Complete Wipe occurs but future enrollment of the device is not possible.

b. **App Removal**: Click the option as **Remove All Enterprise Apps** or **Custom.**

   App Removal window appears in Step two only, if the Admin selects the option as Custom in App Removal. It is also possible only for Enterprise Wipe only. It is done only when certain apps are meant to be preserved even after the wipe

   You as an Admin should specify to remove all enterprise apps or selectively remove enterprise apps. The default behavior is to remove all the enterprise apps.

c. **Change Device Status to**: Select the device status from the drop-down menu. By default, it is set to **Deactivated,** which you can modify to following options:

   - Deactivated: The device is un-enrolled and the device state is changed to Deactivated. The enrollment rule for this case is Allow Enrollment.

- Retired: The device is un-enrolled and the device state is changed to Retired. The enrollment Rule for this case is Never Enroll.

- Suspended: The device remains enrolled and the device state changes to Suspended. This ensures that Admin still has control over the device. The Admin cannot specify any enrollment Rule.

> *Note:* In case a device is suspended, the **Passcode policy** and **Device Restrictions policy** are retained on the device. Rest of all the other policies are removed from the device. However, the device is still expected to be in compliance with the policies assigned to the same.

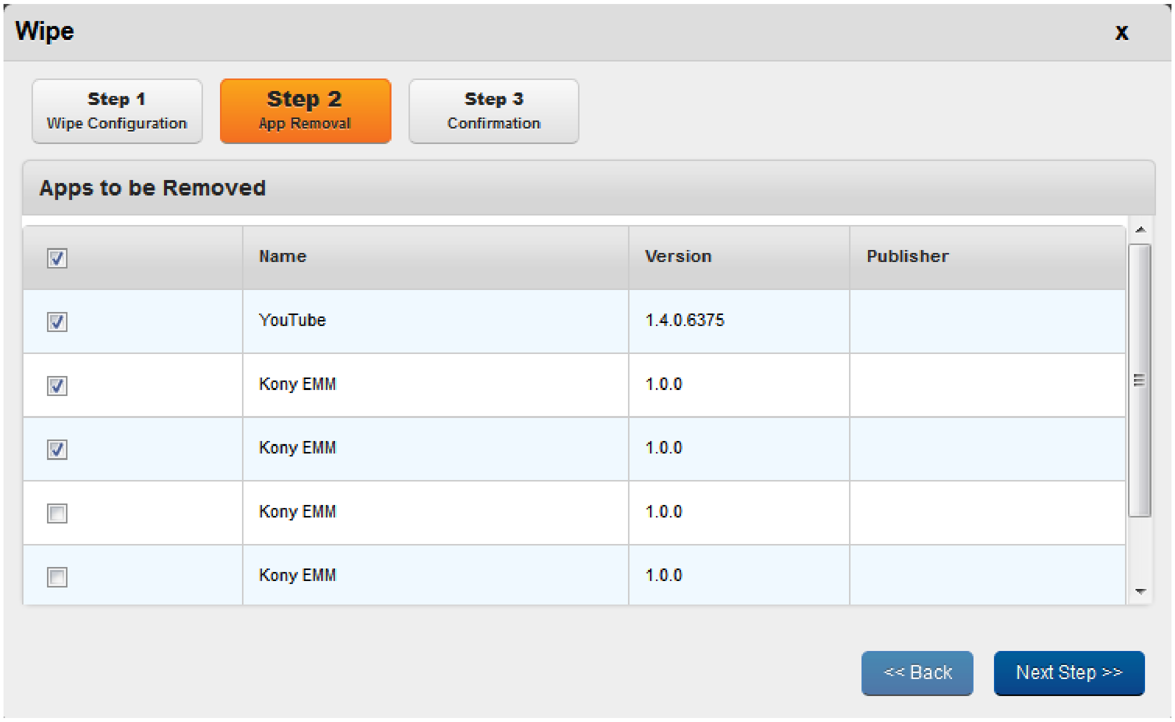
> *Note:* For Android, when a user ignores Enterprise Wipe request, the system continuously prompts the user until he accepts it to fully wipe Enterprise data from the device. User can ignore Enterprise Wipe request either by clicking the **Cancel** button or the **Home** button.

d. **Allow Future Enrollment**: If you select this option, then a device can be enrolled again. This is applicable for Deactivated, Retired, and Device Lost statuses only.Based on corporate policy and your discretion, you can select to allow enrollment or never enroll the device.

> *Important:* : If you perform Enterprise Wipe and select any of the Device Status available, then Kony EMM enterprise store is not removed from the device, although the specific policies are removed

5. Click the **Next step** button to navigate to **Step No 2**.

6. **Step 2 - App Removal**:By default, all the apps in the list view are selected. If required, deselect the check box adjoining app name to retain it.

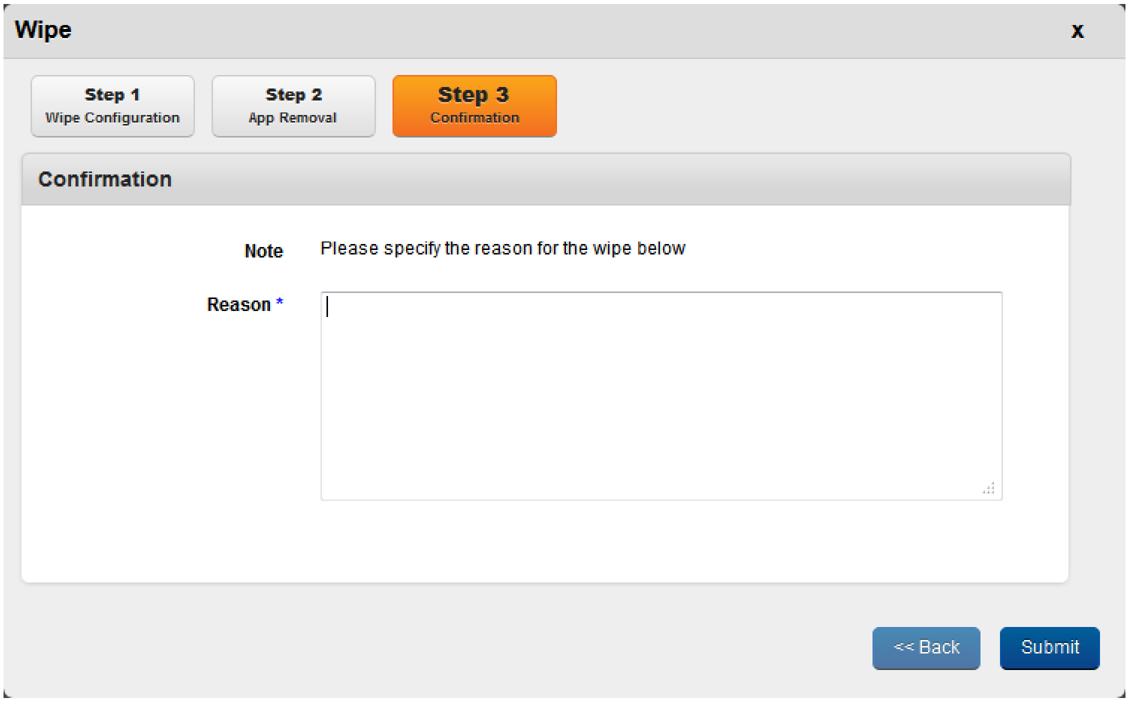


Apps to be Removed

☑	Name	Version	Publisher
☑	YouTube	1.4.0.6375	
☑	Kony EMM	1.0.0	
☑	Kony EMM	1.0.0	
□	Kony EMM	1.0.0	
□	Kony EMM	1.0.0	

> *Important:* EMM enterprise store does not get deleted automatically when the User removes control by deleting the profile.The user is required to delete the Agent,if wishes to enroll again.

7. Click the **Next step** button to navigate to **Step No 3**.
8. **Step 3: Confirmation**: Enter a valid reason for the wipe in the **Reason** Box.



Confirmation

Note Please specify the reason for the wipe below

Reason *

9. Click the **Submit** button. In the confirmation message **(Wipe Device Window)** that appears, click OK to continue.

10. Click OK to return to the main page. When you deactivate or retire the device, system returns to the Device List page. When you suspend the device, system refreshes the Device Details page and displays Resume Device button.

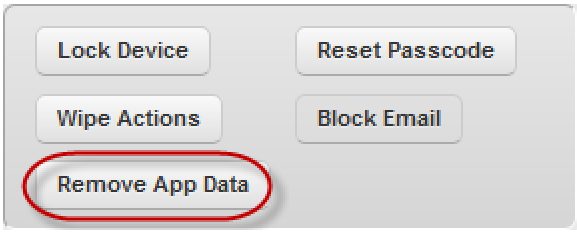
Wipe Device -Windows Phone 8

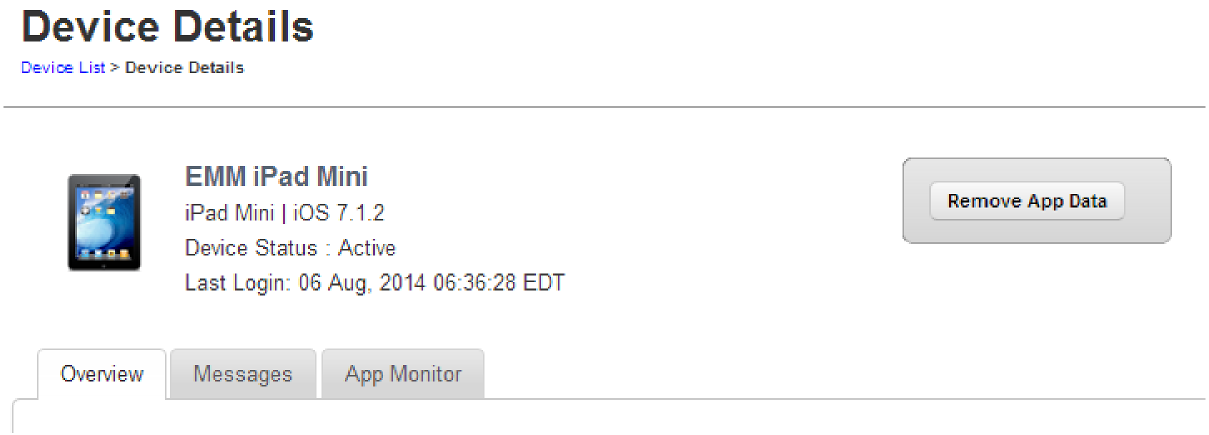
In win Phone 8, we have limitations in identifying control removed state. Win Phone 8 does not report a user initiated disconnection (un-enrollment).

So if a user deletes a company app/account, the user still remains as Enrolled in EMM server. The user can re-enroll with same credentials to resume the provision. If the user tries to re-enroll with different credentials, then the user is wiped after first sync, and previous record (Enrolled state) is marked as suspended.

10.6.2.7 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.





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.

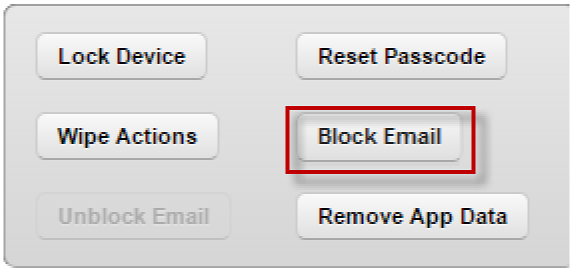
> *Note:* For Windows Phone 8.x devices, the remove app data policy will not work if the app is in use. The policy command will apply when the app is closed and relaunched.

10.6.2.8 Block Email Access on Device

Block Email action prevents access to the Exchange ActiveSync. Exchange Server must be configured and Exchange Security Services installer must be run on the same. The device must also be assigned an Exchange Account for this feature to work. You cannot view emails from Exchange server again. You may wish to block email for various reasons, for example, if a device connects to a non-prescribed Wi-Fi network.

To block email communication to a device, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Block Email** button.



The system displays the warning message (Block Email) asking the user, if really wishes to block email for this device.

3. Click the Block button to block emails for this device. In the confirmation message (Request Sent), click **OK** to return to the page.

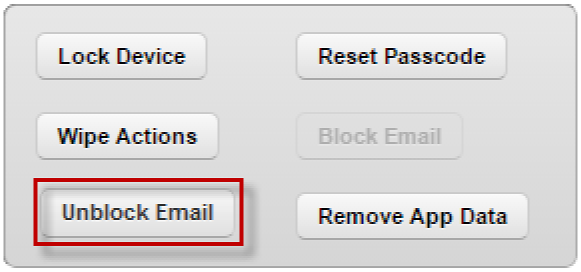
> *Note:*
>
> 1. This option is displayed for AD users only. If you come across any errors, check and ensure that Exchange server is working properly.

> 2. If an already enrolled Local user is overwritten with an AD User then Block Email functionality does not work.
>
> 3. On some Android devices, when Block Email option is initiated, the Native Android email client is not blocked, as Native EAS clients in some Android devices do not share their IMEI numbers with Exchange Server.

10.6.2.9 Unblock Email

Allowing emails on the device removes it from the list of Blocked devices and automatically allows the device to access Exchange ActiveSync again.

To allow email communication to a device, follow these steps:



1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Unblock Email** button.
3. The system displays the warning message (Unblock Email) asking the user, if really wishes to unblock email for this device.
4. Click the **Unblock** button to allow emails for this device. In the confirmation message (Request Sent), click **OK** to return to the page.

> ***Note:*** This option is displayed for AD users only. If you come across any errors, check and ensure that Exchange server is working properly. Exchange must be configured and assigned to device for this functionality to work.

10.6.2.10 Power Off Device (for Android)

Power Off Device feature allows an administrator to remotely power off a device. When the administrator attempts to power off the device, the system displays a confirmation message:"*Are you sure you want to power off the device {$deviceName}?*". Click Yes to confirm if you want to power of the device.

10.6.2.11 Disable SIM Pin Lock (For Android)

An administrator needs a four digit pin to enable or disable a SIM , which allows the addition or removal of a password protection to the SIM card.

The same administrator who enabled a SIM Personal Identification Number (PIN) lock on a device must disable the locked SIM on the same device. The SIM can neither be locked by another Admin of MDM service, nor it can be unlocked by the same Admin.

10.6.2.12 Enable SIM Pin Lock (for Android)

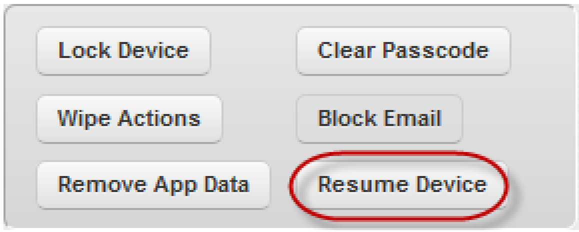
When a user enables a SIM PIN lock, the SIM card is locked and cannot be used until the correct code is entered. That helps protect your account information and other data in case your device is lost or stolen.

When the User moves the SIM to another device, the PIN must be entered. As this Pin is not shared with the User, the usage of the SIM is effectively locked to the device it was locked with. Maximum two attempts for entering pin is allowed.

10.6.2.13 Resume Device

An administrator may decide to change the status of a suspended device. To bring the device out of suspension, the administrator invokes the Resume action. A suspended device is still enrolled, and the EMM server has full control over the device.

To resume a suspended device, follow these steps:



1. Click the required device in the list view. The Device Details page appears.

   Click the **Resume Device** button.

2. The system displays a warning message (Resume Device) asking the user, if the user really wants to resume this device.

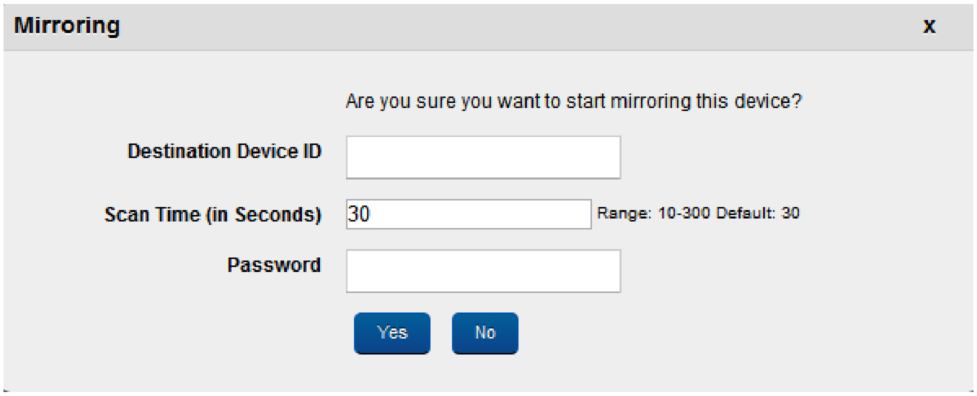
3. Click the **Resume** button to resume the device. In the confirmation message (Resume Device), click OK to return to the page.

10.6.2.14 Start Mirroring (for iOS7+ Devices)

The Start Mirroring feature is a useful tool to conduct job-related presentations or to display your iPhone photos on a bigger screen. When you enable Start Mirroring, your iOS7+ device can connect with another device, such as an Apple TV or a Mac, and share a screen.

To start mirroring, follow these steps:

1. Click the **Start Mirroring** button. The Mirroring dialog appears.



Are you sure you want to start mirroring this device?

Destination Device ID

Scan Time (in Seconds) 30 Range: 10-300 Default: 30

Password

2. In **Destination Device ID**, enter the WiFi Mac ID of the device.

3. In **Scan Time (in seconds)**, by default the time is set to 30 seconds. You can modify the scan time , which is defined by a range of 10 to 300 seconds. The scan time refers to the time that the device has to find the destination.

4. In **Password**, enter the password to connect the destination.

5. Click **Yes**. The system starts mirroring the device.

10.6.2.15 Stop Mirroring (for Supervised iOS7+ Devices)

> ***Note:*** If this is applied for non-supervised devices, the command will not execute.

Stop Mirroring allows you stop an Airplay mirroring that is in progress.

1. To stop airplay mirroring, click **Stop Mirroring** button. The system displays a confirmation message.

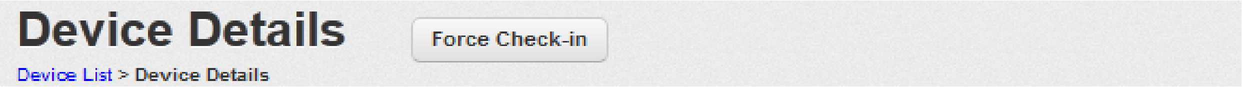
2. Click **Yes** to confirm.

10.6.2.16 Force Check-in

You may wish to view the latest details of the device to analyze its current state and monitor compliance.By invoking this action, the latest device details and compliance states are refreshed and provided.

> ***Note:*** Device Details displays the details according to the last heartbeat (device synchronization with the EMM server).

To perform Force Check-in, follow these steps:



1. Click the **Force Check-in** button next to Device Details label.
2. In the confirmation message (Force Check-in) that appears, click **OK** to return to the main page.

10.6.2.17 Purge

If a device is inactive for the number of days specified continuously, the device will be automatically purged. The device can then be enrolled again. Purge feature allows an administrator to change the status of a device whose control is removed but is unknown to the server. The administrator can delete the device, and users can then enroll the device on their names.

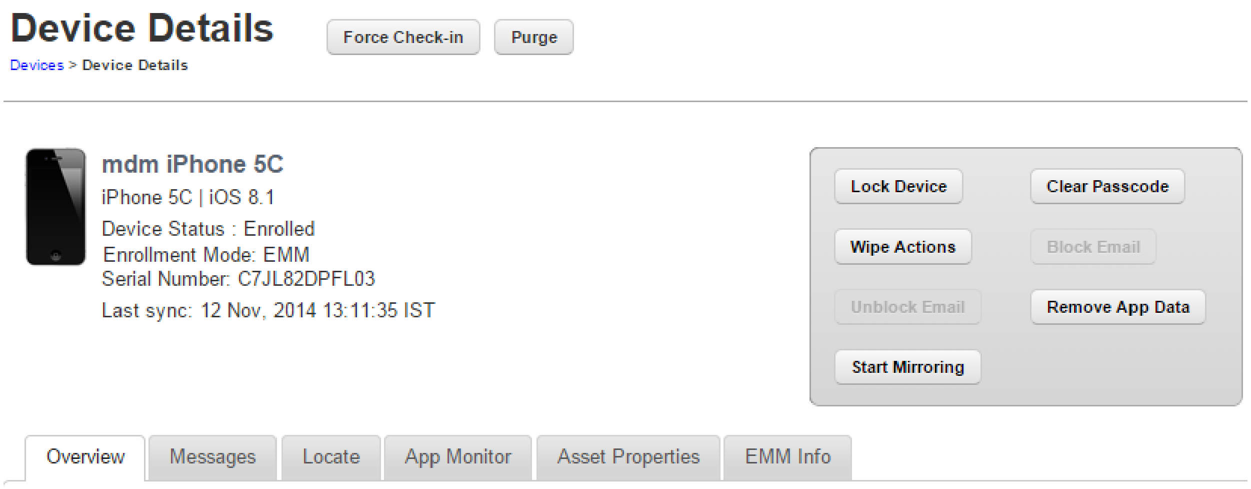
> ***Note:*** On Android devices, enterprise store from purged devices should be deleted for device re-enrollment. On iOS devices, profile should be deleted on a purged device before it is re-enrolled.

To purge a device,

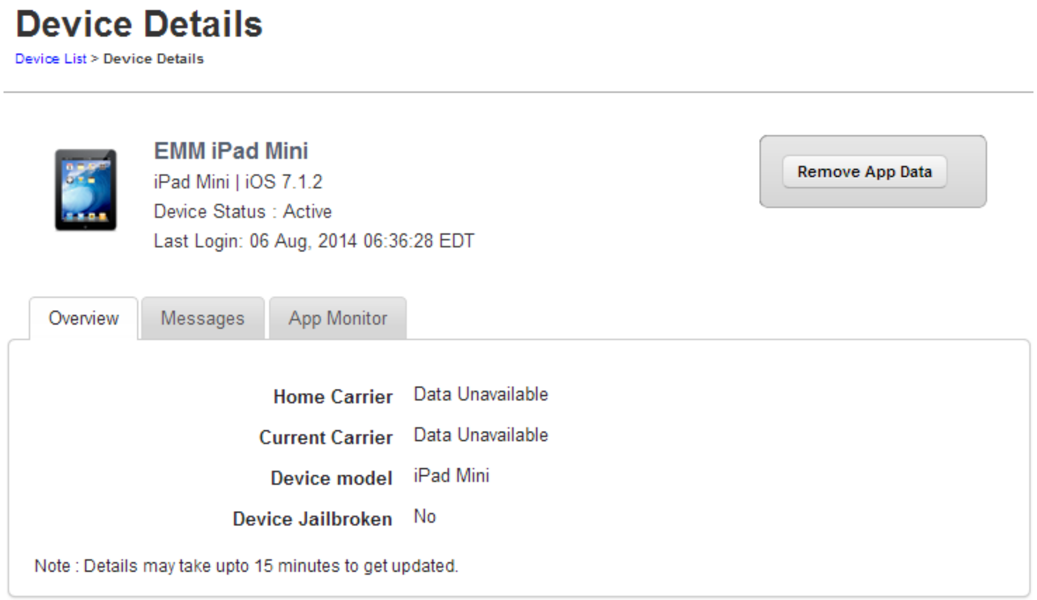
1. In the Device Details page, click **Purge** next to the Device Details label.
2. In the confirmation message (Purge) that appears, click **OK**. Main page appears.

10.6.3 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.



mdm iPhone 5C
iPhone 5C | iOS 8.1
Device Status : Enrolled
Enrollment Mode: EMM
Serial Number: C7JL82DPFL03
Last sync: 12 Nov, 2014 13:11:35 IST



EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

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.

Screen Element Properties	Description
Page Title	This is available on extreme right corner on top of the screen, for example, Device Details.
Navigation Link	This link navigates you to main page, for example, click Device List > Device Details link to navigate to Device List main page.
Device Name	Displays the unique identification name of the device.
Device Status	Displays the current status of the device, for example enrolled.
Enrollment Mode	Displays the enrollment mode of the device.
Serial Number	Displays the unique serial number of the device.
Last Sync	Displays the date and time when the device was last synced with the server.

> ***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

10.6.3.1 Device Details Page Tabs

Device details page displays the following tabs:

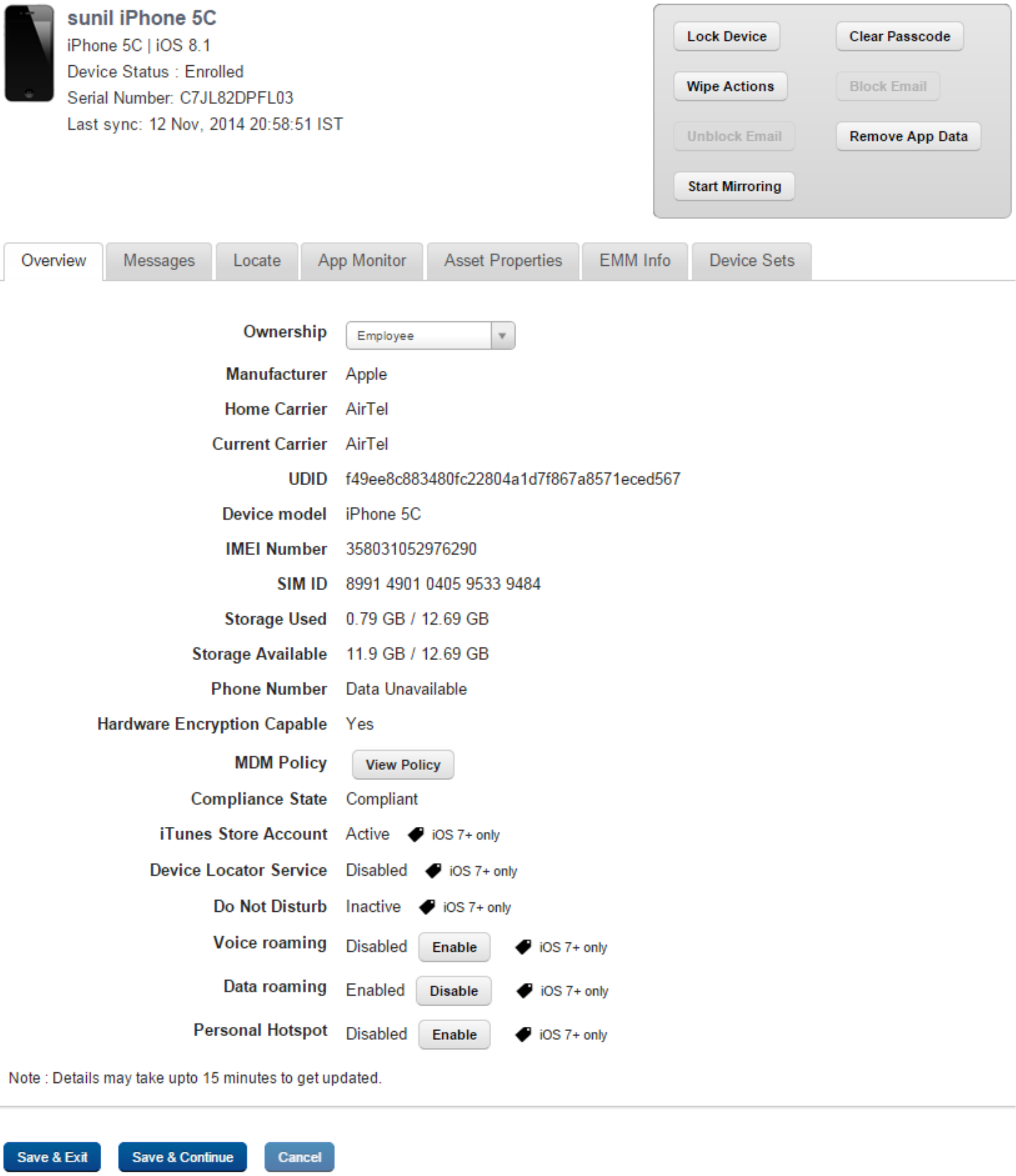
- Overview
- Messages

- Locate
- App Monitor
- Asset Properties
- EMM Info
- Device Sets

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



sunil iPhone 5C
iPhone 5C | iOS 8.1
Device Status : Enrolled
Serial Number: C7JL82DPFL03
Last sync: 12 Nov, 2014 20:58:51 IST

Ownership	Employee
Manufacturer	Apple
Home Carrier	AirTel
Current Carrier	AirTel
UDID	f49ee8c883480fc22804a1d7f867a8571eced567
Device model	iPhone 5C
IMEI Number	358031052976290
SIM ID	8991 4901 0405 9533 9484
Storage Used	0.79 GB / 12.69 GB
Storage Available	11.9 GB / 12.69 GB
Phone Number	Data Unavailable
Hardware Encryption Capable	Yes
MDM Policy	View Policy
Compliance State	Compliant
iTunes Store Account	Active iOS 7+ only
Device Locator Service	Disabled iOS 7+ only
Do Not Disturb	Inactive iOS 7+ only
Voice roaming	Disabled Enable iOS 7+ only
Data roaming	Enabled Disable iOS 7+ only
Personal Hotspot	Disabled Enable iOS 7+ only

Note : Details may take upto 15 minutes to get updated.

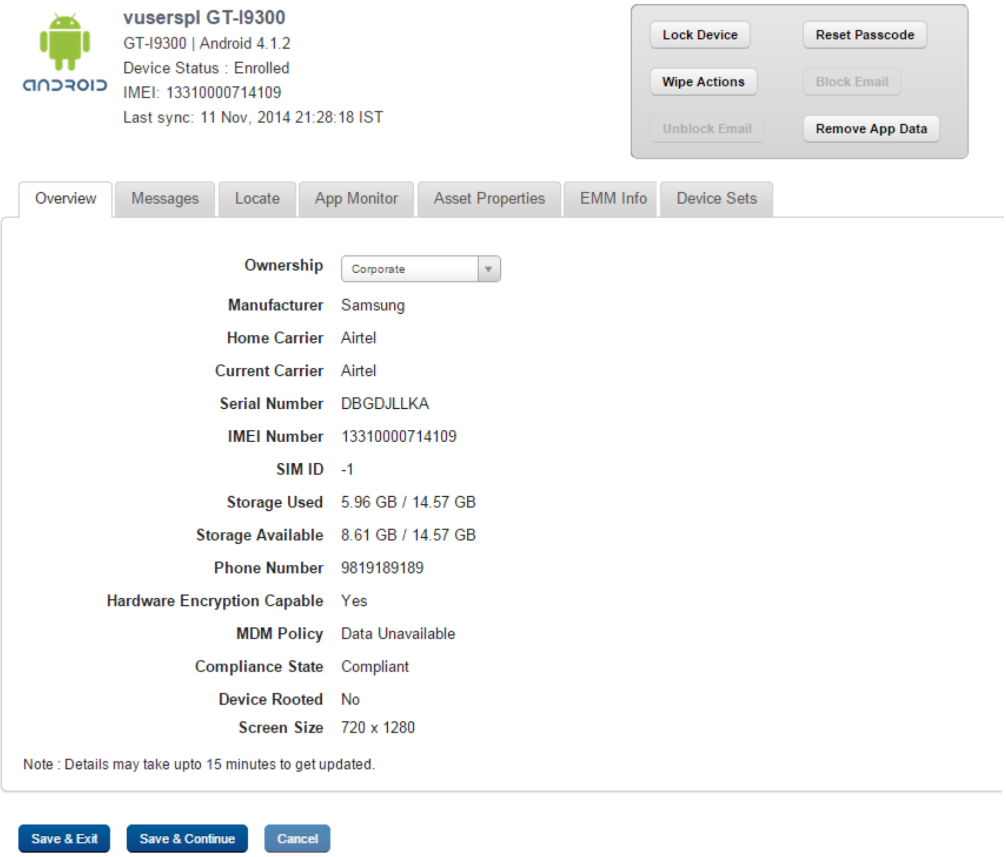
- **Compliance State**: Displays compliance state of the device.

> *Note:* In case of conditional compliance (or both policy and rule), the system displays the policy name and rule name. For example <policy name:rule name>.
>
> In case of simple compliance, the system displays the compliance status.
> For example, <Non Compliant (Min OS Version)>

- **iTunes Store Account Active**: Displays whether an iTunes Store Account is Active.
- **Device Locator service**: Display whether Device Locator service is enabled.
- **Do Not Disturb**: Displays whether Do Not Disturb is in effect.
- **Voice Roaming**: Displays whether Voice Roaming is enabled.

  If you enable Data Roaming, the Voice Roaming is enabled automatically.
- **Data Roaming**: Displays whether Data Roaming is enabled. You can modify it to Disable.
- **Personal Hotspot**: Displays whether Personal Hotspot Enabled. You can modify it to Disable.
- **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.

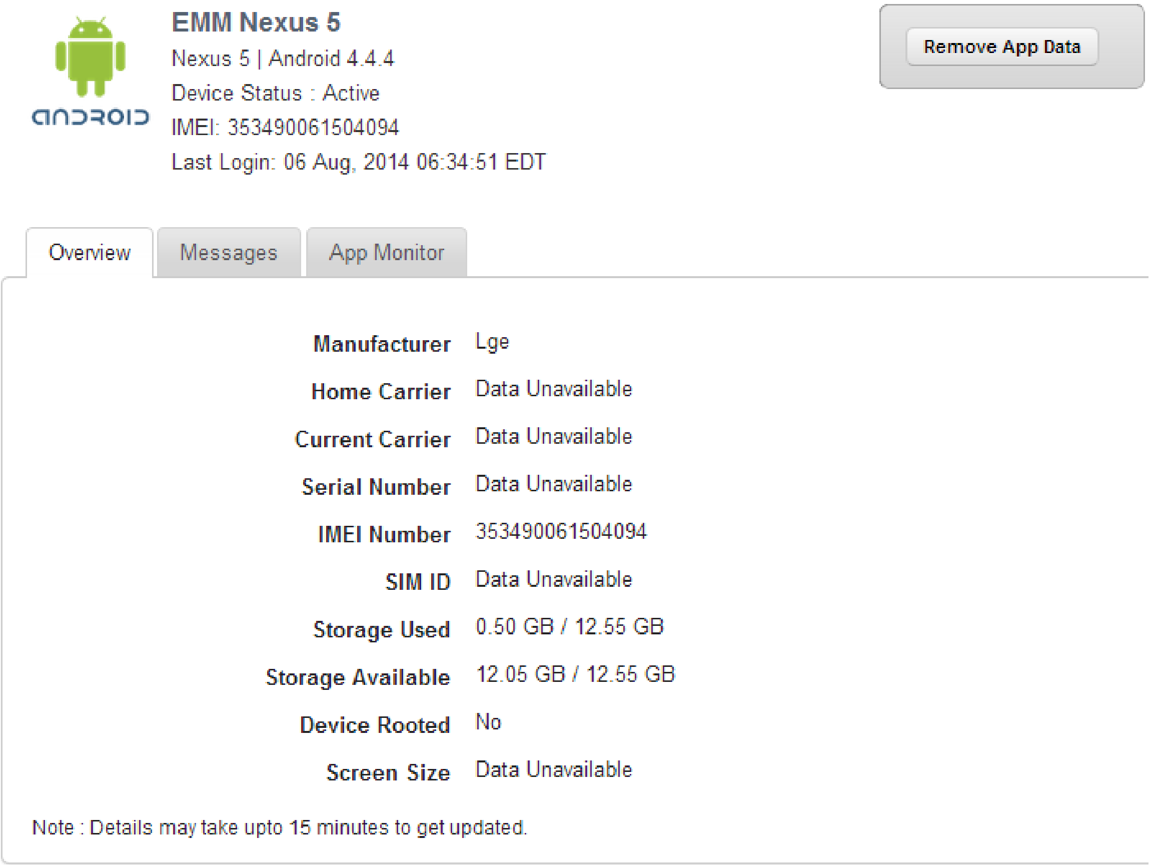
Overview for Android



vuserspl GT-I9300
GT-I9300 | Android 4.1.2
Device Status : Enrolled
IMEI: 13310000714109
Last sync: 11 Nov, 2014 21:28:18 IST

Ownership	Corporate
Manufacturer	Samsung
Home Carrier	Airtel
Current Carrier	Airtel
Serial Number	DBGDJLLKA
IMEI Number	13310000714109
SIM ID	-1
Storage Used	5.96 GB / 14.57 GB
Storage Available	8.61 GB / 14.57 GB
Phone Number	9819189189
Hardware Encryption Capable	Yes
MDM Policy	Data Unavailable
Compliance State	Compliant
Device Rooted	No
Screen Size	720 x 1280

Note : Details may take upto 15 minutes to get updated.



EMM Nexus 5
Nexus 5 | Android 4.4.4
Device Status : Active
IMEI: 353490061504094
Last Login: 06 Aug, 2014 06:34:51 EDT

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.

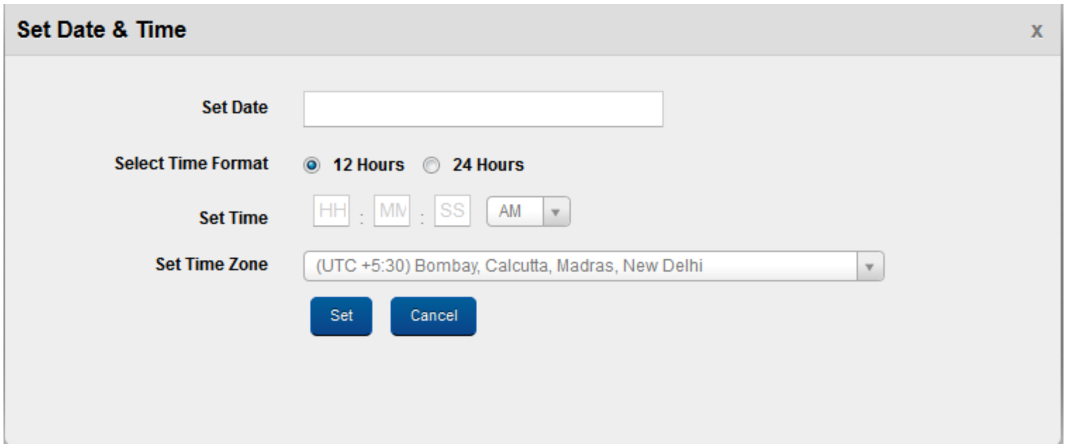
Manufacturer:

- **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 Date & Time**: Displays date and time of the device.
  Date: Displays date of the device.
  Time: Displays time in HH/MM/SS format (12 hour or 24 hour set on device)
  Timezone: Displays timezone of the device.

  The Admin can modify the date and time settings if permissions are granted in the Device Restrictions policy.

  a. Click the **Modify** button if you wish to change the settings.

  Set Date & Time

  Set Date

  Select Time Format ● 12 Hours ○ 24 Hours

  Set Time HH : MM : SS AM

  Set Time Zone (UTC +5:30) Bombay, Calcutta, Madras, New Delhi

  b. In the **Set Date & Time** dialog, enter the details and click **Set**.

- **Compliance State**: Displays compliance state of the device.

> ***Note:*** In case of conditional compliance (or both policy and rule), the system displays the policy name and rule name. For example <policy name:rule name>.
>
> In case of simple compliance, the system displays the compliance status.
> For example, <Non Compliant (Min OS Version)>

- **Device Rooted**: Displays whether device root access is enabled.

- **Screen Size**: Displays the screen size of the device.

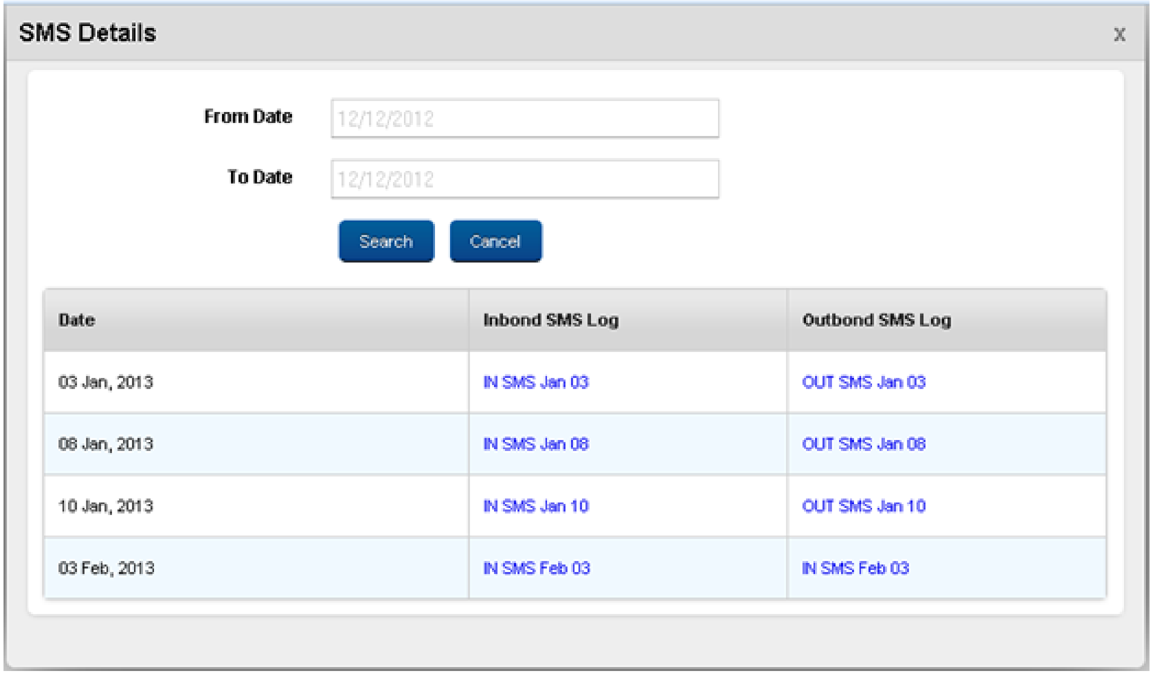
- Certificates (Android SAFE): Displays certificates installed on the device.
  The administrator can remove all of these certificates if required. When the administrator attempts to delete certificates, the system displays a confirmation message "*Do you want to remove all certificates from the credential store?*"
  Click **Yes** to confirm to delete certificates.

- **Block MMS with Storage(Android SAFE)**
  When MMS is blocked, all the MMSes received are stored on the device, but not shown to the User. The administrator can choose to Unblock MMS by clicking the same. Once unblocked, the MMSes are delivered to the User.

- **Block SMS with Storage (Android SAFE)**
  When SMS is blocked, all the SMSs received by the device are stored on the device but not shown to the User. The Admin can choose to Unblock SMS by invoking the same. Once unblocked, the stored SMSs are delivered to the device.

  The Admin can also choose to clear the stored SMS messages by click on the Clear Stored SMS button. If cleared stored SMSs, the SMSs are never delivered. This may need to be done if a device is non-compliant and the Block Action was taken. But the device then must be deactivated. Then instead of delivering the SMSs, the admin choose to clear them.

- **Calls and SMS Stats Capture (Android SAFE)**



From Date 12/12/2012

To Date 12/12/2012

Date	Inbond SMS Log	Outbond SMS Log
03 Jan, 2013	IN SMS Jan 03	OUT SMS Jan 03
08 Jan, 2013	IN SMS Jan 08	OUT SMS Jan 08
10 Jan, 2013	IN SMS Jan 10	OUT SMS Jan 10
03 Feb, 2013	IN SMS Feb 03	IN SMS Feb 03

Through Restrictions Policy, both Calls and SMS stats capture can be enabled. This allows the Admin to get logs of all Call and SMS data.

Daily logs are maintained separately for Incoming and Outgoing Calls and SMSes. The Admin can access these from the Device Overview. These logs are stored in .CSV format. They can be downloaded when the User clicks to see Details. The Admin can specify the date range for which to show logs and all the logs are shown.

The max limit of logs allowed per device is 1 MB. If the logs go above that, they are automatically purged in a first in first out manner.

- **Reset SMS Count (Android SAFE)**
  This resets the number of SMS to 0. User can send SMSes again until they reach the limit as specified in the Device Restrictions policy.
- **Reset Calls Count (Android SAFE)**
  This resets the number of Calls to 0 (zero). User can send Calls again until they reach the limit as specified in the Device Restrictions policy.

- Click the **Save and Exit** button. In the confirmation message that appears, click OK to return to the device list page.

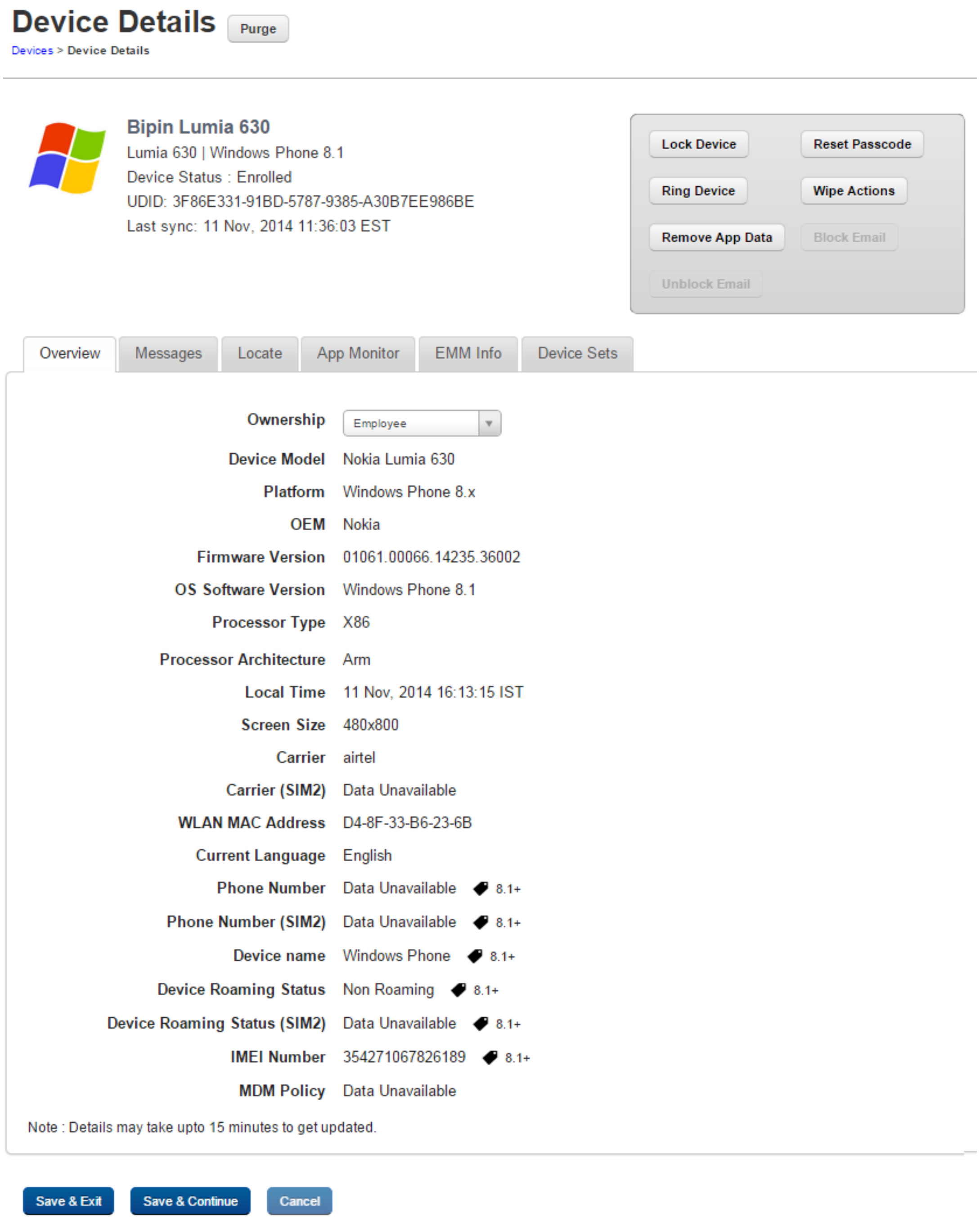
  OR

  To remain on the same page to do other changes immediately, click the **Save and Continue** button.In the confirmation message that appears, click OK to continue.

- Click the **MDM Policy** button to view the policies applied to the device.For more details, refer Device List

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

Overview - Windows Phone 8.x



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

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

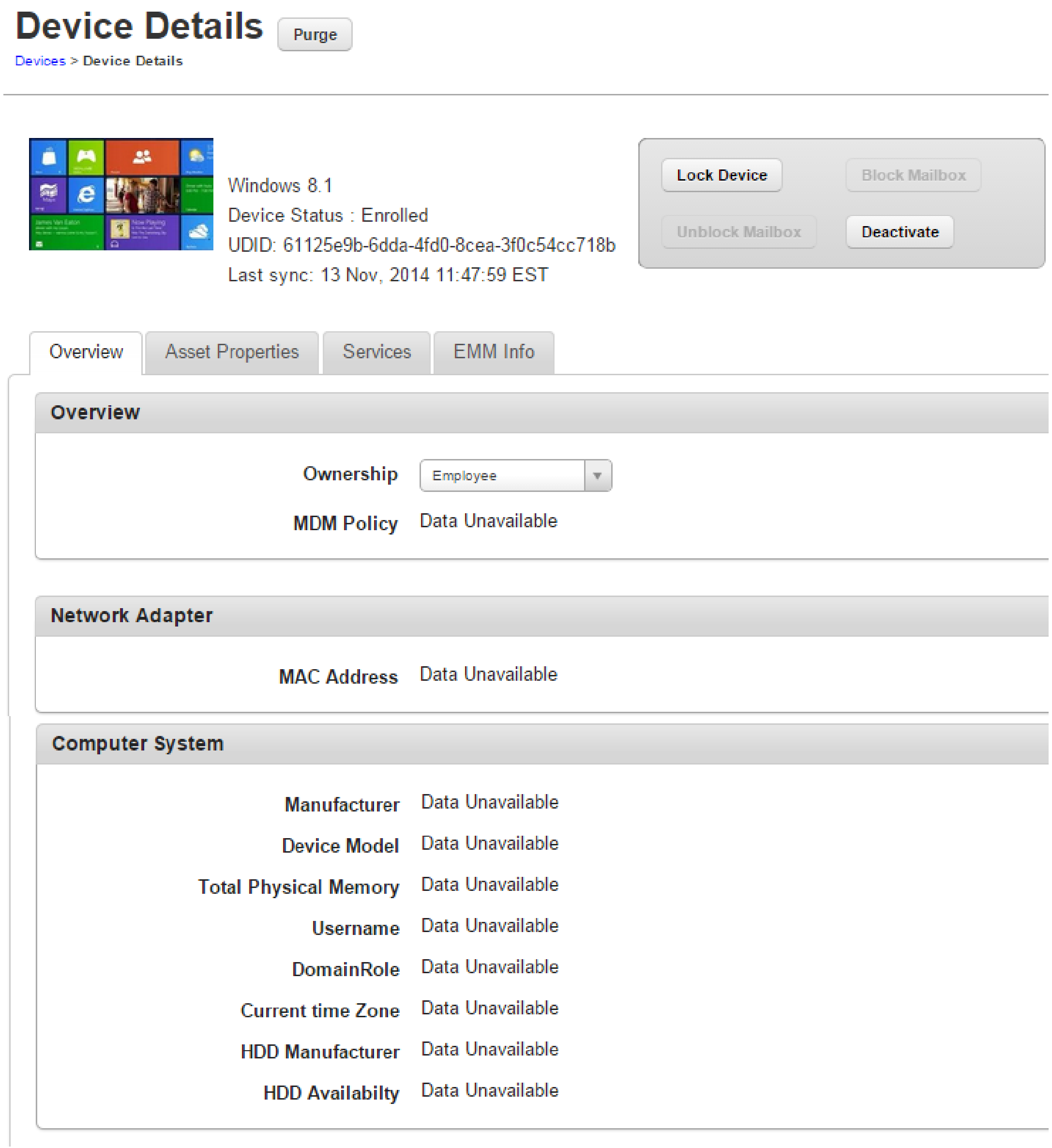
Note : Details may take upto 15 minutes to get updated.

Overview:

- **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.

Overview - Windows 8.1



Device Details

Windows 8.1
Device Status : Enrolled
UDID: 61125e9b-6dda-4fd0-8cea-3f0c54cc718b
Last sync: 13 Nov, 2014 11:47:59 EST

Overview

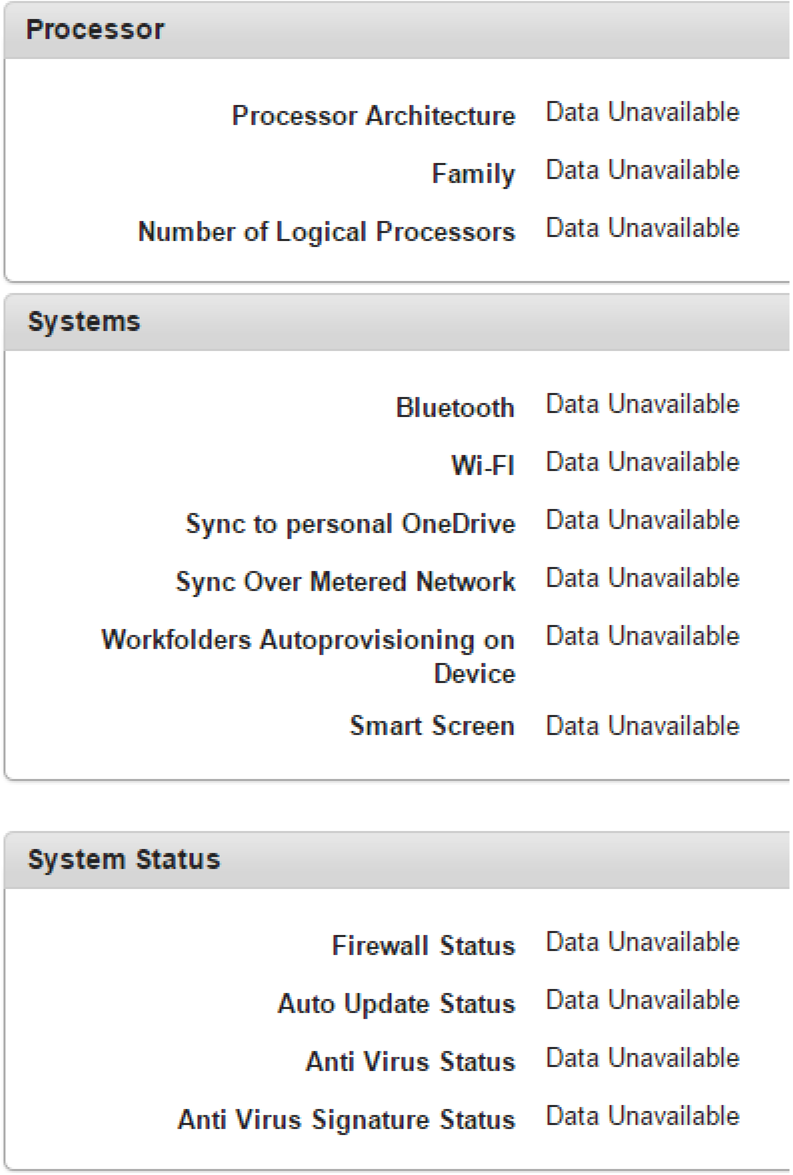
Ownership	Employee
MDM Policy	Data Unavailable

Network Adapter

MAC Address	Data Unavailable

Computer System

Manufacturer	Data Unavailable
Device Model	Data Unavailable
Total Physical Memory	Data Unavailable
Username	Data Unavailable
DomainRole	Data Unavailable
Current time Zone	Data Unavailable
HDD Manufacturer	Data Unavailable
HDD Availabilty	Data Unavailable



Processor

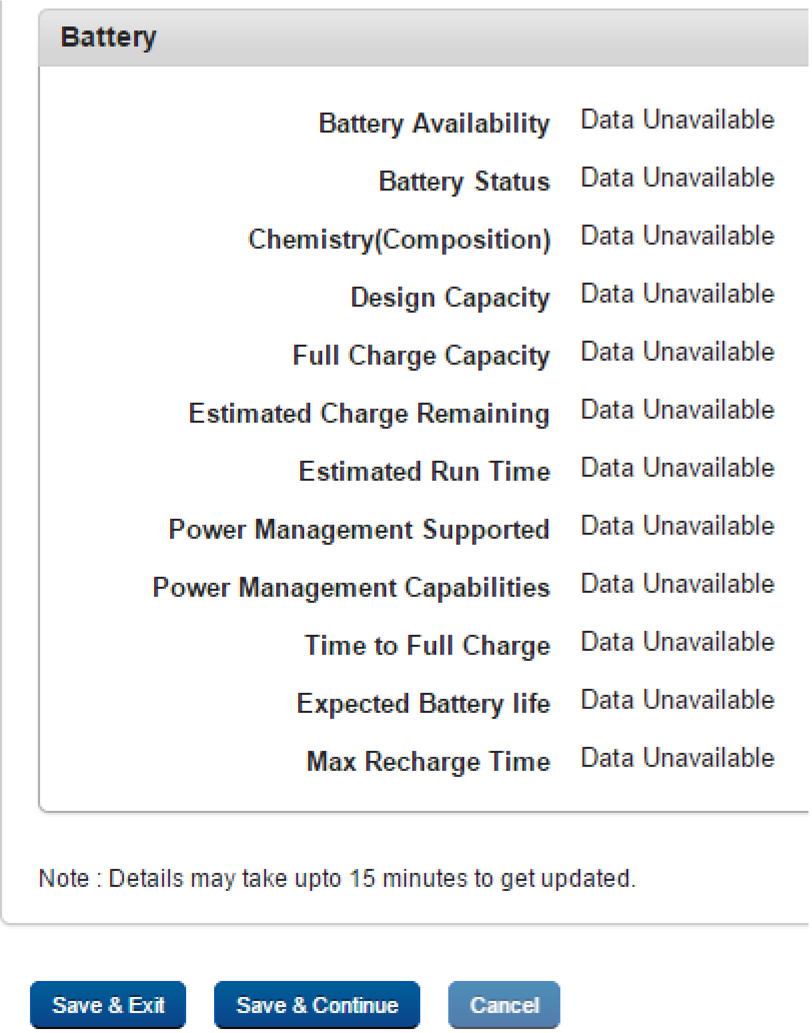
Processor Architecture	Data Unavailable
Family	Data Unavailable
Number of Logical Processors	Data Unavailable

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.

- **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.

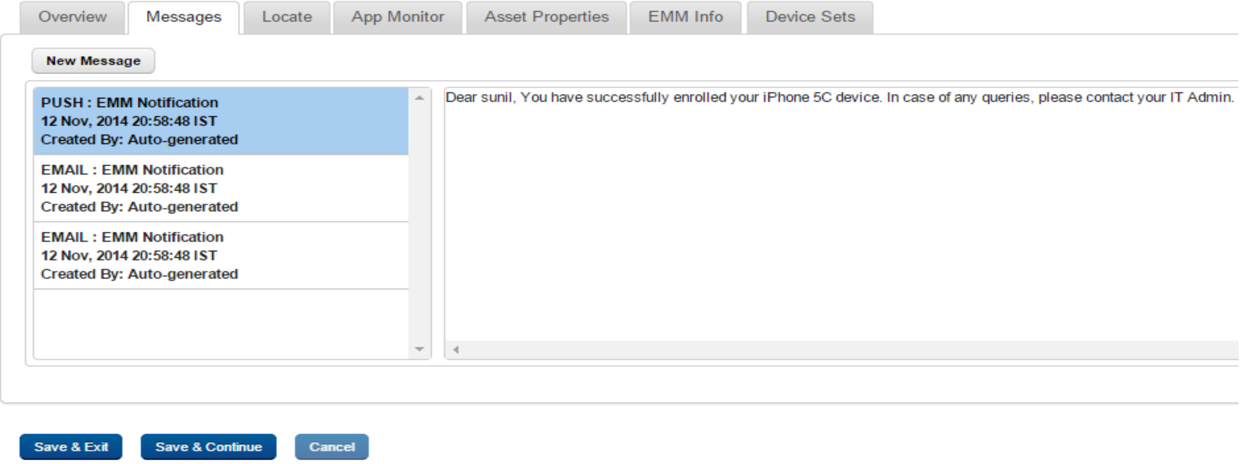
- **Username**: Displays username of the device user.
- **DomainRole**: Displays details of domain role of the device.
- **Current time Zone**: Displays the local time zone details of the device.
- **HDD Manufacturer**: Displays details of the HDD manufacturer.
- **HDD Availability**: Displays details 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 synched 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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

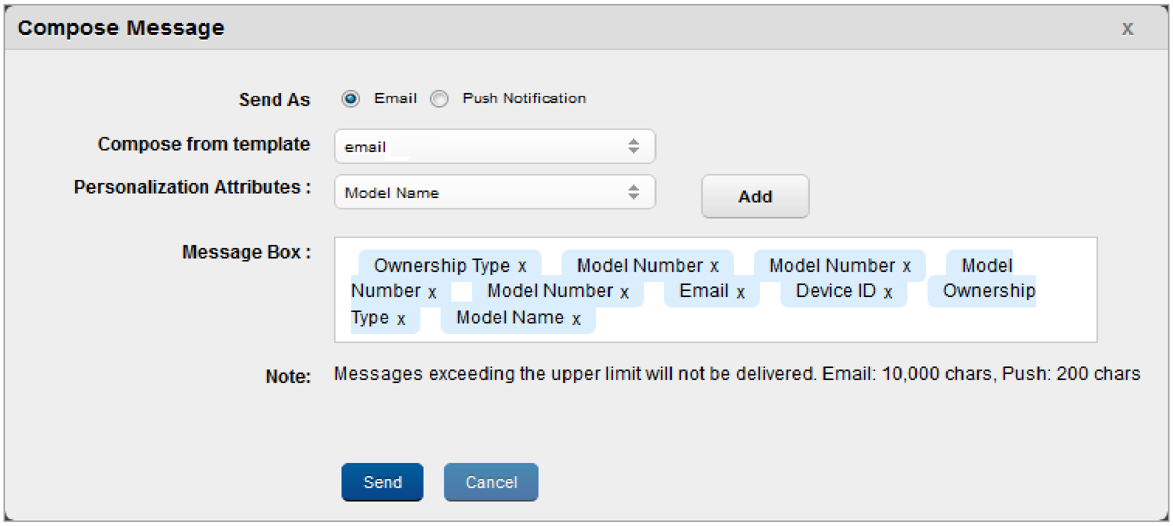
EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

To compose a message, follow these steps:

1. Click the **New Message** button to open the **Compose Message** window. Enter the following details:



Send As ● Email ○ Push Notification

Compose from template: email

Personalization Attributes : Model Name

Message Box : Ownership Type x Model Number x Model Number x Model Number x Model Number x Email x Device ID x Model Ownership Type x Model Name x

Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

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.

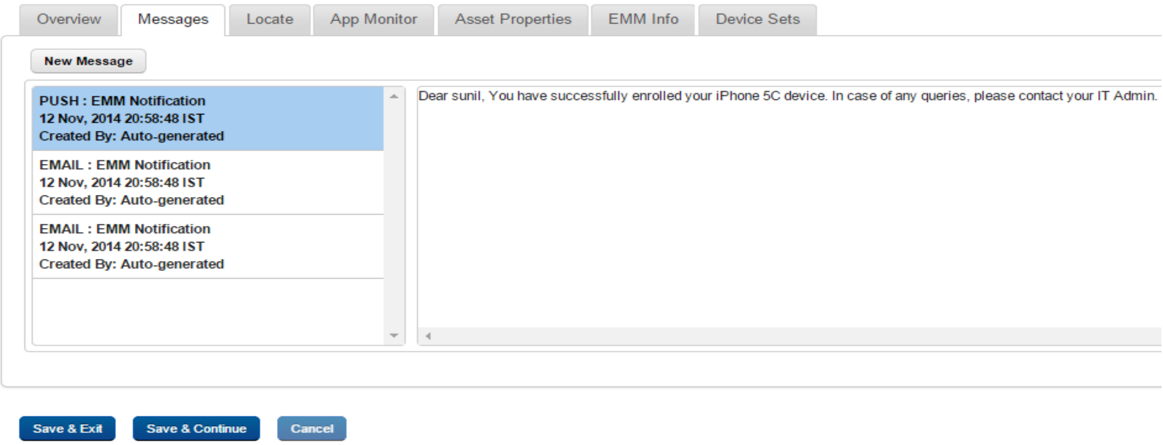
   To automate the work-flow process, you create message templates under Device Settings > Message Templates section. You can access these messages in Compose Message window through Compose from Template dropdown list.

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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

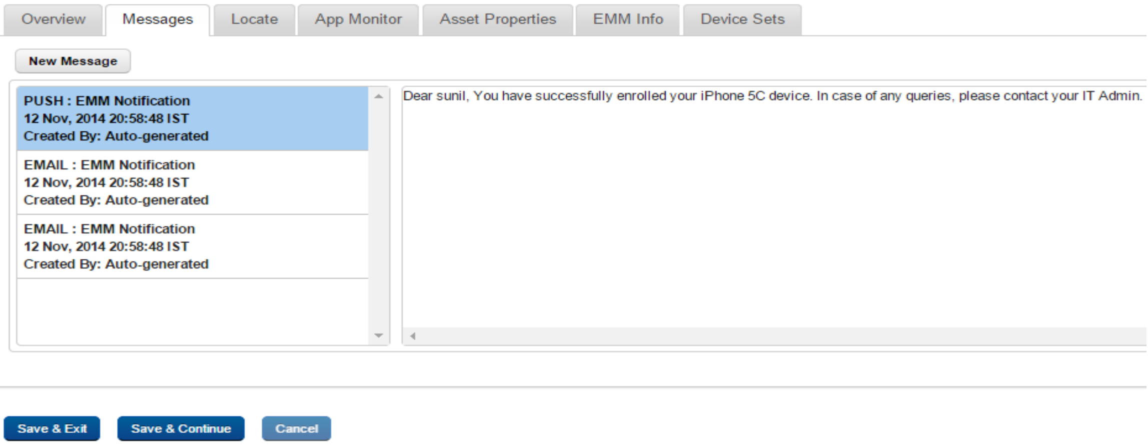
Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

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.



PUSH : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

EMAIL : EMM Notification
12 Nov, 2014 20:58:48 IST
Created By: Auto-generated

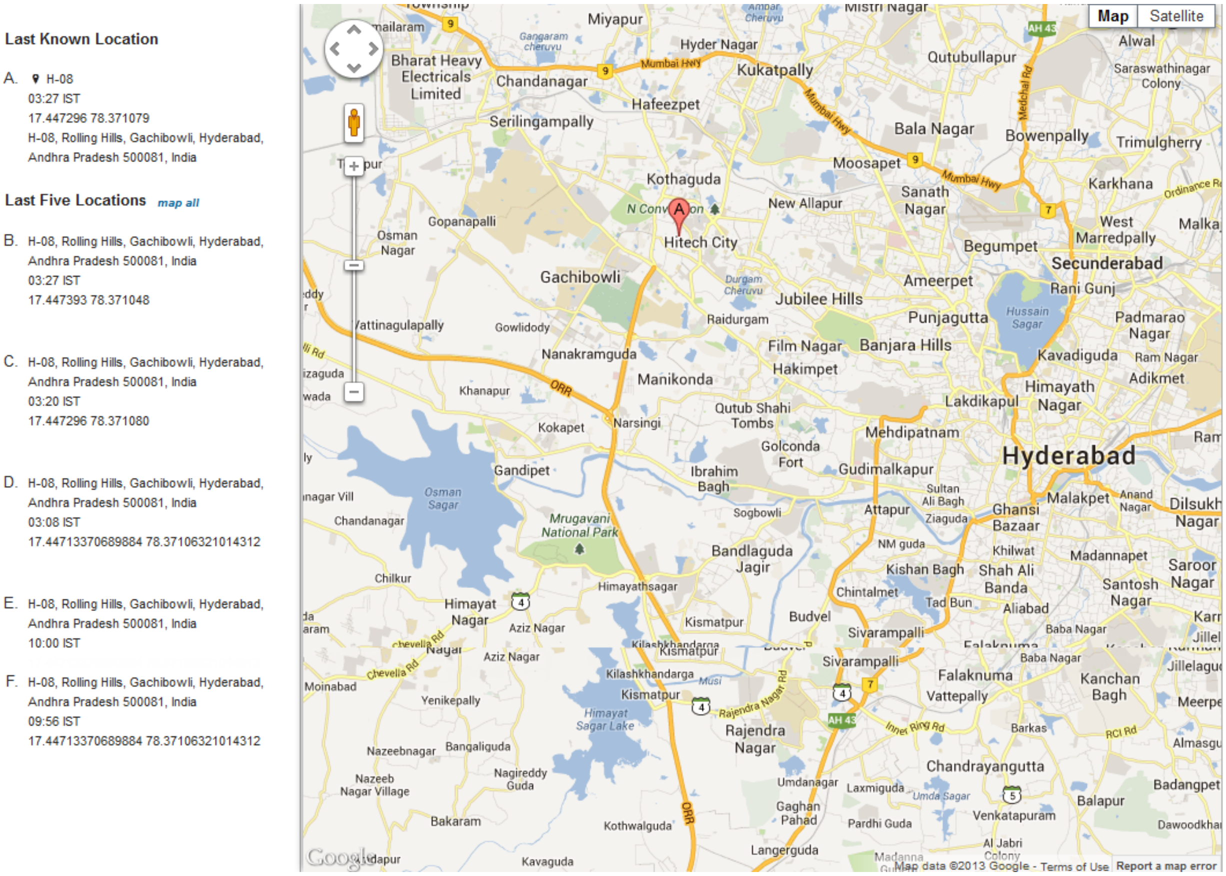
Dear sunil, You have successfully enrolled your iPhone 5C device. In case of any queries, please contact your IT Admin.

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.

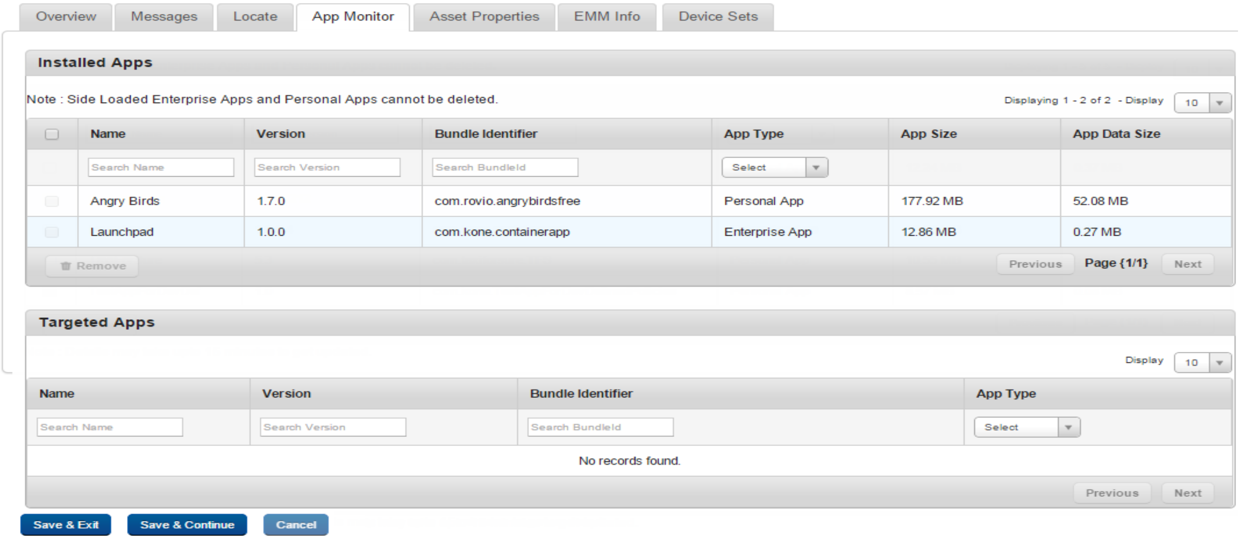
There are three types of Apps.

- Enterprise Applications: Apps which are published into Enterprise Store are known as Enterprise Apps. These can be deleted by the Administrator, if they are downloaded through the Enterprise Store. They cannot be deleted in iOS devices if they are side-loaded.

- Personal Applications: Apps which are downloaded through Public Apps store like Apple App Store or Google App Store are considered as Personal Apps. If Whitelisted apps are installed by a User from the Apple App Store or Google Play, they are considered as Personal apps as they are not pushed by the EMM Server. These apps cannot be deleted.
- Managed Apps: Public Apps pushed through EMM are considered as Managed Apps. They can be deleted.

For Windows 6.x devices, none of the apps can be removed remotely.

App Monitor for iOS



Installed Apps

Note : Side Loaded Enterprise Apps and Personal Apps cannot be deleted.

Displaying 1 - 2 of 2 - Display 10

□	Name	Version	Bundle Identifier	App Type	App Size	App Data Size
	Search Name	Search Version	Search BundleId	Select		
□	Angry Birds	1.7.0	com.rovio.angrybirdsfree	Personal App	177.92 MB	52.08 MB
□	Launchpad	1.0.0	com.kone.containerapp	Enterprise App	12.86 MB	0.27 MB

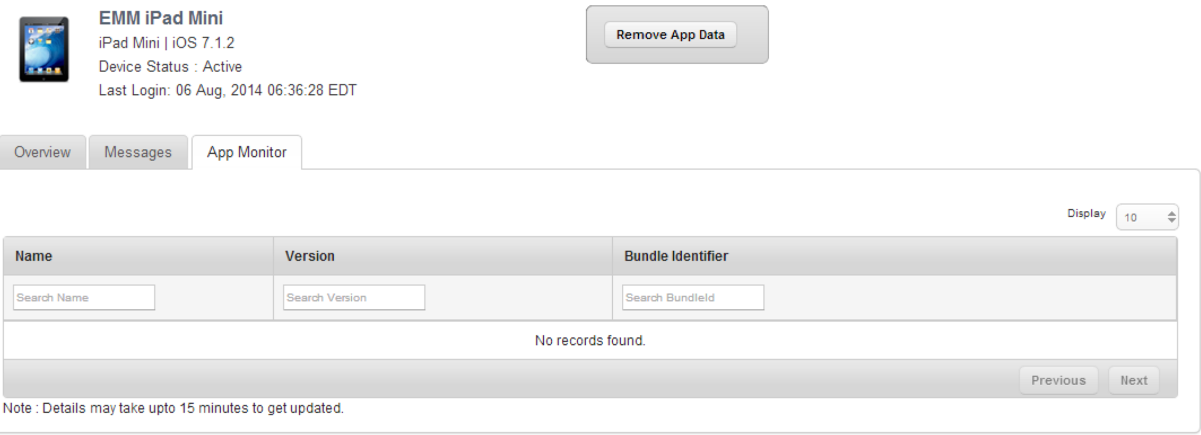
Page {1/1}

Targeted Apps

Display 10

Name	Version	Bundle Identifier	App Type
Search Name	Search Version	Search BundleId	Select

No records found.


EMM iPad Mini
iPad Mini | iOS 7.1.2
Device Status : Active
Last Login: 06 Aug, 2014 06:36:28 EDT

Display 10

Name	Version	Bundle Identifier
Search Name	Search Version	Search BundleId

No records found.

Note : Details may take upto 15 minutes to get updated.

The App Monitor list view for iOS has the following details:

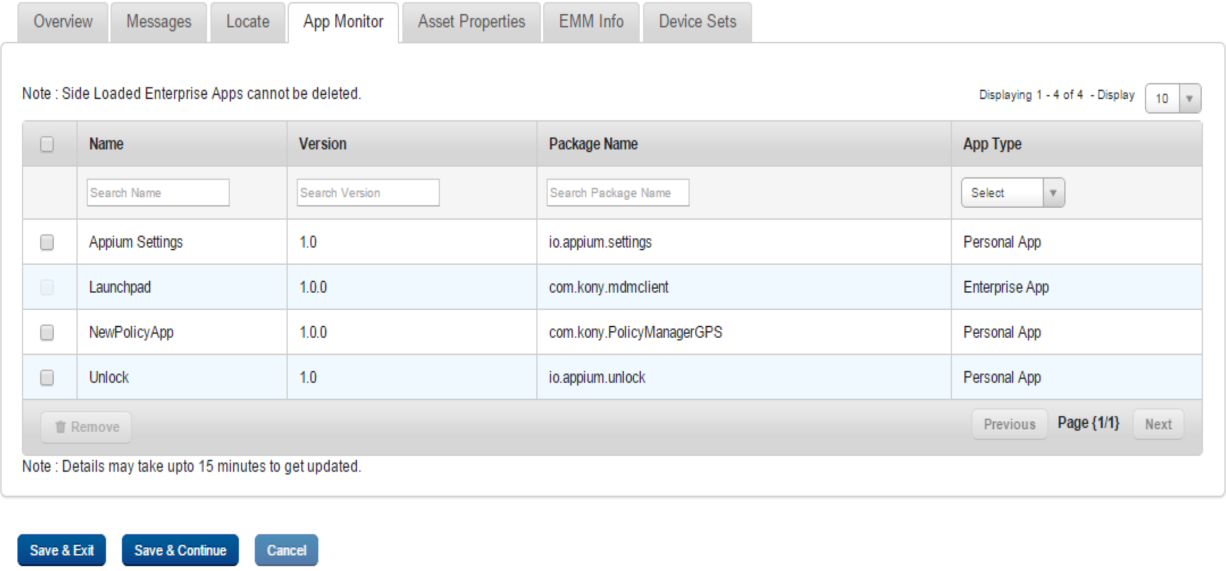
- **Name**: Displays the Name of the application.
- **Version**: Displays the Version of the application.
- **Bundle Identifier**: Displays the bundle ID of the application.

> *Note:* In the App Monitor tab for iOS, Publisher has been replaced with Bundle Identifier.

- **App Type**: Displays the type of the application.
- **App Size**: Displays the size of the installed application.
- **App Data Size**: Displays the size of the data in the application.

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.

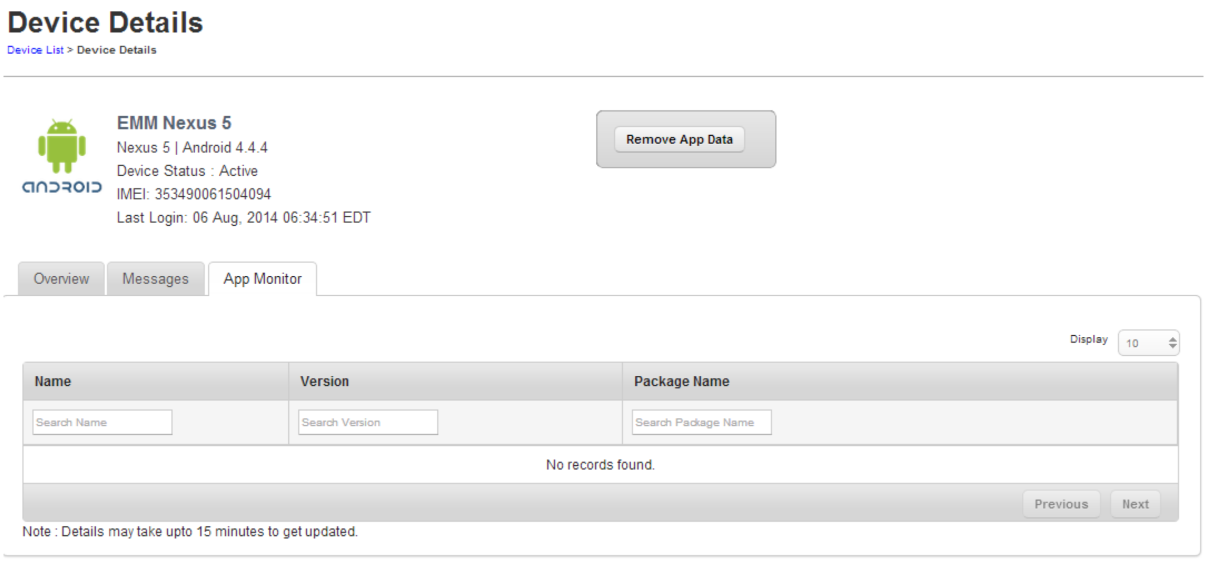


Note : Side Loaded Enterprise Apps cannot be deleted.

Displaying 1 - 4 of 4 - Display 10

□	Name	Version	Package Name	App Type
	Search Name	Search Version	Search Package Name	Select
□	Appium Settings	1.0	io.appium.settings	Personal App
□	Launchpad	1.0.0	com.kony.mdmclient	Enterprise App
□	NewPolicyApp	1.0.0	com.kony.PolicyManagerGPS	Personal App
□	Unlock	1.0	io.appium.unlock	Personal App

Note : Details may take upto 15 minutes to get updated.



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

Name	Version	Package Name
Search Name	Search Version	Search Package Name
No records found.		

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.

> ***Note:*** In the App Monitor tab for Android, Publisher has been replaced with Package Name.

4. **App Type**: Displays the type of the application.
5. **App Status**:Displays the status of the application.
6. **App Running**: Displays whether the application is running or not running. The administrator can change App Running status remotely.
7. **App Uninstallation Mode**: Displays whether the uninstallation of the application is allowed or not on the device.
8. **Actions**: An administrator can perform additional tasks available in the drop-down list.

Based on several combinations with App Status, App Running, and App Uninstallation Mode, the actions are shown in the **Actions** drop-down list.

- If App Status is Enabled, the system displays available action as Disable App in the **Actions**. An administrator can disable or enable the app.
- If an app running is running, an administrator can stop the app by selecting the Stop App in the **Actions** drop-down list. An administrator can start or stop an app based on the running status.
- If an app is Not Allowed for uninstallation, an administrator can allow user to uninstall the app by selecting the Allow Uninstallation in the **Actions** drop-down list. An administrator can allow or deny user to uninstall an app based on the uninstallation mode status.

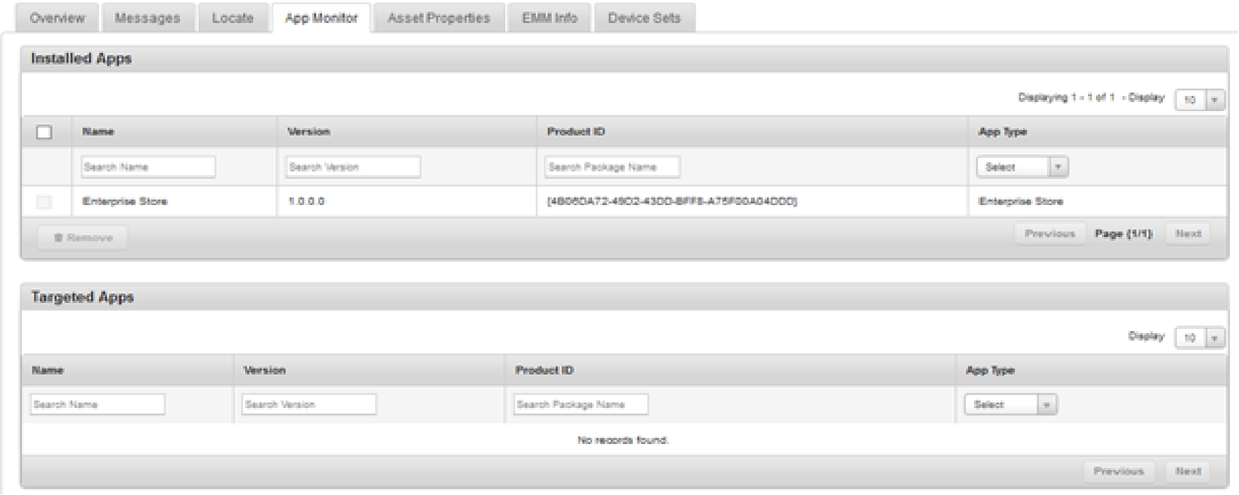
The following table shows the list of actions present with different possible conditions.

If			Then, the system displays the following actions
App Status	App Running	App Uninstallation Mode	
Enabled	Yes	Allowed	• Disable App • Stop App • Disallow Uninstallation
Enabled	No	Not Allowed	• Disable App • Start App • Allow Uninstallation

If			Then, the system displays the following actions
App Status	App Running	App Uninstallation Mode	
Disabled	No	Allowed	• Enable App • Disallow Uninstallation
Disabled	No	Not Allowed	• Enable App • Allow Uninstallation

9. The Admin can get more information of an application. To view more information, hover your mouse on an app under the **Name** column. The system displays the following information shown below:
   - App Cache Size (in MB)
   - App Data Size (in MB)
   - App CPU Usage (in %)
10. According to your search filters criteria, the list view is updated with respective applications details.

App Monitor for Windows Phone 8



Installed Apps

Displaying 1 - 1 of 1 - Display 10

□	Name	Version	Product ID	App Type
	Search Name	Search Version	Search Package Name	Select
□	Enterprise Store	1.0.0.0	{4B06DA72-49D2-43DD-BFF8-A75F00A04DDD}	Enterprise Store

Page (1/1)

Targeted Apps

Display 10

Name	Version	Product ID	App Type
Search Name	Search Version	Search Package Name	Select

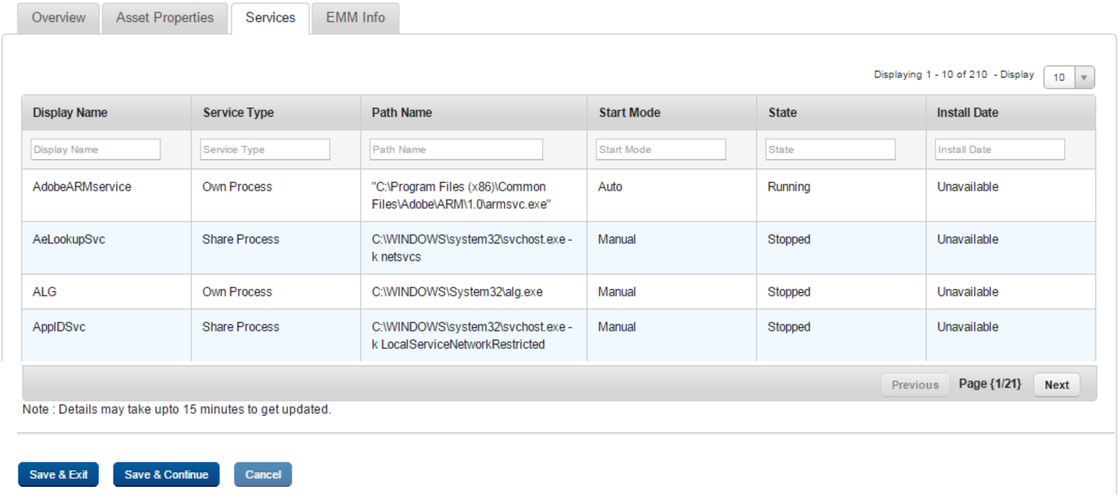
No records found.

The App Monitor list view for Windows Phone 8 has the following details:

- **Name**: Displays the name of the application.
- **Version**: Displays the version of the application.
- **Product ID**: Displays the product ID of the application.
- **App Type**: Displays the type of the application.

Services for Windows 8.1

For Windows 8.1 devices, Asset Properties tab is replaced with Services tab.



Displaying 1 - 10 of 210 - Display 10

Display Name	Service Type	Path Name	Start Mode	State	Install Date
Display Name	Service Type	Path Name	Start Mode	State	Install Date
AdobeARMservice	Own Process	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"	Auto	Running	Unavailable
AeLookupSvc	Share Process	C:\WINDOWS\system32\svchost.exe -k netsvcs	Manual	Stopped	Unavailable
ALG	Own Process	C:\WINDOWS\System32\alg.exe	Manual	Stopped	Unavailable
AppIDSvc	Share Process	C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted	Manual	Stopped	Unavailable

Page (1/21)

Note : Details may take upto 15 minutes to get updated.

The Services list view for Windows 8.1 has the following details:

- **Display Name**: Displays the name of the service.
- **Service Type**: Displays the service type.
- **Path Name**: Displays path name.
- **Start mode**: Displays whether the service starts automatically or manually.
- **State**: Displays details on the running status of the service.
- **Install Date**: Displays the date on that the service is installed.

Removing an App

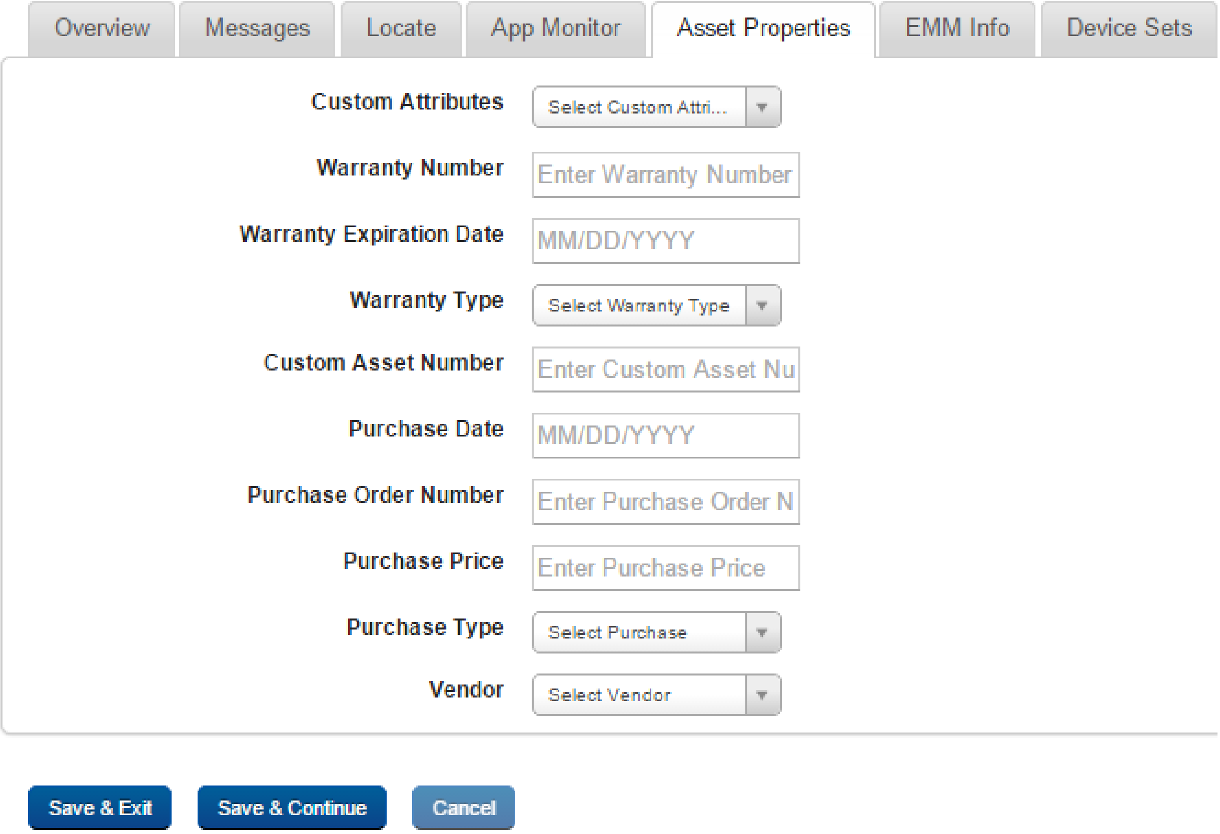
To remove an app, follow these steps:

1. Select the check box next to the app name in the list view.
2. Click the **Remove** button. In the confirmation message **(Remove Application)** that appears, click the **OK** button to return to the details page.
3. Click the **Save and Exit** button.In the confirmation message (**Device details**) that appears, click the **OK** button. The updated device is displayed in the list view.
4. Click the **Save and Continue** button to remain on the same page to update other details.

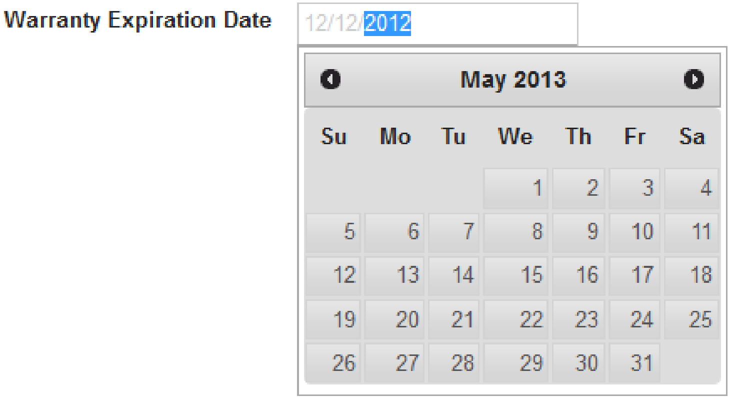
> ***Note:*** You can not remove any child apps from the devices manually.

Asset Properties

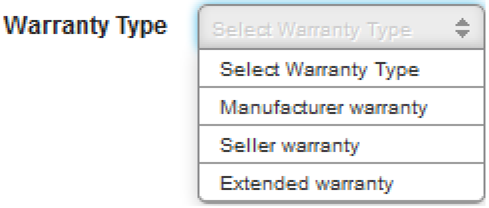
You can view and update the Asset Properties as captured during device enrollment. You can update the asset details through Asset Properties tab.



1. To perform the updates, follow these steps:
   a. **Custom Attributes**: Select a custom attribute you want to add from the list.
   b. **Warranty Number**: Enter Warranty Number in the **Enter Warranty Number** text field.
   c. **Warranty Expiration Date**: Click in the field to open the **Calendar window** to select the warranty expiration date.



Click the required date in the calendar. The selected date appears in the date field.



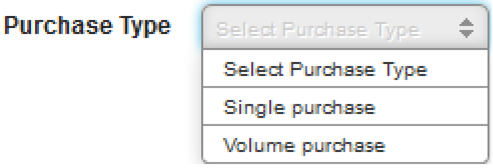
d. **Warranty Type**: Select the required warranty type from the dropdown list.

e. **Custom Asset Number**: Enter the custom asset number in the text field.

f. **Purchase Date**: Click in the field to open **Calendar window** to select the warranty expiration date.

g. **Purchase Order Number**: Enter the purchase order number in the text field.

h. **Purchase Price**: Enter the price of the asset.



i. **Purchase Type:** Select the appropriate purchase type from the dropdown list.

j. **Vendor**: Select the correct vendor from the dropdown list.

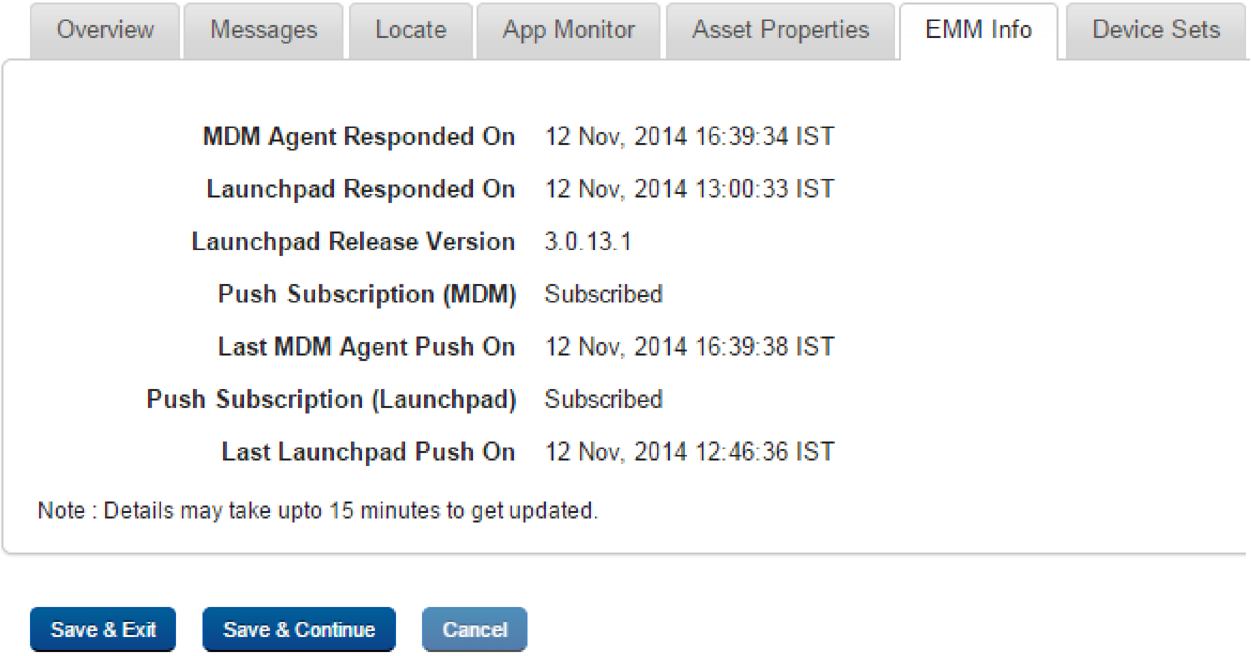
2. Click the **Save and Continue** button. In the confirmation message (Save Device Details - Success)that appears, click OK to continue.

   OR

3. Click the **Save and Exit** button to save the updates and exit the page.

EMM Info

You can view EMM Info as captured during device enrollment.



MDM Agent Responded On	12 Nov, 2014 16:39:34 IST
Launchpad Responded On	12 Nov, 2014 13:00:33 IST
Launchpad Release Version	3.0.13.1
Push Subscription (MDM)	Subscribed
Last MDM Agent Push On	12 Nov, 2014 16:39:38 IST
Push Subscription (Launchpad)	Subscribed
Last Launchpad Push On	12 Nov, 2014 12:46:36 IST

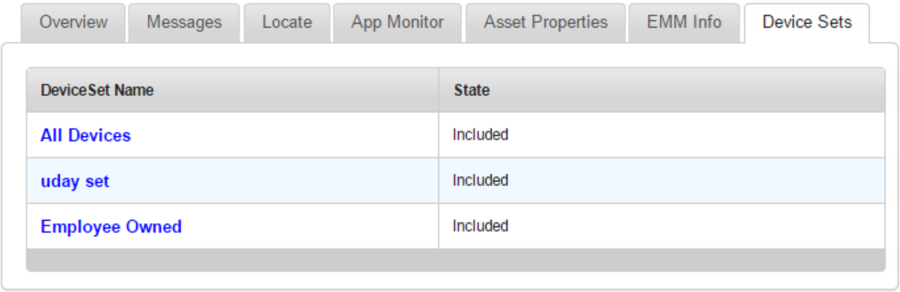
Note : Details may take upto 15 minutes to get updated.

- **MDM Agent Responded On**: Displays details about when the MDM agent responded.
- **Enterprise Store Responded On**: Displays details on when Enterprise Store responded.
- **Enterprise Store Release Version**: Displays Enterprise Store release version number.
- **Push Subscription (MDM)**: Displays whether MDM push is subscribed.
- **Last MDM Agent Push On**: Displays details on when the last MDM agent push occurred.
- **Push Subscription (Enterprise Store)**: Displays whether Enterprise Store push is subscribed.

- **Last Enterprise Store Push On**: Displays details on when the last Enterprise Store push occurred.

Device Sets

The Device Sets tab displays device set names the device belongs to.



DeviceSet Name	State
All Devices	Included
uday set	Included
Employee Owned	Included

- **Device Set Name**: Name of the device set.
- **State**: Displays the device state. The state can be included or excluded. The included state denotes that the device adheres to policies of the device set. The excluded state means that the device is excluded from all policies of the device set.

10.6.3.2 Device Details Page Actions

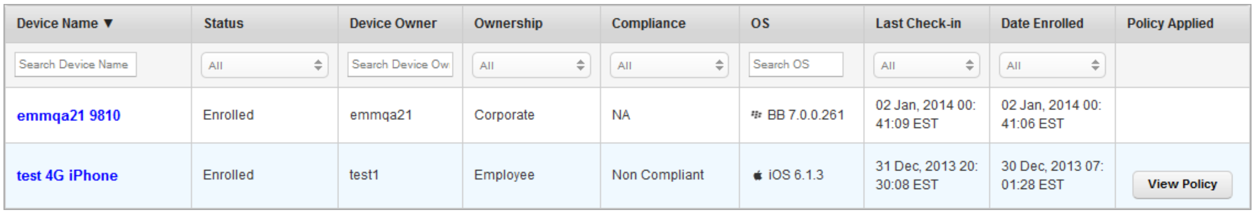
You can perform the following activities from Device List page.

- Searching for Devices
- Updating Device Details
- Locking a Device
- Device Passcode
- Remove App Data
- Block Email Access on Device
- Allow Email Access on Device

- Power Off Device (For Android)
- Disable Sim Pin Lock (For Android)
- Enable Sim Pin Lock (For Android)
- Resume Device
- Start Mirroring
- Stop Mirroring
- Force Check-in
- Purge

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 ▼	Status	Device Owner	Ownership	Compliance	OS	Last Check-in	Date Enrolled	Policy Applied
Search Device Name	All	Search Device Ow	All	All	Search OS	All	All	
emmqa21 9810	Enrolled	emmqa21	Corporate	NA	BB 7.0.0.261	02 Jan, 2014 00:41:09 EST	02 Jan, 2014 00:41:06 EST	
test 4G iPhone	Enrolled	test1	Employee	Non Compliant	iOS 6.1.3	31 Dec, 2013 20:30:08 EST	30 Dec, 2013 07:01:28 EST	View Policy

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. **Compliance**: Select the required compliance type from the dropdown list.

f. **OS**: Enter desired operating system version in the **Search OS** text field.

g. **Last Check-in** : Select the date on which the device was last checked-in to EMM from the dropdown list.

h. **Date Enrolled**: Select the date on which the device was enrolled to EMM from the dropdown list.

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.

Updating Device Details

The primary purpose to update a device details is to fulfill the requirement of existing business rules. To update a device, click the required device in the list view. Update the details for each tab of the device as required. For more information on this, see Device Details section.

Locking a Device

This action is used to lock the selected device in the following circumstances:

- When a Device is thought to be lost or stolen. The device is locked for a duration before the status is decided as Lost.
- The Device is found to be not in compliance with the rules, and can be locked (for Android). The device is locked automatically with the existing passcode.
- If the Device is not issued to any User, the device can be locked.

If Administrator tries to manually take action on the device, Administrator selects a device from the device list and invokes the Lock action.

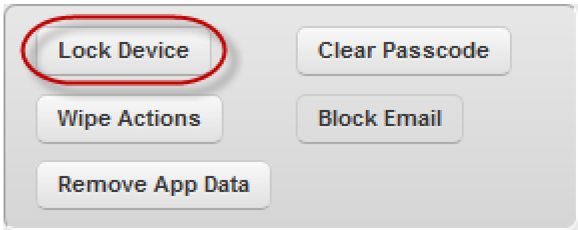
For iOS Devices

In case of iOS devices, the system seeks confirmation from the Administrator about the intention to lock. The Administrator receives a message with options. The administrator has to confirm the action by choosing either to Lock or Cancel the action.

By choosing Lock, the device is locked with the passcode existing on the device.

To lock a device, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.



2. Click the **Lock Device** button next to the Reset Passcode button to open the **Lock Device** window.
    a. **Message**: Enter text that to be appeared on the device.
    b. **Phone Number**: Enter a phone number that to be displayed on the device. Once this number is dialed, your device connects to that number.
3. Click **Lock**. The Lock Device confirmation message appears.
4. Click **OK** to continue .

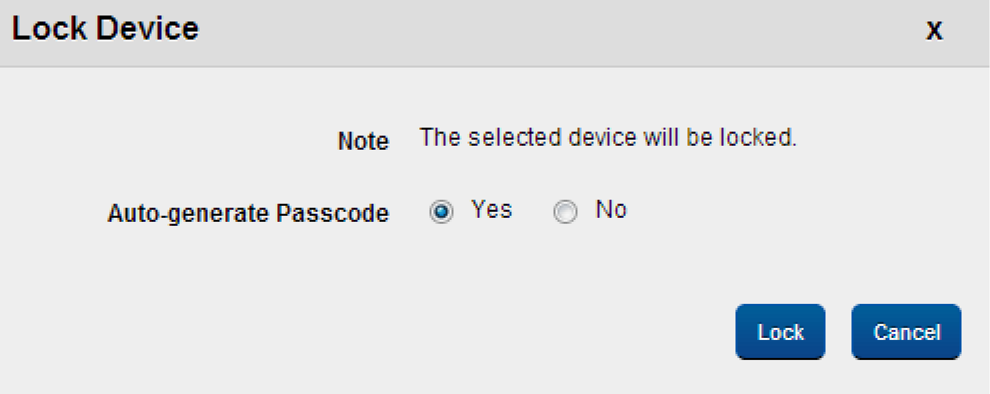
For Android Devices

For Android Devices, the Admin is informed through a message and a choice is provided for the Admin to Auto-Generate the Passcode prior locking the device with the two choices as **Yes** and **No**.

If the Admin chooses to Lock, An automated passcode is generated and applied. The system displays a message confirming that the device has been locked.

If the selected option is No and the Admin chooses to lock, the device is locked with the current passcode. The system displays a message confirming that the device has been locked.

> ***Note:*** Do not use Auto-generate Passcode if you have any other administrator for the device other than EMM.



Note The selected device will be locked.

Auto-generate Passcode ● Yes ○ No

1. Click the **Lock Device** button next to the Reset Passcode button to open the Lock Device window.
2. The Lock Device window appears with the following options:
3. **Auto-generate Passcode**:Click the Lock button. In the confirmation message (Lock Device) that appears, click OK to continue.

Device Passcode

As an Admin, you may require to reset the passcode of a device under following circumstances:

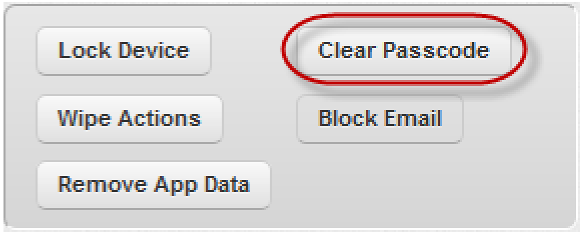
- If the Device User requests it.
- If the Device is missing and yet not declared as Lost.
- If the Device is out of compliance and the administrator wishes to stop any further access to the device temporarily (for Android).
- If the device user is changed.

- If a new Passcode is applied, then the new passcode overrides the existing passcode on the device. The device is automatically locked and you should unlock the device before use it again.
- If the passcode is cleared, no passcode exists on the device for a limited period of time. You need to assign a passcode for the device, which is in compliance with their passcode policy.
- For Android, if you fail to assign a new passcode within the stipulated duration, the system triggers an auto-generated passcode and a lock device command.

Clear Passcode for iOS Devices

To clear the passcode for iOS devices , follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Clear Passcode** button next to Lock Device button.

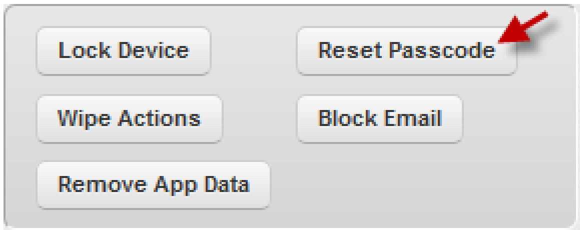
   Clear Passcode window appears with the warning message that if user wishes to clear the passcode, this action will clear the passcode and a new passcode will be generated as per policy.
3. Click Yes to continue.
4. In the confirmation message (Reset Passcode) that appears, click OK to return to the main page.

> *Note:* (For iOS Platform only) When a user is on Passcode lock screen, and at the same moment Administrator initiates the Clear Passcode; the device hangs and the user needs to restart the device.

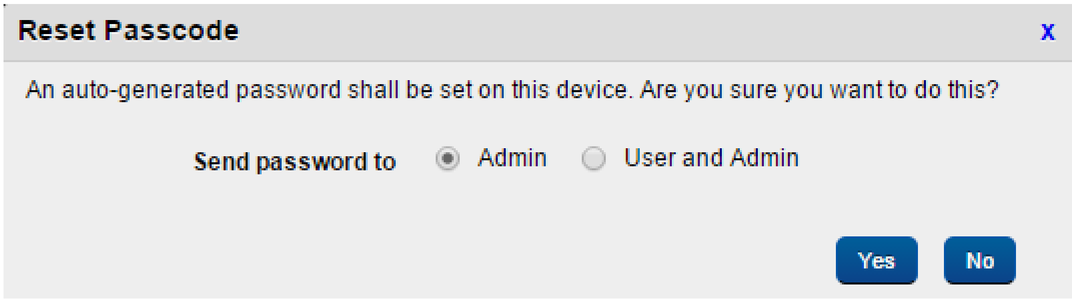
Reset Passcode for Android Devices

To reset the passcode for Android devices, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Reset Passcode** button next to Lock Device button.

   Reset Passcode window appears.

   An auto-generated password shall be set on this device. Are you sure you want to do this?

   Send password to ● Admin ○ User and Admin

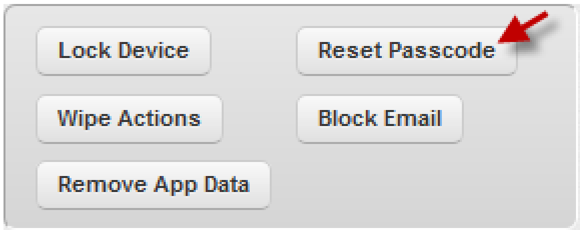
3. **Send password to**: Select where you want to send the reset password. You can choose to end it to the admin alone or to the admin or both admin and the user. By default Send password to is set to **Admin**.
4. Click the **Yes** button. The System displays the confirmation message stating that the request to reset the passcode is successfully submitted and will be executed shortly.
5. Click the **Cancel** button to return to the main page.

Reset Passcode for Windows 8.1 Phone Devices

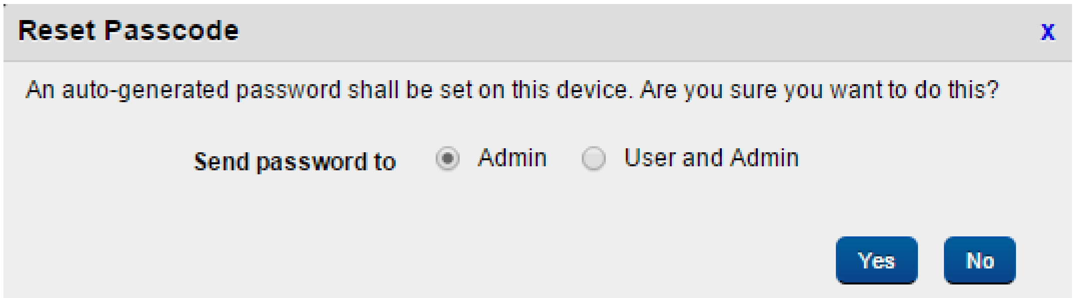
To reset the passcode for Windows 8.1 Phone devices, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.

2. Click the **Reset Passcode** button.



Reset Passcode window appears.



An auto-generated password shall be set on this device. Are you sure you want to do this?

Send password to ● Admin ○ User and Admin

3. **Send password to**: Select where you want to send the reset password. You can choose to end it to the admin alone or to the admin or both admin and the user. By default Send password to is set to **Admin**.

4. Click the **Yes** button. The System displays the confirmation message stating that the request to reset the passcode is successfully submitted and will be executed shortly.

5. Click the **Cancel** button to return to the main page.

Ring Device for Windows Phone 8.x Devices

You can ring a Windows Phone 8.x device using the Ring Device feature.

To ring a Windows Phone 8.x device,

1. Navigate to the Device Details page of the Windows Phone 8.x device you want to ring.

2. Click **Ring Device**. Ring Device confirmation page appears.

3. Click **Ring**. A confirmation message appears stating that the request is submitted.
4. Click **OK**.

Wipe Device

This feature is used to clear the device settings.As an administrator, you may require to wipe the device under several situations:

- If the Device User requests it, for example, the device has become too slow.
- If the Device is missing and yet not declared as Lost.
- The Device is out of compliance and the administrator wishes to stop any further access to the device temporarily.
- If the device user is changed.

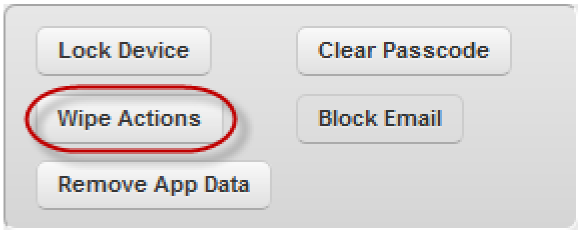
The generic process to wipe a device is as follows:

1. The Admin selects a device, which needs to be wiped.
2. The Admin invokes the Wipe action.
   a. For Corporate owned and Shared devices, two options are available: Enterprise Wipe or Complete Wipe.
   b. For Employee owned devices only Enterprise Wipe can be conducted.
3. Admin defines the Status for the completion of Wipe action. The Status can be Deactivated, Retired, Device Lost or Suspended.

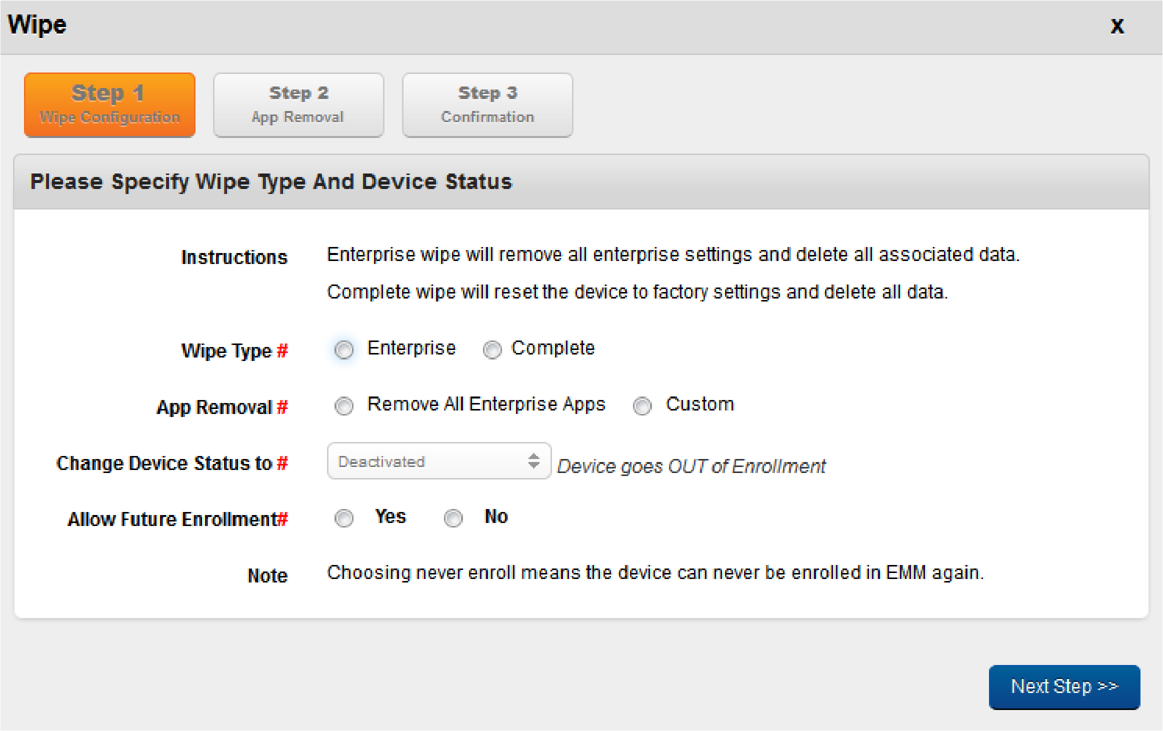
> ***Note:*** If a user tries to re-enroll a completely wiped device listed under Enrollment Denied List, the device displays the Terms and Conditions page, in a loop every time a user tries to login. In Enterprise wiped device it works as expected.

To wipe a device follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. To open the Wipe window, click the **Wipe Actions** button next to the Block Email button.



3. The **Wipe Window** appears. The Wipe window includes three steps to wipe a device.
4. **Step One- Wipe Configuration**:Enter the following details:



Please Specify Wipe Type And Device Status

Instructions: Enterprise wipe will remove all enterprise settings and delete all associated data. Complete wipe will reset the device to factory settings and delete all data.

Wipe Type #: ○ Enterprise ○ Complete

App Removal #: ○ Remove All Enterprise Apps ○ Custom

Change Device Status to #: Deactivated *Device goes OUT of Enrollment*

Allow Future Enrollment#: ○ Yes ○ No

Note: Choosing never enroll means the device can never be enrolled in EMM again.

a. **Wipe Type**: Select the Wipe Type as **Enterprise** or **Complete**.

   If Enterprise Wipe is selected then the selected device is un-enrolled and all enterprise data is deleted through EMM profiles, policies and internal applications.The EMM server still holds control over the device. Enterprise Wipe can be applied on all the devices. enterprise store app data is deleted for iOS but not for Android upon Enterprise wipe.

   If the device is completely wiped, the device should be reset to factory settings. All data on the device - enterprise or personal is deleted. Once this wipe is complete, EMM cannot control the device any longer. Complete Wipe can be applied on Corporate and Shared Devices.

   > *Important:*
   > **(For Employee owned Devices only)**
   > If you select Complete Wipe as Enforcement Action, then Enterprise Wipe with deactivated state is sent to the device.
   >
   > **(For Corporate and Shared Devices)**
   > If you select Complete Wipe as Enforcement Action, then Complete Wipe occurs but future enrollment of the device is not possible.

b. **App Removal**: Click the option as **Remove All Enterprise Apps** or **Custom.**

   App Removal window appears in Step two only, if the Admin selects the option as Custom in App Removal. It is also possible only for Enterprise Wipe only. It is done only when certain apps are meant to be preserved even after the wipe

   You as an Admin should specify to remove all enterprise apps or selectively remove enterprise apps. The default behavior is to remove all the enterprise apps.

c. **Change Device Status to**: Select the device status from the drop-down menu. By default, it is set to **Deactivated,** which you can modify to following options:

   - Deactivated: The device is un-enrolled and the device state is changed to Deactivated. The enrollment rule for this case is Allow Enrollment.

- Retired: The device is un-enrolled and the device state is changed to Retired. The enrollment Rule for this case is Never Enroll.
- Suspended: The device remains enrolled and the device state changes to Suspended. This ensures that Admin still has control over the device. The Admin cannot specify any enrollment Rule.

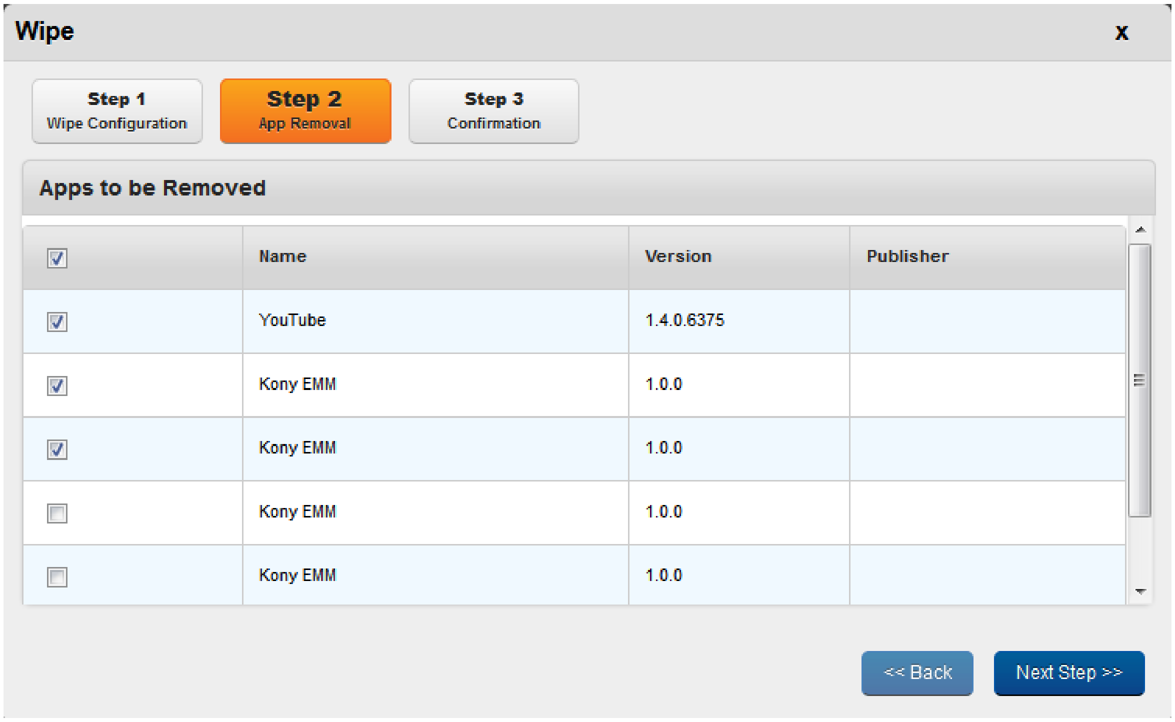
> *Note:* In case a device is suspended, the **Passcode policy** and **Device Restrictions policy** are retained on the device. Rest of all the other policies are removed from the device. However, the device is still expected to be in compliance with the policies assigned to the same.

> *Note:* For Android, when a user ignores Enterprise Wipe request, the system continuously prompts the user until he accepts it to fully wipe Enterprise data from the device. User can ignore Enterprise Wipe request either by clicking the **Cancel** button or the **Home** button.

d. **Allow Future Enrollment**: If you select this option, then a device can be enrolled again. This is applicable for Deactivated, Retired, and Device Lost statuses only.Based on corporate policy and your discretion, you can select to allow enrollment or never enroll the device.

> *Important:* : If you perform Enterprise Wipe and select any of the Device Status available, then Kony EMM enterprise store is not removed from the device, although the specific policies are removed

5. Click the **Next step** button to navigate to **Step No 2**.
6. **Step 2 - App Removal**:By default, all the apps in the list view are selected. If required, deselect the check box adjoining app name to retain it.

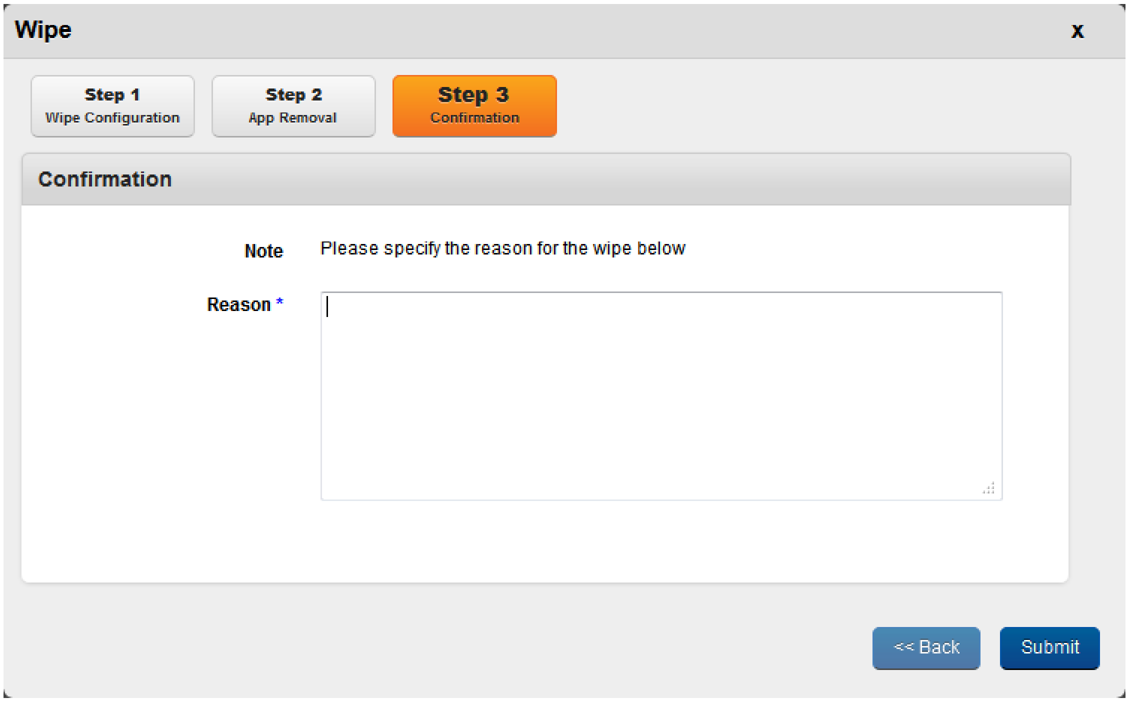


Apps to be Removed

☑	Name	Version	Publisher
☑	YouTube	1.4.0.6375	
☑	Kony EMM	1.0.0	
☑	Kony EMM	1.0.0	
□	Kony EMM	1.0.0	
□	Kony EMM	1.0.0	

> *Important:* EMM enterprise store does not get deleted automatically when the User removes control by deleting the profile.The user is required to delete the Agent,if wishes to enroll again.

7. Click the **Next step** button to navigate to **Step No 3**.
8. **Step 3: Confirmation**: Enter a valid reason for the wipe in the **Reason** Box.



Note Please specify the reason for the wipe below

Reason *

9. Click the **Submit** button. In the confirmation message **(Wipe Device Window)** that appears, click OK to continue.

10. Click OK to return to the main page. When you deactivate or retire the device, system returns to the Device List page. When you suspend the device, system refreshes the Device Details page and displays Resume Device button.

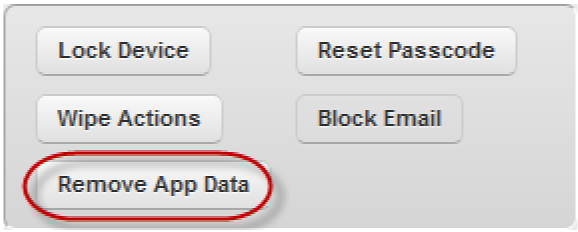
Wipe Device -Windows Phone 8

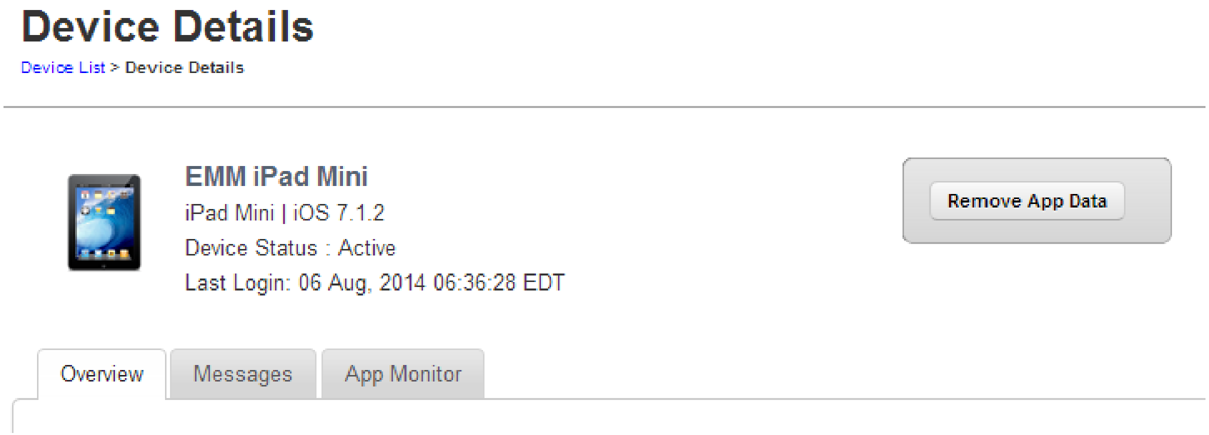
In win Phone 8, we have limitations in identifying control removed state. Win Phone 8 does not report a user initiated disconnection (un-enrollment).

So if a user deletes a company app/account, the user still remains as Enrolled in EMM server. The user can re-enroll with same credentials to resume the provision. If the user tries to re-enroll with different credentials, then the user is wiped after first sync, and previous record (Enrolled state) is marked as suspended.

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.





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.

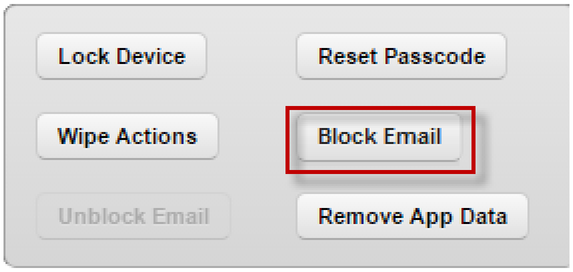
> *Note:* For Windows Phone 8.x devices, the remove app data policy will not work if the app is in use. The policy command will apply when the app is closed and relaunched.

Block Email Access on Device

Block Email action prevents access to the Exchange ActiveSync. Exchange Server must be configured and Exchange Security Services installer must be run on the same. The device must also be assigned an Exchange Account for this feature to work. You cannot view emails from Exchange server again. You may wish to block email for various reasons, for example, if a device connects to a non-prescribed Wi-Fi network.

To block email communication to a device, follow these steps:

1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Block Email** button.



The system displays the warning message (Block Email) asking the user, if really wishes to block email for this device.

3. Click the Block button to block emails for this device. In the confirmation message (Request Sent), click **OK** to return to the page.

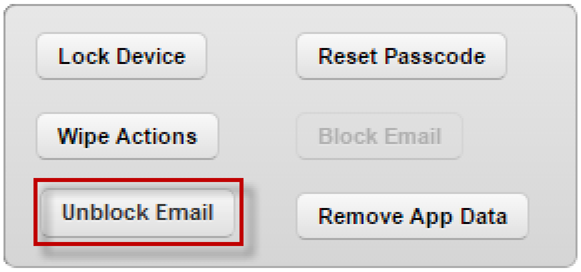
> *Note:*
>
> 1. This option is displayed for AD users only. If you come across any errors, check and ensure that Exchange server is working properly.

> 2. If an already enrolled Local user is overwritten with an AD User then Block Email functionality does not work.
>
> 3. On some Android devices, when Block Email option is initiated, the Native Android email client is not blocked, as Native EAS clients in some Android devices do not share their IMEI numbers with Exchange Server.

Unblock Email

Allowing emails on the device removes it from the list of Blocked devices and automatically allows the device to access Exchange ActiveSync again.

To allow email communication to a device, follow these steps:



1. Click the required device in the list view. The **Device Details** page appears.
2. Click the **Unblock Email** button.
3. The system displays the warning message (Unblock Email) asking the user, if really wishes to unblock email for this device.
4. Click the **Unblock** button to allow emails for this device. In the confirmation message (Request Sent), click **OK** to return to the page.

> ***Note:*** This option is displayed for AD users only. If you come across any errors, check and ensure that Exchange server is working properly. Exchange must be configured and assigned to device for this functionality to work.

Power Off Device (for Android)

Power Off Device feature allows an administrator to remotely power off a device. When the administrator attempts to power off the device, the system displays a confirmation message:"*Are you sure you want to power off the device {$deviceName}?*". Click Yes to confirm if you want to power of the device.

Disable SIM Pin Lock (For Android)

An administrator needs a four digit pin to enable or disable a SIM , which allows the addition or removal of a password protection to the SIM card.

The same administrator who enabled a SIM Personal Identification Number (PIN) lock on a device must disable the locked SIM on the same device. The SIM can neither be locked by another Admin of MDM service, nor it can be unlocked by the same Admin.

Enable SIM Pin Lock (for Android)

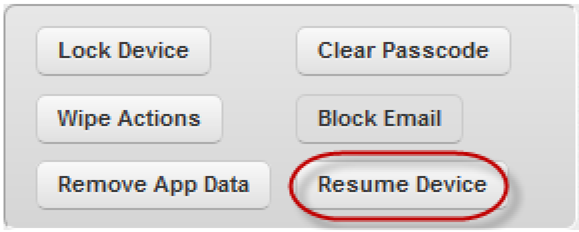
When a user enables a SIM PIN lock, the SIM card is locked and cannot be used until the correct code is entered. That helps protect your account information and other data in case your device is lost or stolen.

When the User moves the SIM to another device, the PIN must be entered. As this Pin is not shared with the User, the usage of the SIM is effectively locked to the device it was locked with. Maximum two attempts for entering pin is allowed.

Resume Device

An administrator may decide to change the status of a suspended device. To bring the device out of suspension, the administrator invokes the Resume action. A suspended device is still enrolled, and the EMM server has full control over the device.

To resume a suspended device, follow these steps:



1. Click the required device in the list view. The Device Details page appears.

   Click the **Resume Device** button.

2. The system displays a warning message (Resume Device) asking the user, if the user really wants to resume this device.

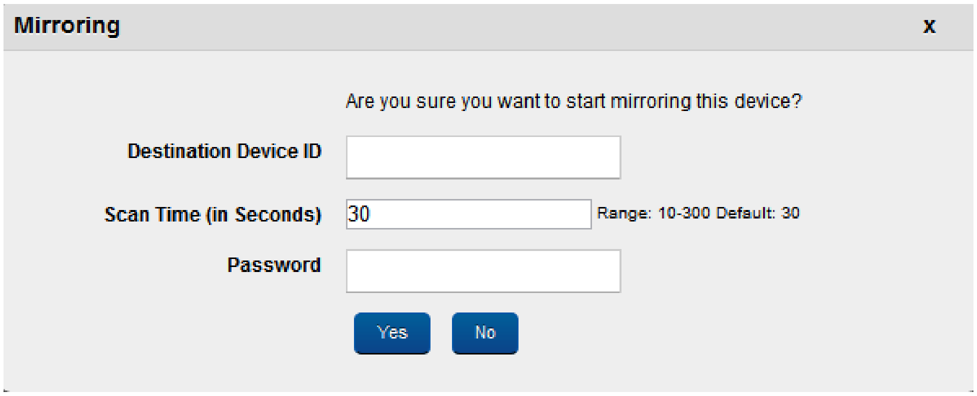
3. Click the **Resume** button to resume the device. In the confirmation message (Resume Device), click OK to return to the page.

Start Mirroring (for iOS7+ Devices)

The Start Mirroring feature is a useful tool to conduct job-related presentations or to display your iPhone photos on a bigger screen. When you enable Start Mirroring, your iOS7+ device can connect with another device, such as an Apple TV or a Mac, and share a screen.

To start mirroring, follow these steps:

1. Click the **Start Mirroring** button. The Mirroring dialog appears.



Mirroring

Are you sure you want to start mirroring this device?

Destination Device ID

Scan Time (in Seconds) 30 Range: 10-300 Default: 30

Password

2. In **Destination Device ID**, enter the WiFi Mac ID of the device.
3. In **Scan Time (in seconds)**, by default the time is set to 30 seconds. You can modify the scan time , which is defined by a range of 10 to 300 seconds. The scan time refers to the time that the device has to find the destination.
4. In **Password**, enter the password to connect the destination.
5. Click **Yes**. The system starts mirroring the device.

Stop Mirroring (for Supervised iOS7+ Devices)

> ***Note:*** If this is applied for non-supervised devices, the command will not execute.

Stop Mirroring allows you stop an Airplay mirroring that is in progress.

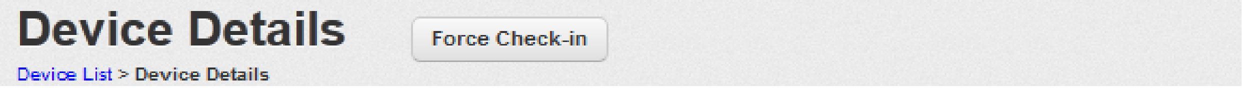
1. To stop airplay mirroring, click **Stop Mirroring** button. The system displays a confirmation message.
2. Click **Yes** to confirm.

Force Check-in

You may wish to view the latest details of the device to analyze its current state and monitor compliance.By invoking this action, the latest device details and compliance states are refreshed and provided.

> ***Note:*** Device Details displays the details according to the last heartbeat (device synchronization with the EMM server).

To perform Force Check-in, follow these steps:



1. Click the **Force Check-in** button next to Device Details label.

2. In the confirmation message (Force Check-in) that appears, click **OK** to return to the main page.

Purge

If a device is inactive for the number of days specified continuously, the device will be automatically purged. The device can then be enrolled again. Purge feature allows an administrator to change the status of a device whose control is removed but is unknown to the server. The administrator can delete the device, and users can then enroll the device on their names.

> ***Note:*** On Android devices, enterprise store from purged devices should be deleted for device re-enrollment. On iOS devices, profile should be deleted on a purged device before it is re-enrolled.

To purge a device,

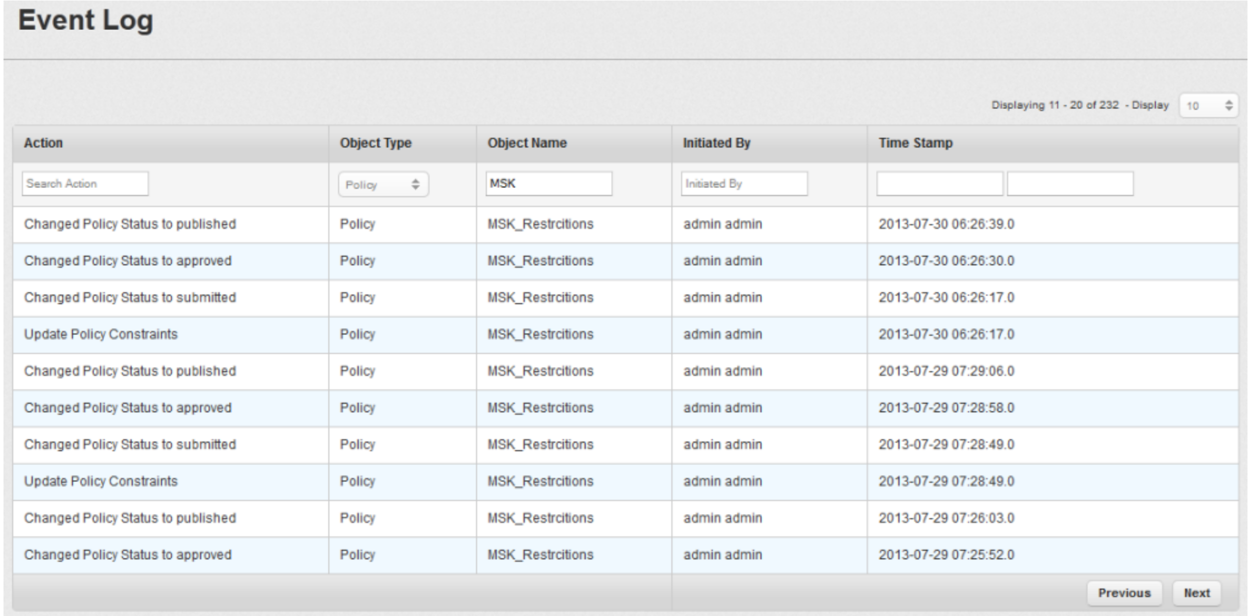
1. In the Device Details page, click **Purge** next to the Device Details label.

2. In the confirmation message (Purge) that appears, click **OK**. Main page appears.

10.7 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

Action	Object Type	Object Name	Initiated By	Time Stamp
Search Action	Policy	MSK	Initiated By	
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:39.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:30.0
Changed Policy Status to submitted	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:17.0
Update Policy Constraints	Policy	MSK_Restrcitions	admin admin	2013-07-30 06:26:17.0
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:29:06.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:58.0
Changed Policy Status to submitted	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:49.0
Update Policy Constraints	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:28:49.0
Changed Policy Status to published	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:26:03.0
Changed Policy Status to approved	Policy	MSK_Restrcitions	admin admin	2013-07-29 07:25:52.0

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.

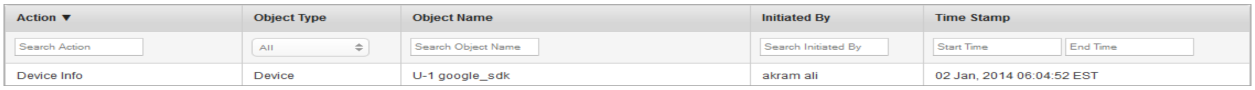
Search Elements Properties	Description
Object Name	Displays a list of the object names.
Initiated By	Displays name of the administrators who initiated action on a device, policy or a device set.
Time Stamp	Displays a list with the duration and the time stamp.

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

- Search Event Log

10.7.1 Search Event Log

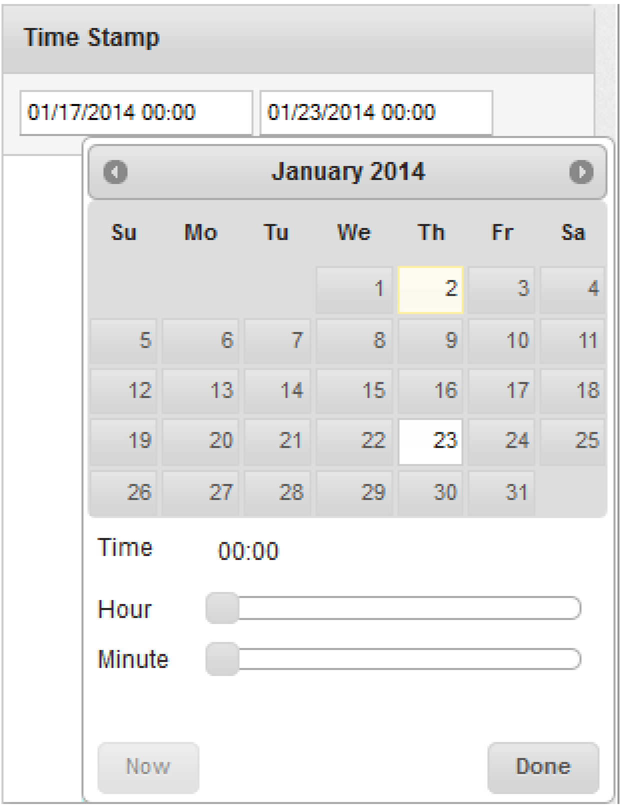
You can search a required action carried out on a device, device set or policy through search filters based on all the grid columns. You can apply a single or a combination of search filters to define the search criteria and get the refined outcome. To search for an action, follow these steps:



Action ▼	Object Type	Object Name	Initiated By	Time Stamp
Search Action	All	Search Object Name	Search Initiated By	Start Time 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.



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.

11. 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.

11.1 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.

11.2 Managing Apps

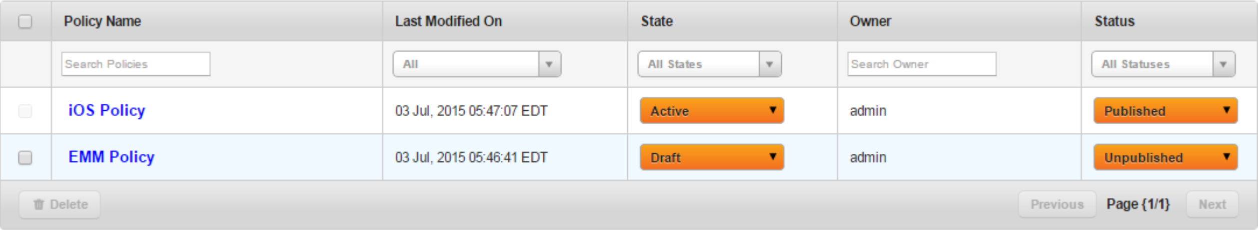
Managing applications includes:

- Policies
- Categories
- Enterprise Apps List
- VPP Apps

11.3 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.



□	Policy Name	Last Modified On	State	Owner	Status
	Search Policies	All ▾	All States ▾	Search Owner	All Statuses ▾
□	iOS Policy	03 Jul, 2015 05:47:07 EDT	Active ▾	admin	Published ▾
□	EMM Policy	03 Jul, 2015 05:46:41 EDT	Draft ▾	admin	Unpublished ▾

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

11.3.1 Creating a New Policy

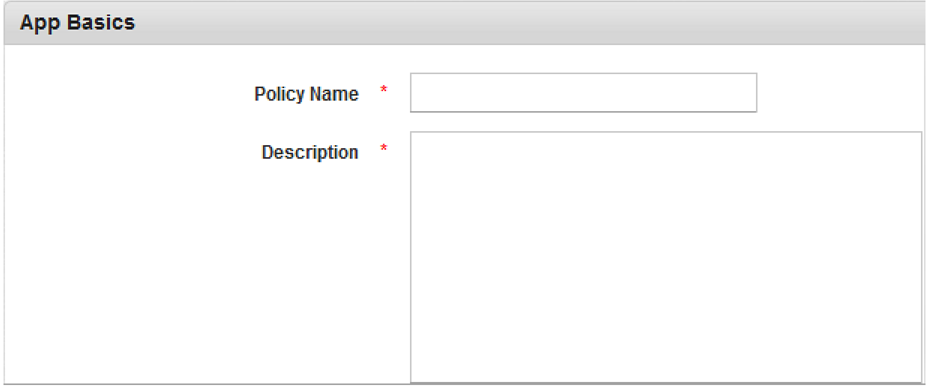
When a new app is enrolled, the administrator must decide if it should be protected by a policy. Click **+New Policy** button on Policies main screen to open **New Policy** screen.

The New Policy screen includes following sections:

- App Basics
- App Usage
- Network
- Storage
- Phone Features

11.3.1.1 App Basics

The app basics section refers to adding a title and description to the new policy. To add app basics, follow these steps:



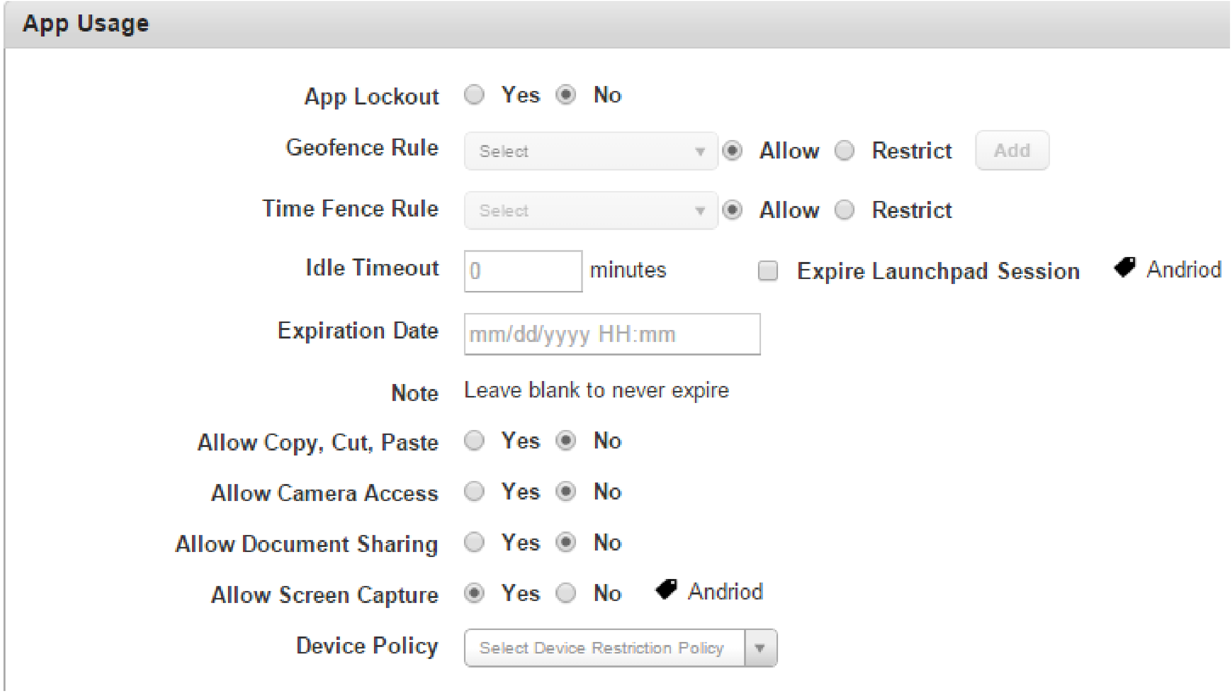
App Basics

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.

11.3.1.2 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 Select ▾ ● Allow ○ Restrict Add

Time Fence Rule Select ▾ ● Allow ○ Restrict

Idle Timeout 0 minutes □ Expire Launchpad Session Andriod

Expiration Date mm/dd/yyyy HH:mm

Note Leave blank to never expire

Allow Copy, Cut, Paste ○ Yes ● No

Allow Camera Access ○ Yes ● No

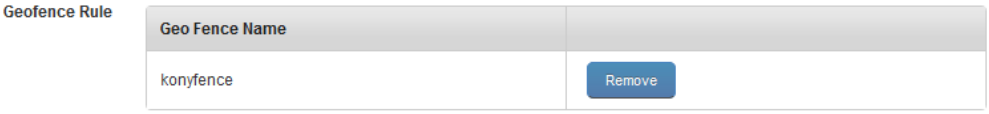
Allow Document Sharing ○ Yes ● No

Allow Screen Capture ● Yes ○ No Andriod

Device Policy Select Device Restriction 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.



Geofence Rule

Geo Fence Name	
konyfence	Remove

   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 enrolled 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.

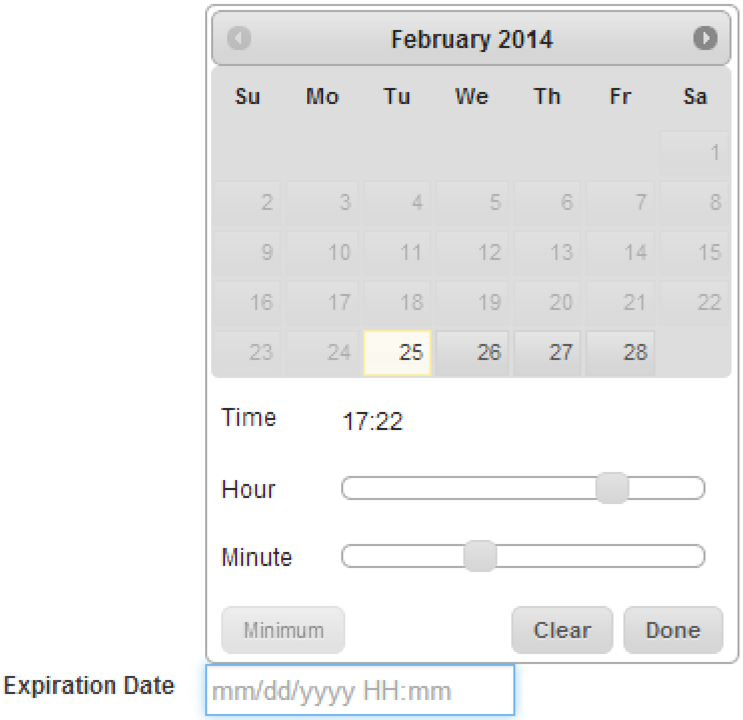
> ***Note:*** If the device is offline mode, user can access the app by changing the device time.
>
> When the device is offline, the device cannot communicate with the EMM server and therefore must rely on device time to implement time related rules. Therefore there is a possibility for the User to manipulate device time to bypass some of the rules.

4. **Idle Timeout:** Set the idle timeout for the device in minutes.

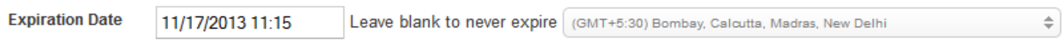
   Idle Time out means that, if the application does not use the connection to the device for scheduled time period, then connection is closed automatically.

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.



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 11/17/2013 11:15 Leave blank to never expire (GMT+5:30) Bombay, Calcutta, Madras, New Delhi

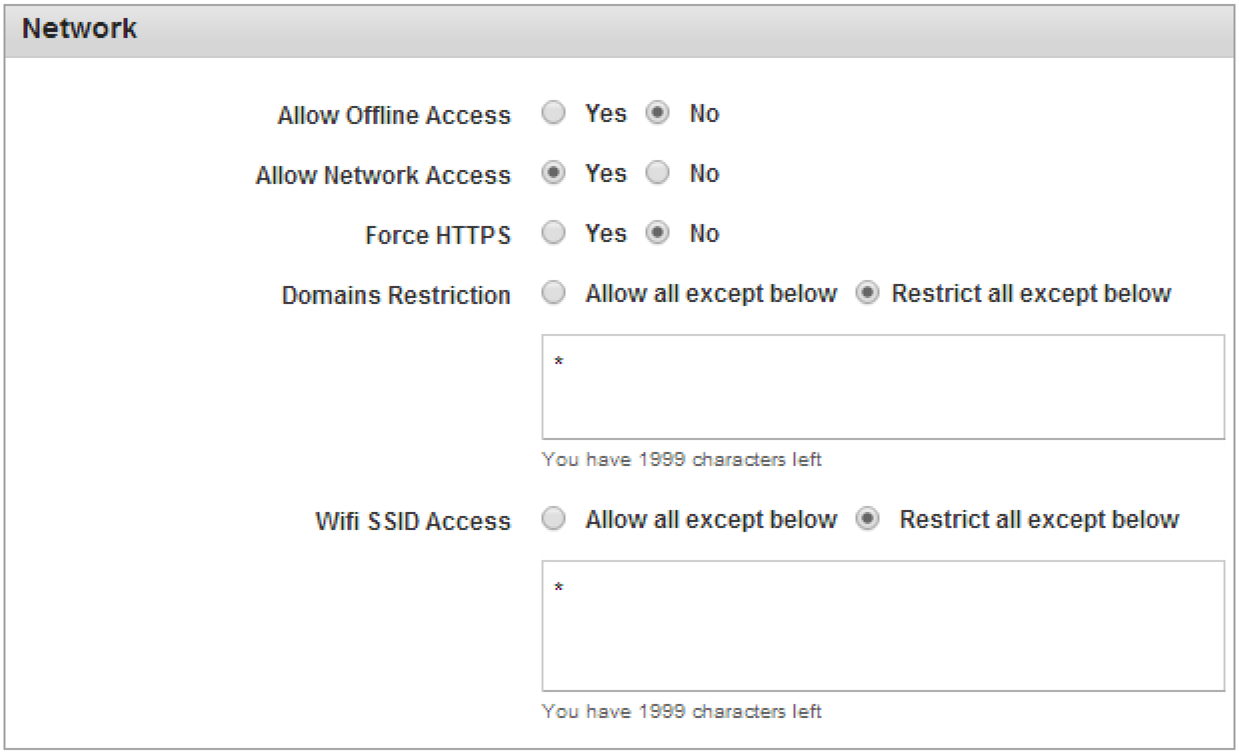
When an app expiry policy is pushed to enrolled device, the policy will be fetched based on server time and time zone selected in Device Settings page. Policy reflection is not dependent on device time and time zone as long as the device is online.

> ***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 with in 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.

11.3.1.3 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.

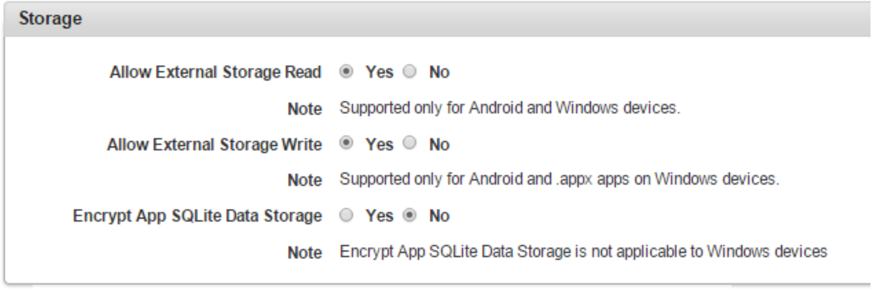
   Force HTTPS option forces every user request to access the device via HTTPS.

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.

11.3.1.4 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.

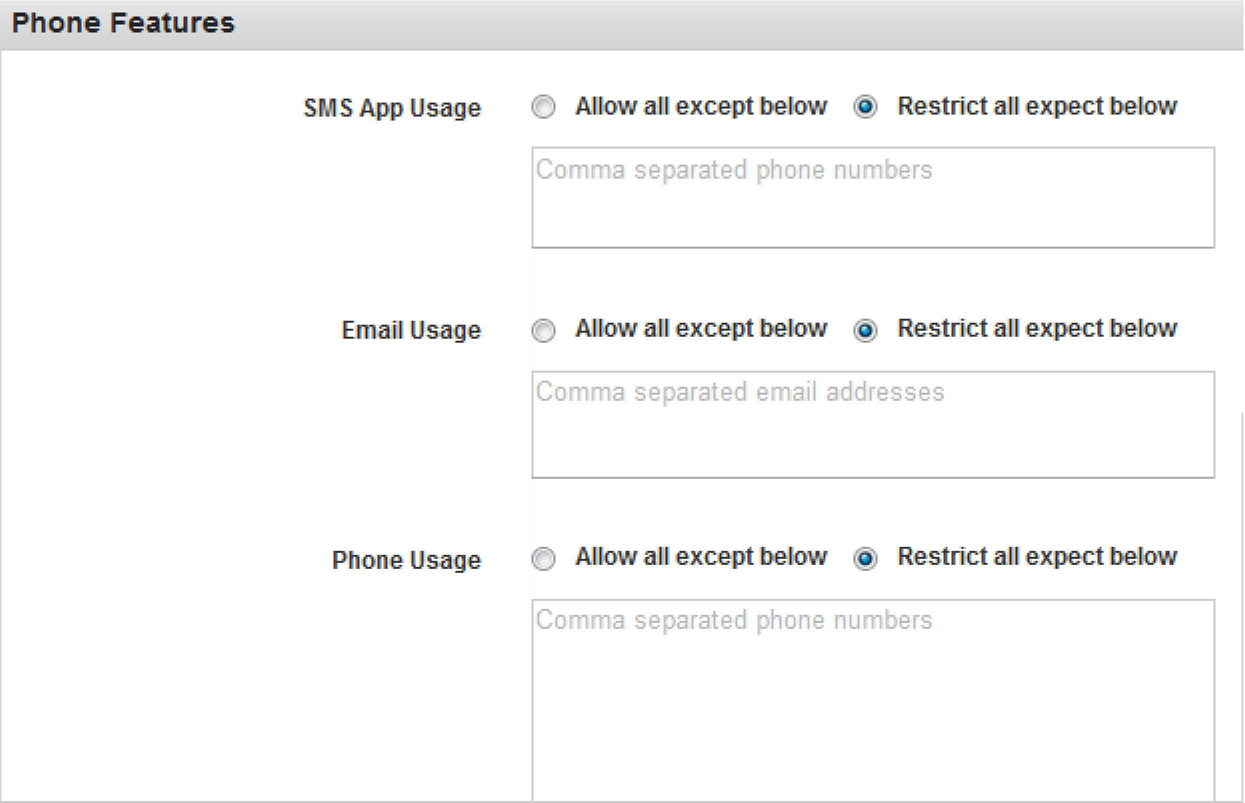
Important: As part of wrapping, SQLite is replaced with SQLCipher. SQLCipher is used for database encryption. There is a subtle difference between SQLCipher and SQLite. In your app, if string data (i.e. base64 string for image) is stored in blob column then it works for SQLite and not SQLCipher. Please 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.

11.3.1.5 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.

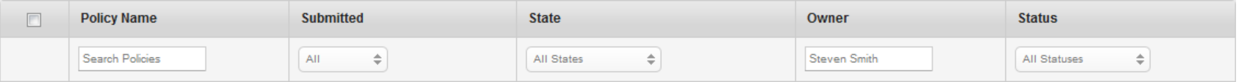
11.3.2 Applying Policies

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.

11.3.3 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.



□	Policy Name	Submitted	State	Owner	Status
	Search Policies	All	All States	Steven Smith	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.

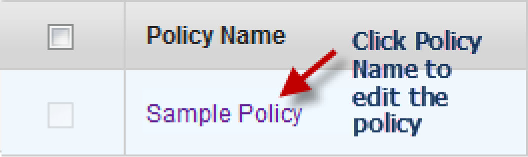
   d. **Owner**: Enter partial or the complete name of the administrator in the text field.

   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.

11.3.4 Updating a Policy

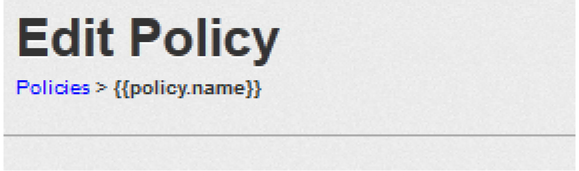
You may need to update a policy detail for specific reasons, for example, you may need to update a policy name or its description.



☐	Policy Name
☐	Sample Policy

Click Policy Name to edit the policy

Click the Policy Name. **Edit Policy** page appears.



Edit Policy

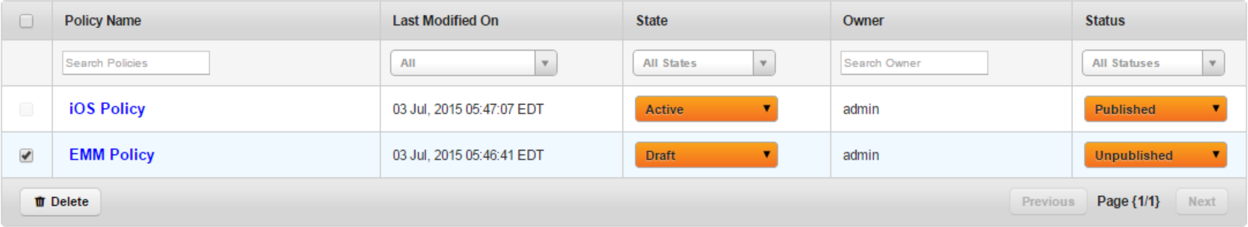
Policies > {{policy.name}}

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)

11.3.5 Deleting a Policy

If a policy has been deprecated, or no longer required, you can delete it.



☐	Policy Name	Last Modified On	State	Owner	Status
	Search Policies	All ▾	All States ▾	Search Owner	All Statuses ▾
☐	iOS Policy	03 Jul, 2015 05:47:07 EDT	Active ▾	admin	Published ▾
☑	EMM Policy	03 Jul, 2015 05:46:41 EDT	Draft ▾	admin	Unpublished ▾

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.

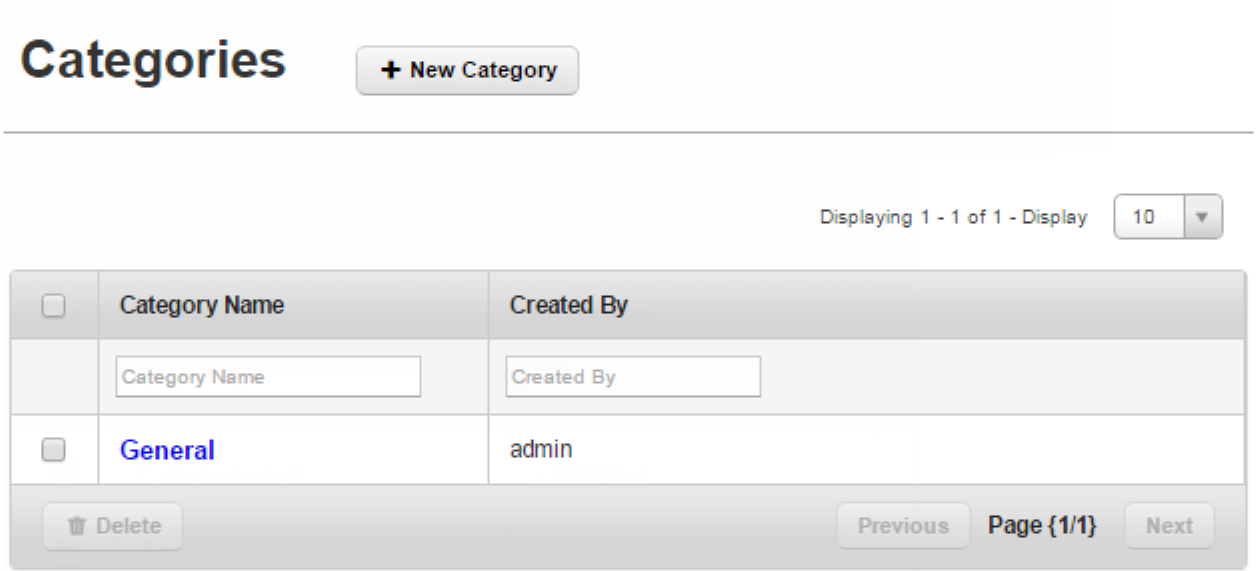
   The policy is no longer displayed in the list view. Only unpublished policies can be deleted.

11.4 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.



□	Category Name	Created By
	Category Name	Created By
□	General	admin

The Categories list view displays the following columns:

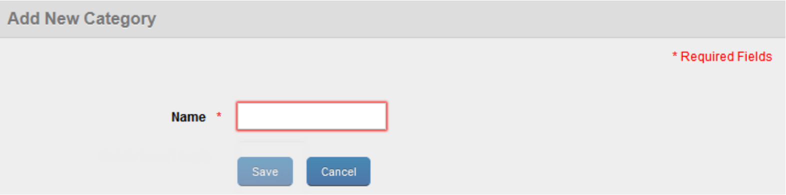
Columns	Description
Name	Provides a list of all the categories.
Created By	Provides a list of all the administrators.

You can perform following activities from this page:

- Creating a New Category
- Searching for Categories
- Updating a Category
- Deleting a Category

11.4.1 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:



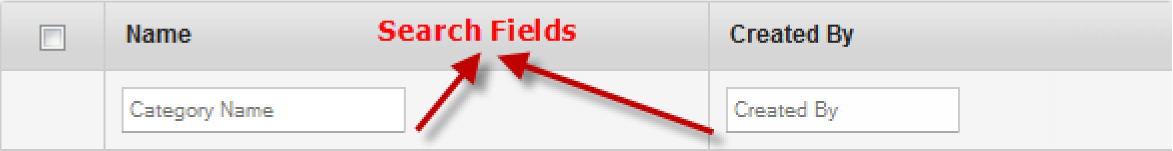
1. **Category Name**: Enter a unique name for the category.
2. Click the **Save** button. In the success message that appears, click OK to continue.The newly added category appears in the list view.

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

   Field with the red asterisk sign is mandatory.

11.4.2 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

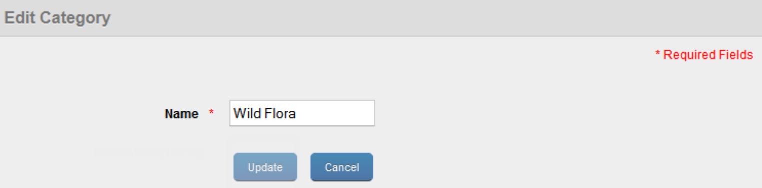
    b. **Created By**: Enter partial or the complete name of the administrator in the text field..

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.

11.4.3 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:



Edit Category

* Required Fields

Name * Wild Flora

1. **Category Name**: If required, change the category name.

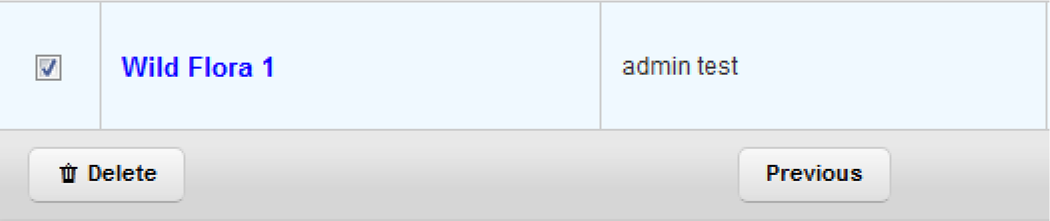
2. After all the updates, the Update button becomes active.

3. Click the **Update** button.In the confirmation message that appears, click OK to continue.

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

11.4.4 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.

11.5 Enterprise Stores

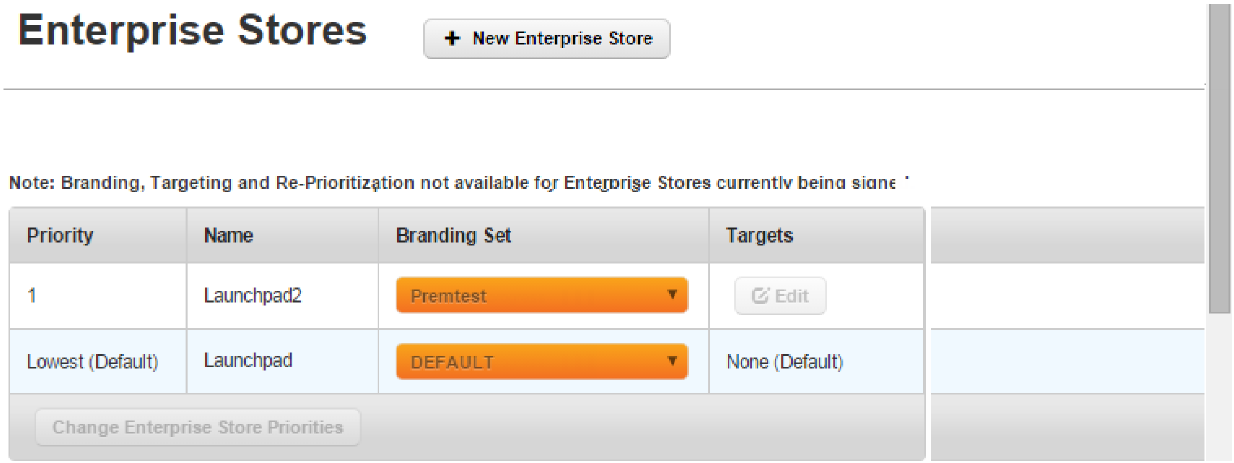
An enterprise store allows you to define and use a branding set for your users and groups. You can define the required branding based on your specific requirements.

> ***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

Note: Branding, Targeting and Re-Prioritization not available for Enterprise Stores currently being signe

Priority	Name	Branding Set	Targets
1	Launchpad2	Premtest	Edit
Lowest (Default)	Launchpad	DEFAULT	None (Default)

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

11.5.1 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.

11.5.2 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.

11.5.3 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.

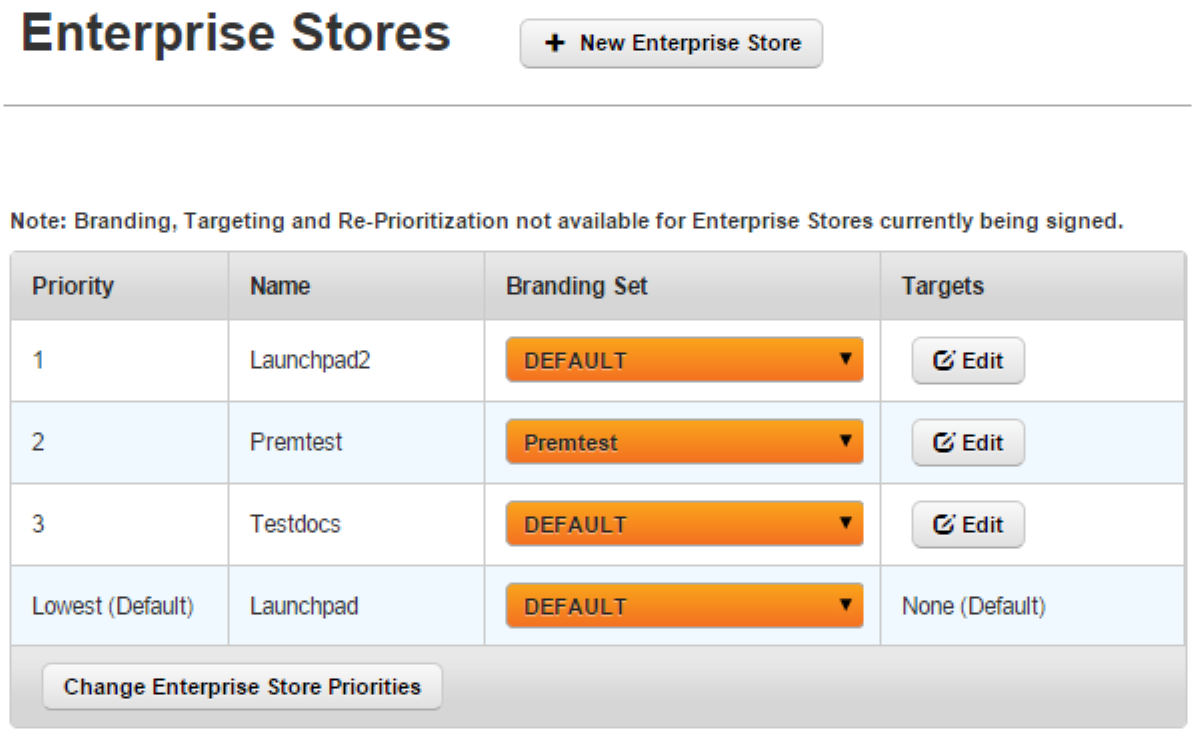
7. Click **Yes**. The Success page appears.

8. Click **OK**. The page closes and the targets are modified.

11.5.4 Changing Enterprise Store Priorities

To change priorities for an enterprise store, follow these steps:

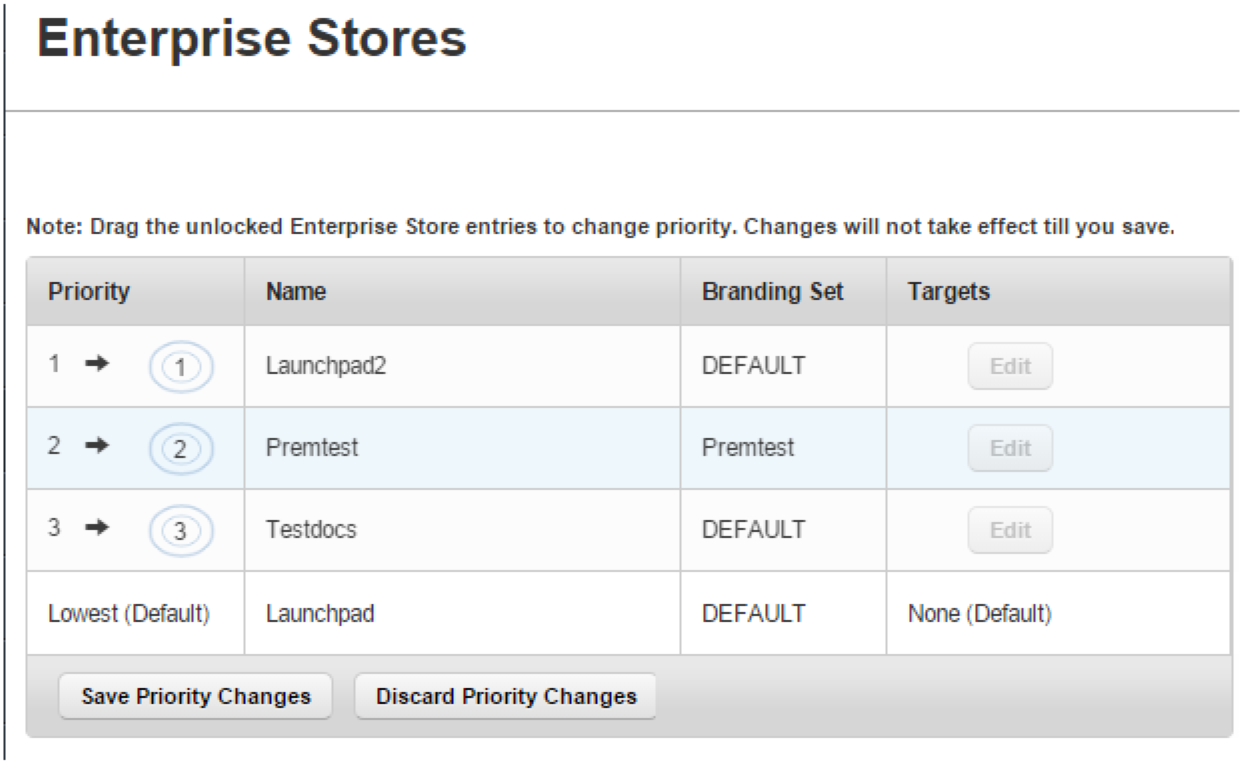
1. In Kony Management Suite Management console, click **Enterprise Stores**. The Enterprise Stores page appears.



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)

2. Click **Change Enterprise Store Priorities**. The Priority column is editable.

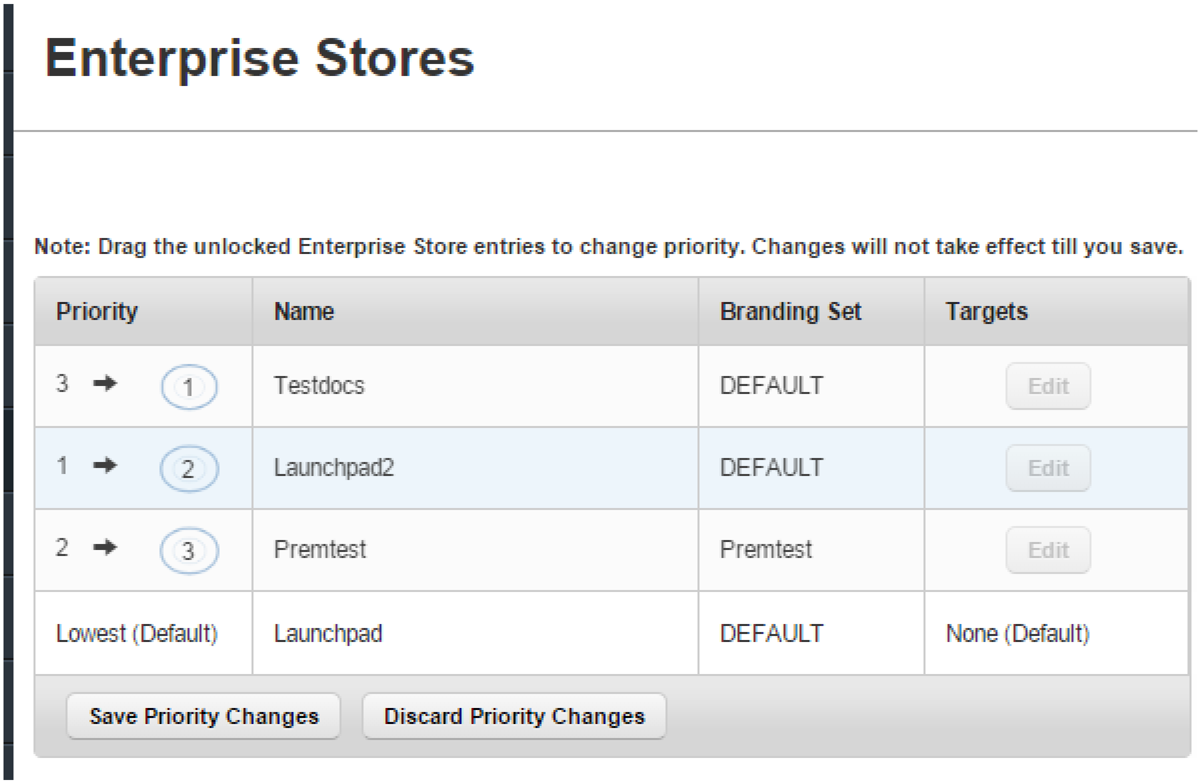


Enterprise Stores

Note: Drag the unlocked Enterprise Store entries to change priority. Changes will not take effect till you save.

Priority	Name	Branding Set	Targets
1 ➡ ①	Launchpad2	DEFAULT	Edit
2 ➡ ②	Premtest	Premtest	Edit
3 ➡ ③	Testdocs	DEFAULT	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	Edit
1 ➜ (2)	Launchpad2	DEFAULT	Edit
2 ➜ (3)	Premtest	Premtest	Edit
Lowest (Default)	Launchpad	DEFAULT	None (Default)

4. Click **Save Priority Changes**. The Confirm Action page appears.

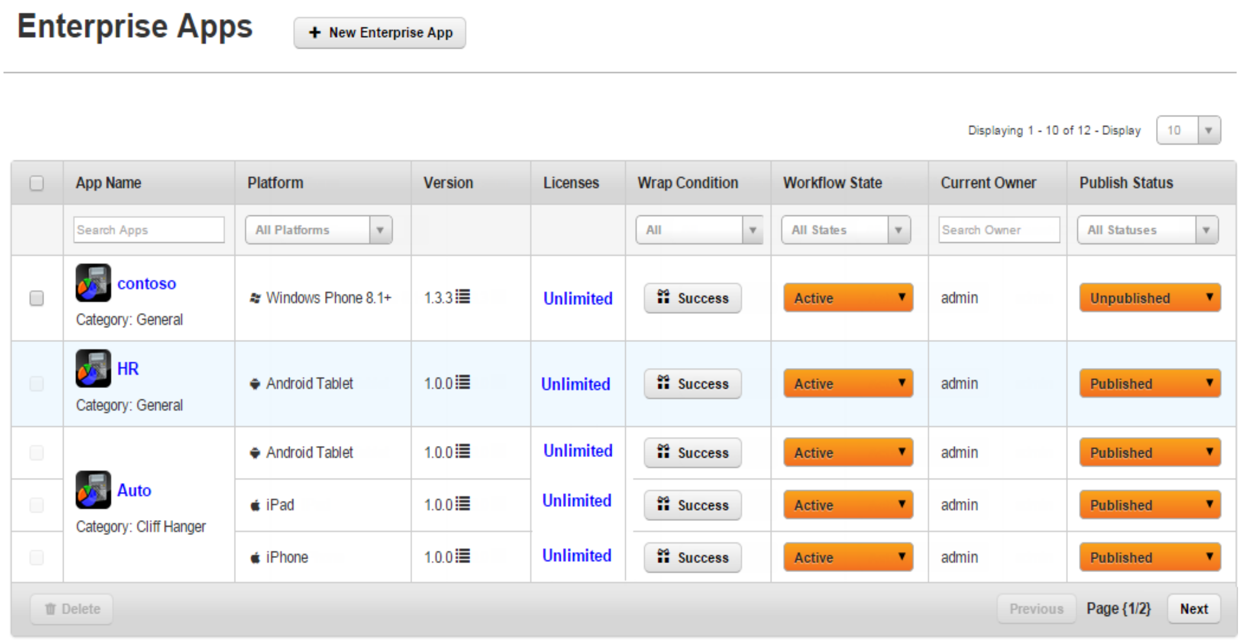
5. Click **Yes**. The Success page appears.

6. Click **OK**. The Priority order of the enterprise stores is modified.

11.6 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 10

□	App Name	Platform	Version	Licenses	Wrap Condition	Workflow State	Current Owner	Publish Status
	Search Apps	All Platforms			All	All States	Search Owner	All Statuses
□	contoso Category: General	Windows Phone 8.1+	1.3.3	Unlimited	Success	Active	admin	Unpublished
□	HR Category: General	Android Tablet	1.0.0	Unlimited	Success	Active	admin	Published
□	Auto Category: Cliff Hanger	Android Tablet	1.0.0	Unlimited	Success	Active	admin	Published
□		iPad	1.0.0	Unlimited	Success	Active	admin	Published
□		iPhone	1.0.0	Unlimited	Success	Active	admin	Published

Delete Previous Page (1/2) Next

The Apps view displays the following columns:

Columns	Description
App Name	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. *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.
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.

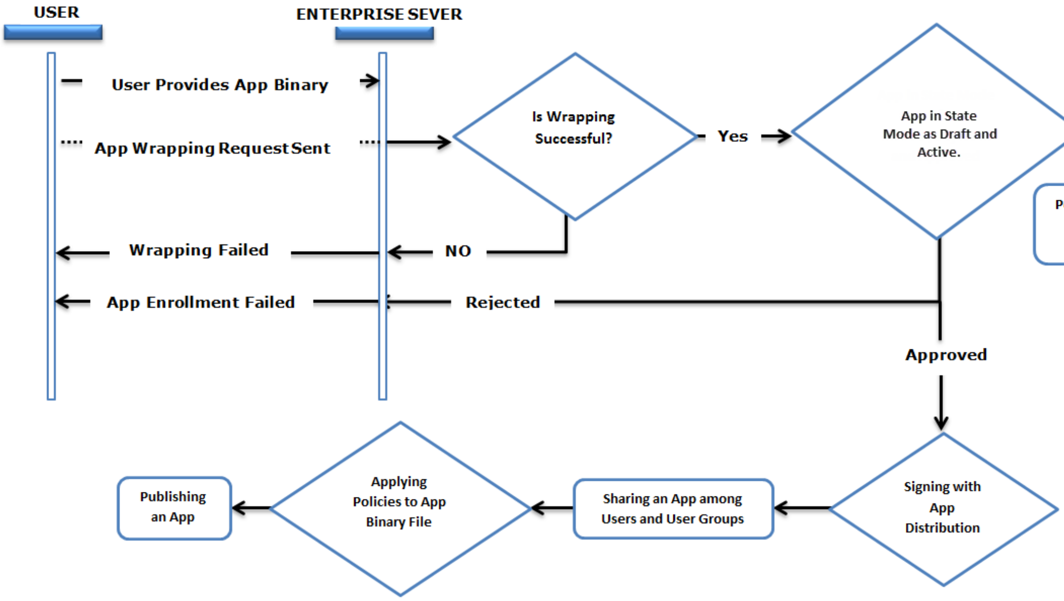
You can perform the following activities from the **Enterprise Apps List** page:

- 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

11.6.1 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.


USER
ENTERPRISE SEVER
User Provides App Binary
App Wrapping Request Sent
Is Wrapping Successful?
Yes
App in State Mode as Draft and Active.
Pending State for Draft and In-Review State
Wrapping Failed
NO
App Enrollment Failed
Rejected
Approved
Signing with App Distribution
Sharing an App among Users and User Groups
Applying Policies to App Binary File
Publishing an App

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:

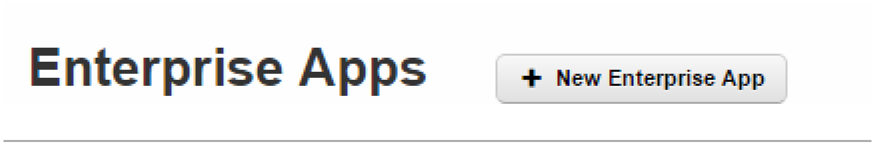
- Step 1: App Basics
- Step 2: App Details
- Step 3: Signing and Targeting
- Step 4: App Specifics
- Step 5: Approve and Confirm

11.6.1.1 Step 1: App Basics

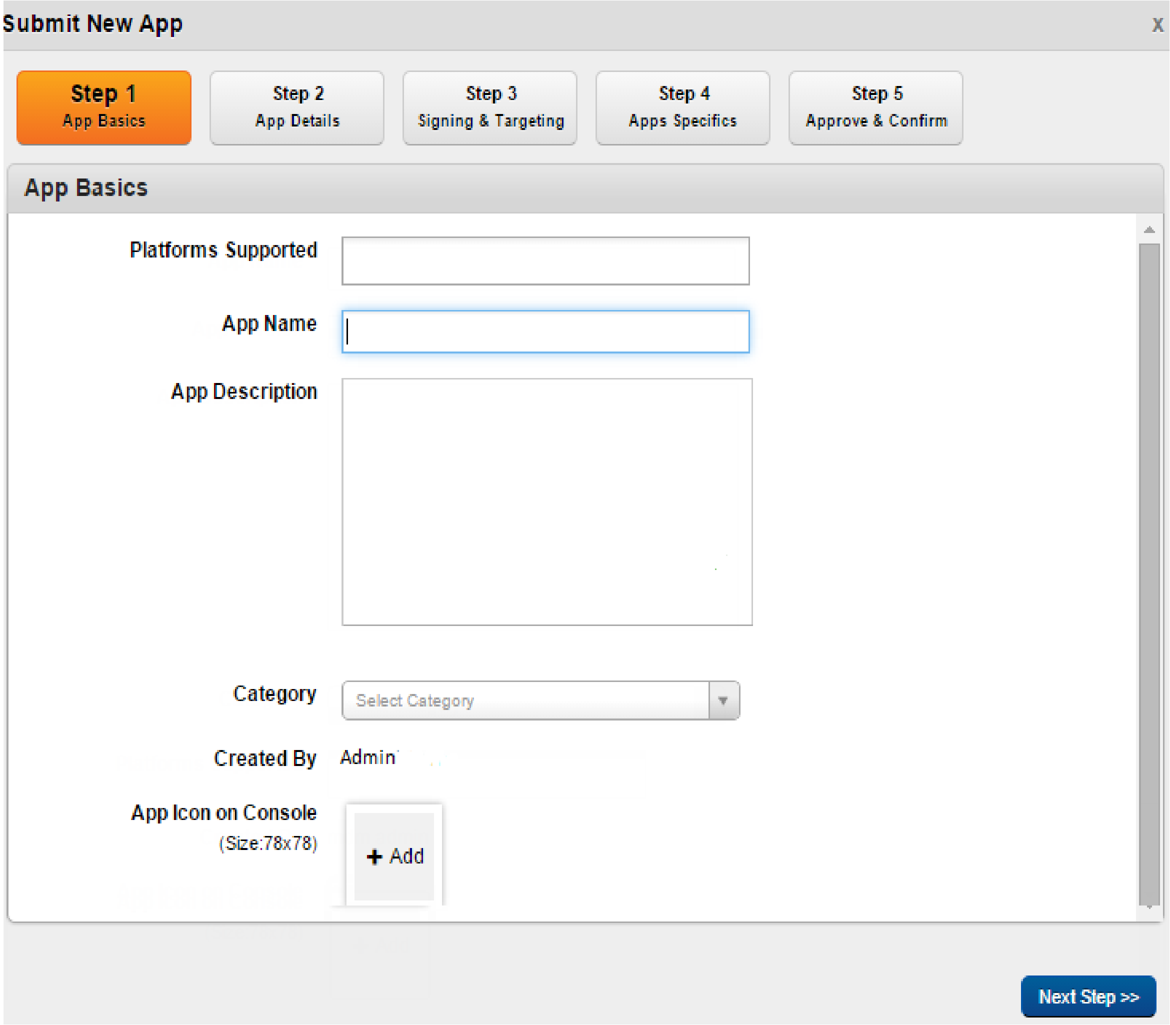
To add a new app, follow these steps:

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
developer.android.com > graphics



2. The **Submit New App** window appears. Enter the following details in the App Basics, under Step 1.



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.

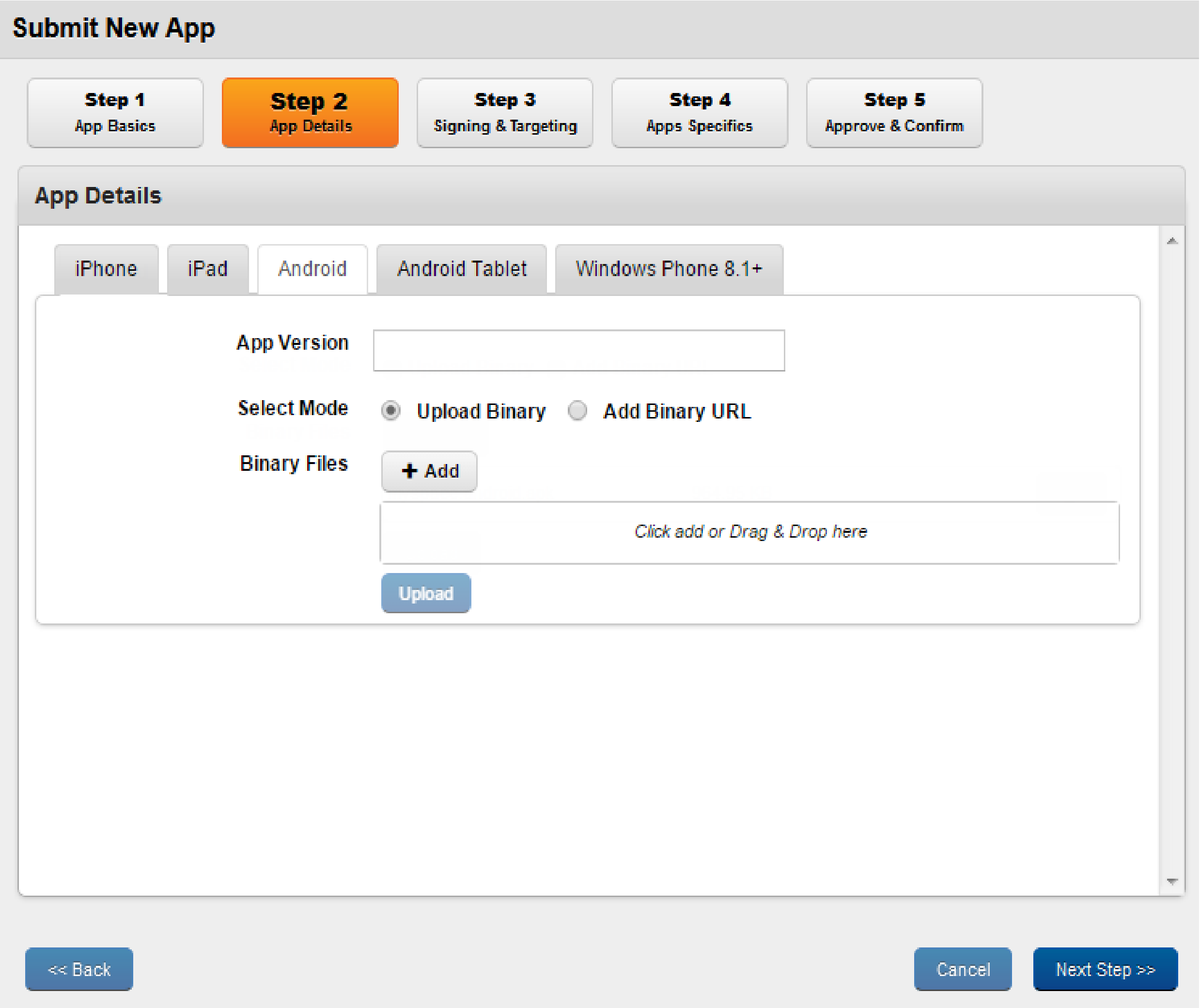
3. Click the **Next Step** button to open **Step 2** window.

> *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.

11.6.1.2 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

App Details

App Version

Select Mode ● Upload Binary ○ Add Binary URL

Binary Files

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.

   c

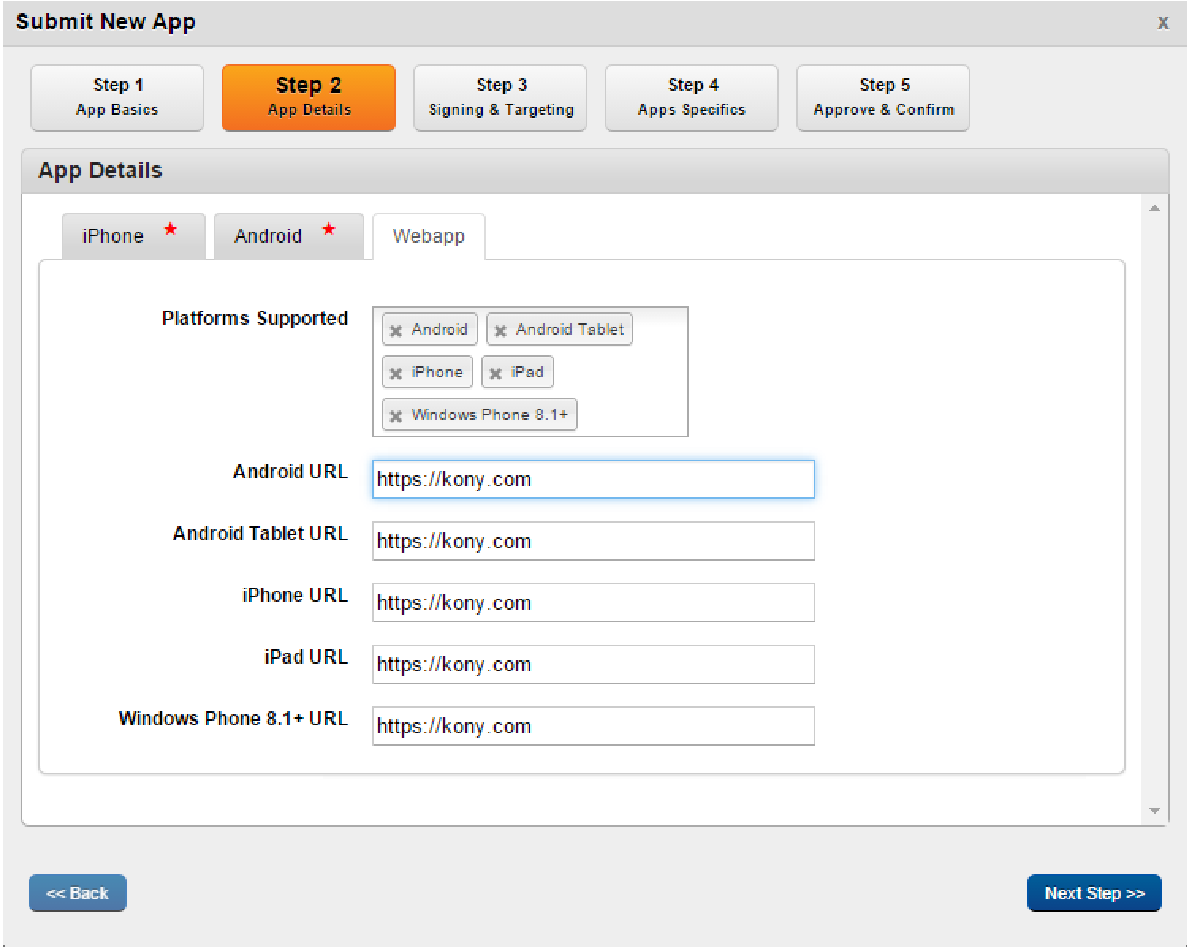
   > ***Note:*** When a Binary URL is added, it is important to remember that the application cannot be wrapped and policies cannot be added to the binary URL as apps can only be signed. Only app distribution can be managed for apps uploaded through this method.

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.



Platforms Supported: Android, Android Tablet, iPhone, iPad, Windows Phone 8.1+

Android URL: https://kony.com

Android Tablet URL: https://kony.com

iPhone URL: https://kony.com

iPad URL: https://kony.com

Windows Phone 8.1+ URL: https://kony.com

- **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.
- **Widows 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:

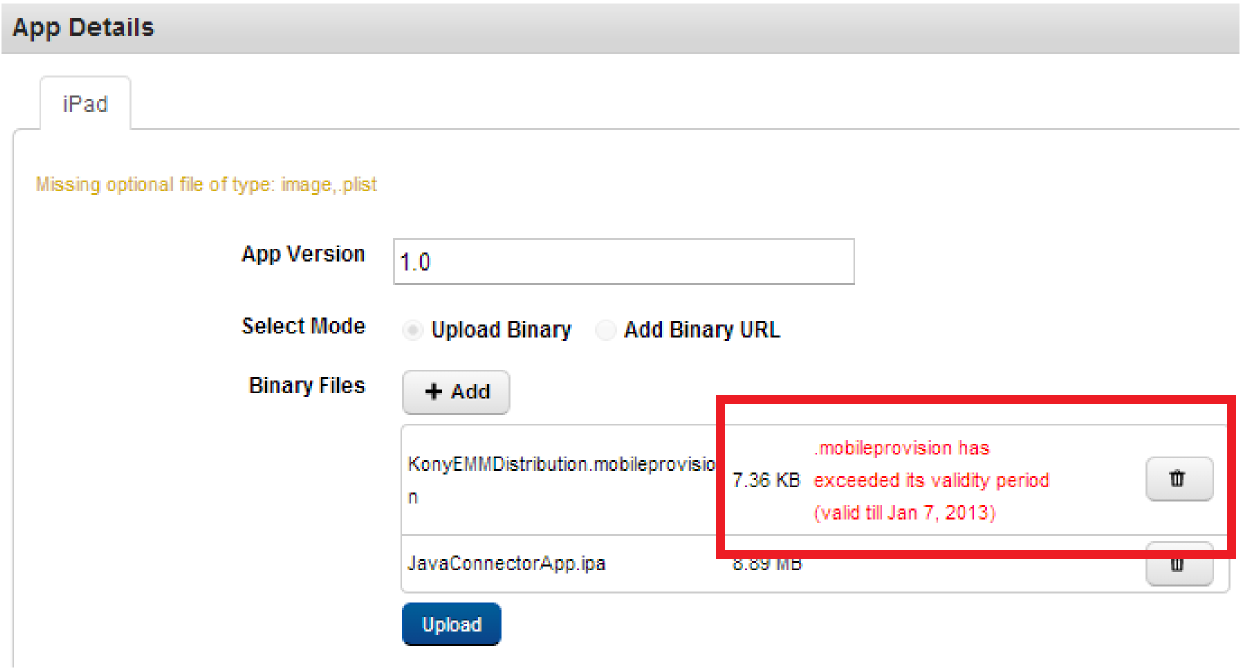
No.	If you upload	The system displays
1	A `.plist` file and a `Mobileprovision adhoc certificate <.mobileprovision>`,	Bundle Identifier as `<com.kone.test.myapp>` The priority for bundle id is given from <.mobileprovision> file. For example, if a .plist file has tag as `<com.kone.myGoogle>` and mobileprovision file has tag as `<com.kone.test.myapp>`, then the bundle id is `<com.kone.test.myapp>`
2	A `.plist` file, a `MobileProvision` adhoc certificate, and a `wildcard certificate`,	Bundle Identifier as `<com.kone.test.myGoogle>` For example, if .plist 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 .plist 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 `adhoc mobileprovision` file,	Bundle Identifier as per adhoc 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

Missing optional file of type: image,.plist

App Version: 1.0

Select Mode: ● Upload Binary ○ Add Binary URL

Binary Files: + Add

KonyEMMDistribution.mobileprovision	7.36 KB	.mobileprovision has exceeded its validity period (valid till Jan 7, 2013)
JavaConnectorApp.ipa	8.89 MB	

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.

11.6.1.3 Step 3: Signing and Targeting

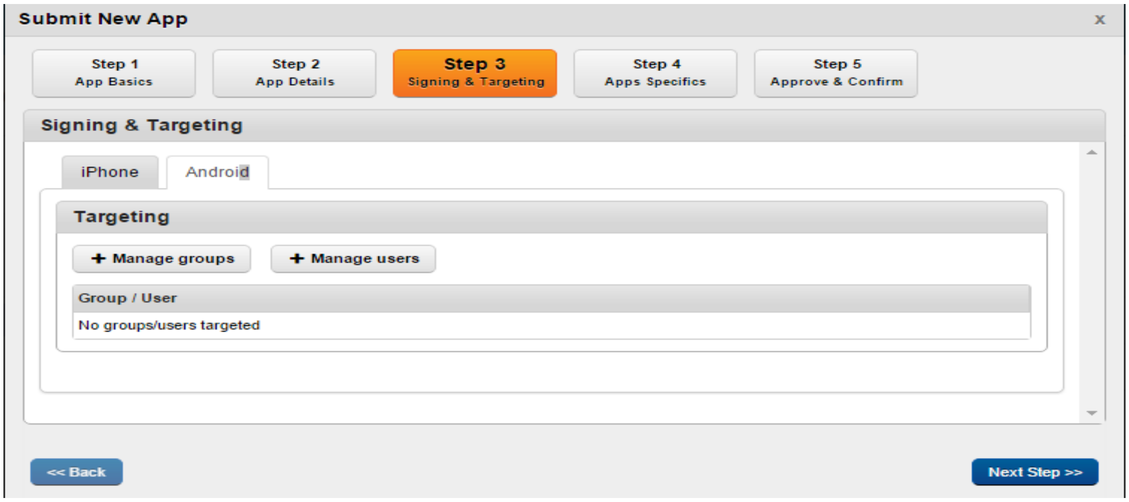
The App Signing window includes three sections:

- 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.



Group / User
No groups/users targeted

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.

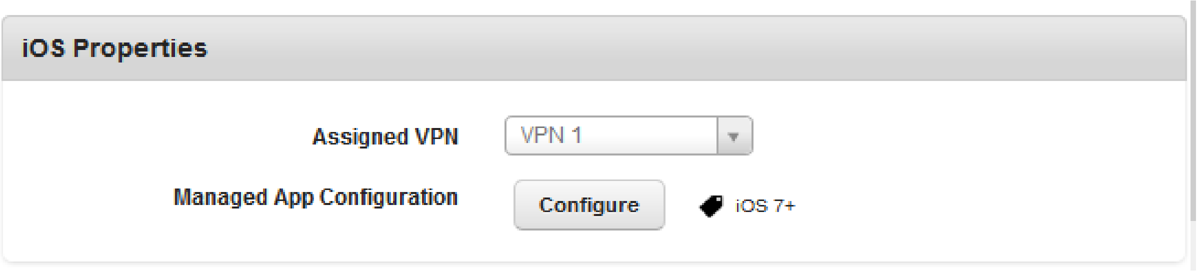
  If an enterprise app and the enterprise store are authenticated with the same OpenID 2.0 server, logging into the enterprise store automatically authenticates the user to use the enterprise app. Suppose the enterprise store does not have OpenID 2.0 authentication enabled, but the enterprise app has OpenID 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



Assigned VPN

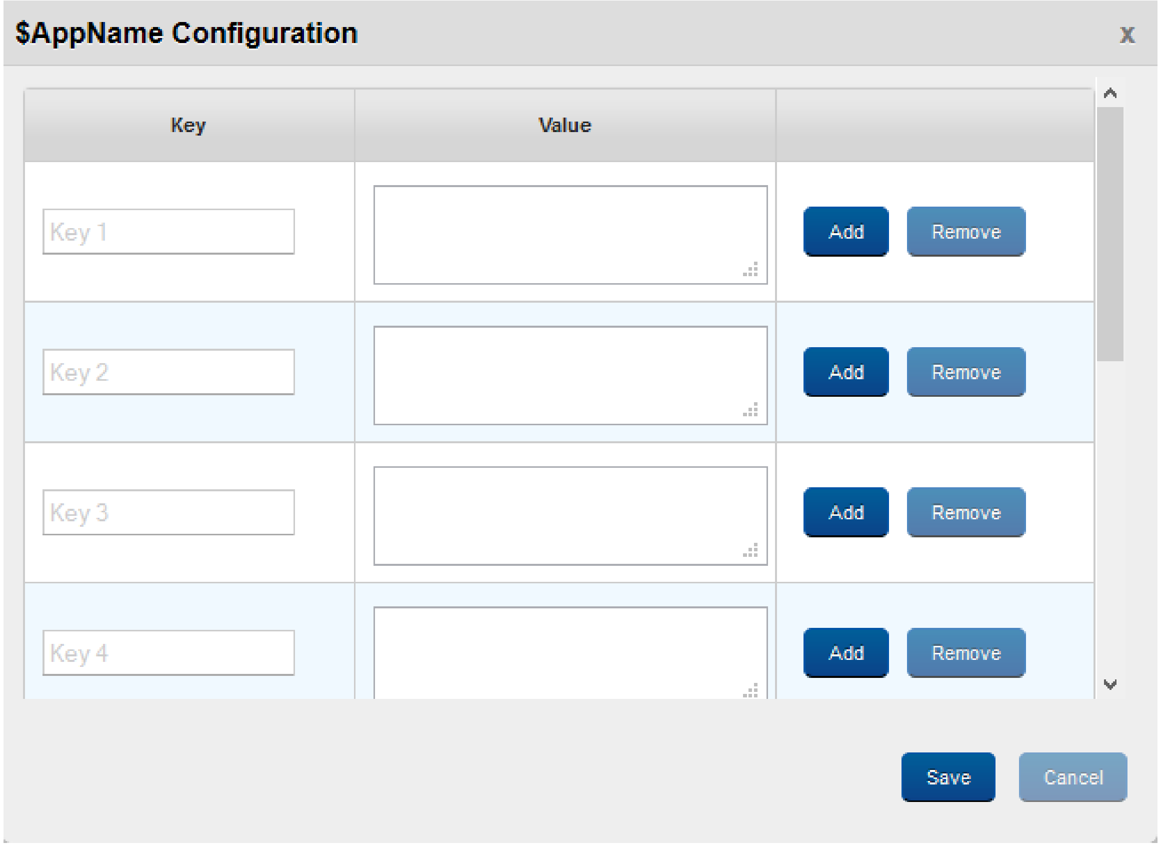
Only VPNs enabled to be Per App VPN are displayed in the **Assigned VPN** drop-down list. For more details, refer to Assigning Per App VPN for iOS. Per App VPNs can be assigned to Enterprise apps while creating apps, updating apps, upgrading apps, or adding new platforms. Per App VPNs can be assigned 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.



$AppName Configuration

Key	Value	
Key 1		Add Remove
Key 2		Add Remove
Key 3		Add Remove
Key 4		Add 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.

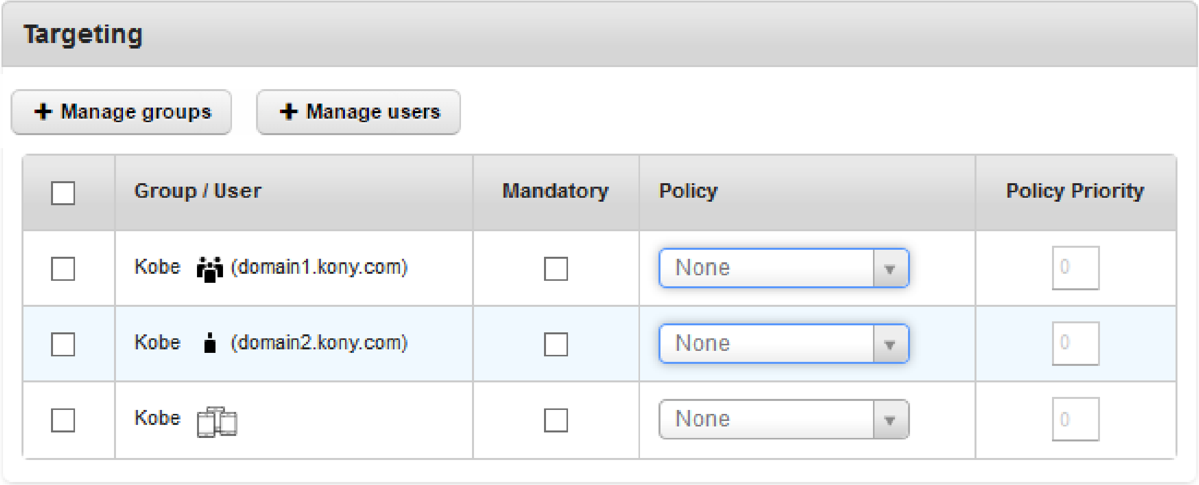
Custom Attributes

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.



□	Group / User	Mandatory	Policy	Policy Priority
□	Kobe (domain1.kony.com)	□	None	0
□	Kobe (domain2.kony.com)	□	None	0
□	Kobe	□	None	0

Apps can be targeted to individual users or groups associated with domains. Take the following steps:

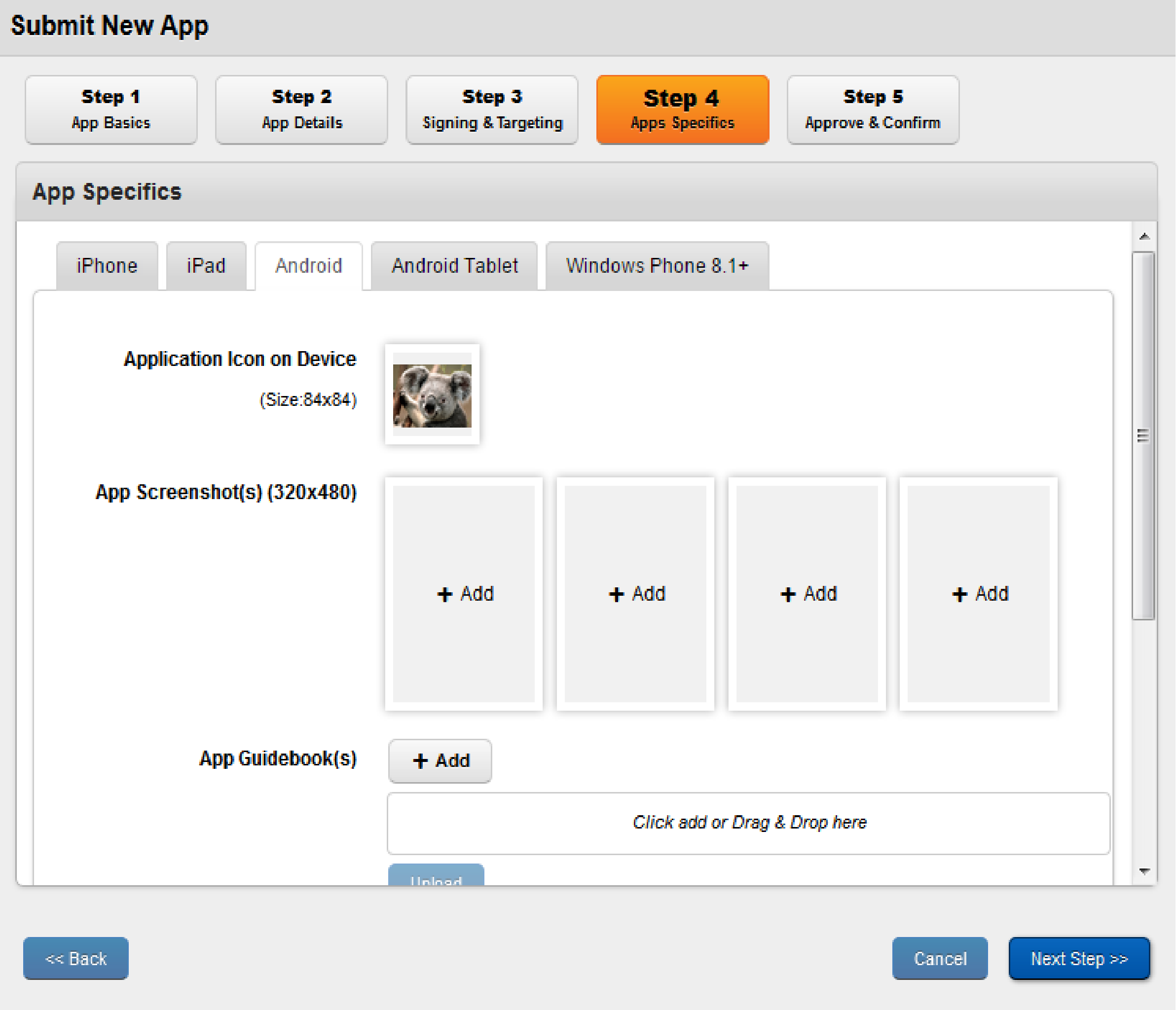
1. Click **Manage Users**, and select the targeted users for the app.
2. Click **Manage Groups**, and select the targeted groups. The domain of the users or groups is always shown here.
3. A list of users associated with domains appear. You can search for the required user by entering a partial or complete 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.

11.6.1.4 Step 4: App Specifics

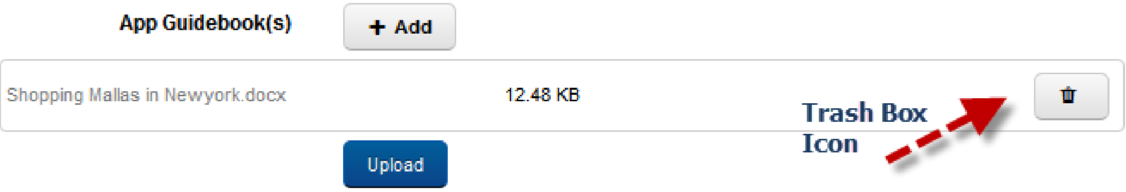
In the App Specifics window, you can upload application-specific files like icons, screenshots, user guides. Select the required files for the fields.



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.

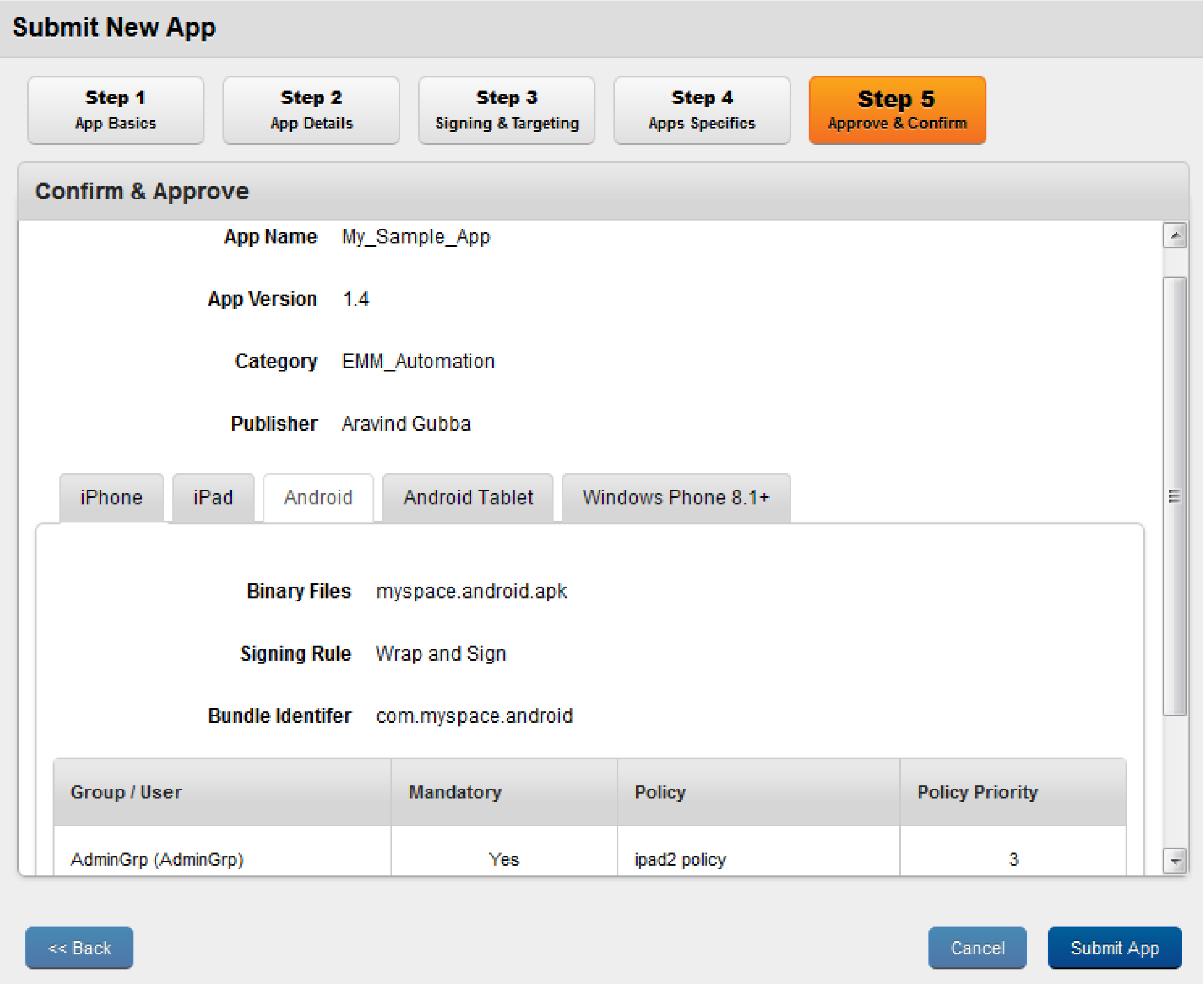
   Guidebooks are documents to help a user to understand how to use the application being uploaded. They appear along with the app in the Enterprise Store.The guidebook can be a plain text file, in rich text format or a PDF.

4. Click the **Next** button to navigate to Step 5: Approve and Confirm

   Click the **Back** button to navigate to Step 3: Signing & Targeting.

11.6.1.5 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

Confirm & Approve

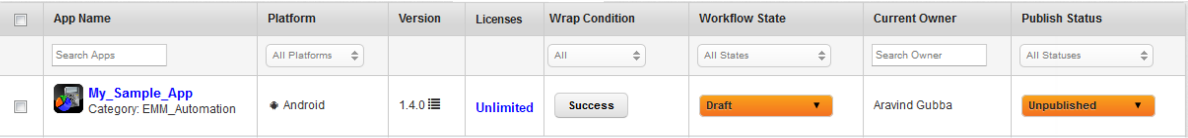
App Name	My_Sample_App
App Version	1.4
Category	EMM_Automation
Publisher	Aravind Gubba

Binary Files	myspace.android.apk
Signing Rule	Wrap and Sign
Bundle Identifer	com.myspace.android

Group / User	Mandatory	Policy	Policy Priority
AdminGrp (AdminGrp)	Yes	ipad2 policy	3

1. Once you confirm the details, click the **Submit App** button to enroll 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.

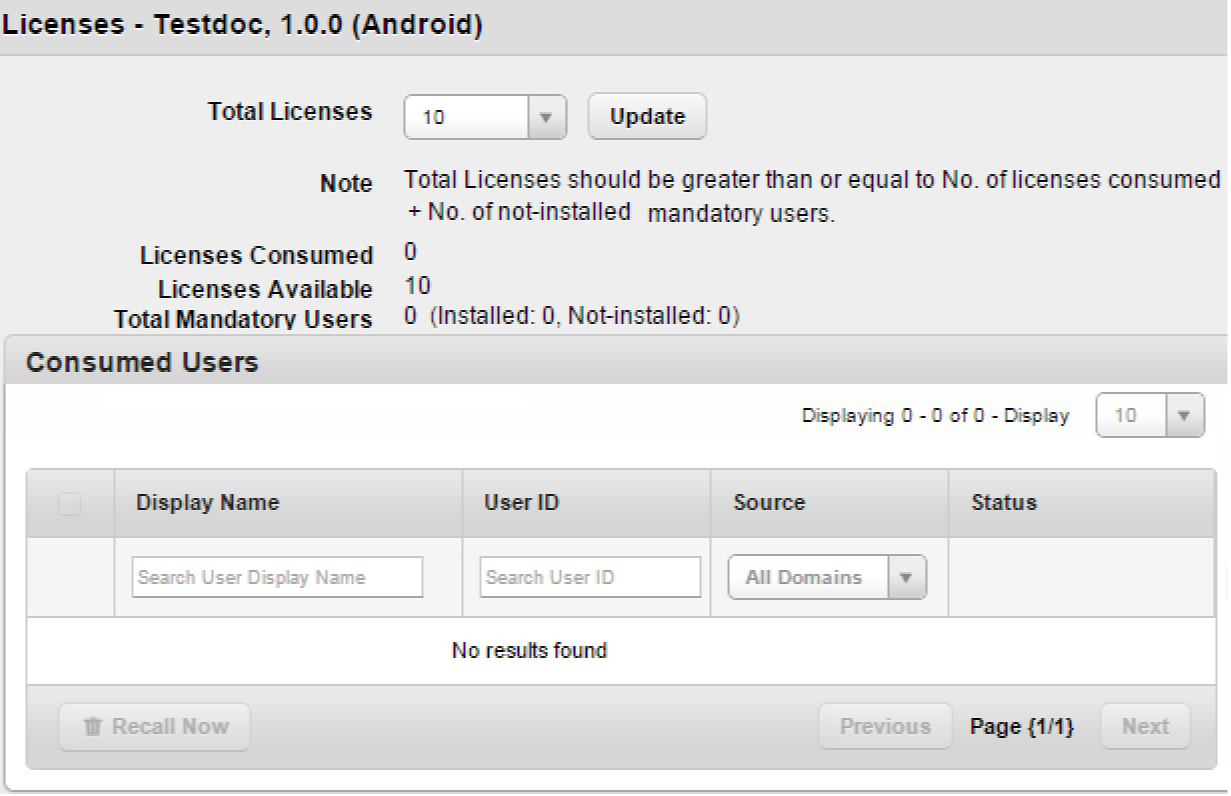
□	App Name	Platform	Version	Licenses	Wrap Condition	Workflow State	Current Owner	Publish Status
	Search Apps	All Platforms			All	All States	Search Owner	All Statuses
□	My_Sample_App Category: EMM_Automation	Android	1.4.0	Unlimited	Success	Draft ▼	Aravind Gubba	Unpublished ▼

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

11.6.2 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: 10

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 10

□	Display Name	User ID	Source	Status
	Search User Display Name	Search User ID	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).

11.6.3 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.

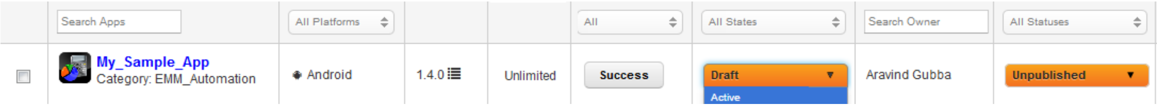
State Name	Description
Active	Appears when the binary has passed review and approved by an administrator and is active.

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.

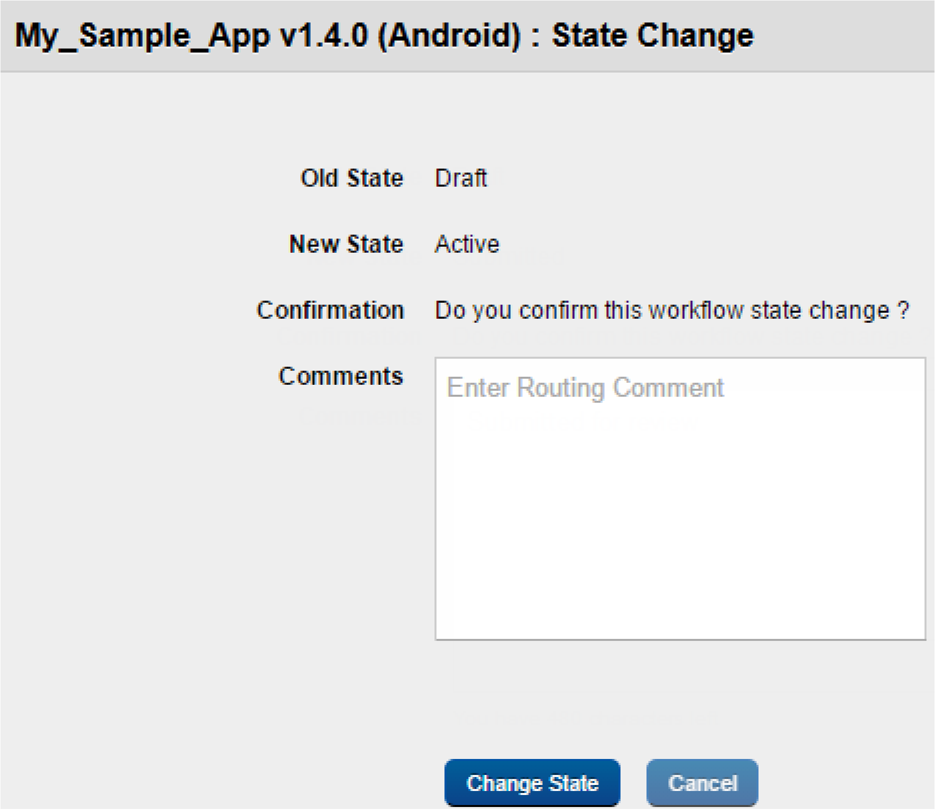
To publish an app, follow these steps:

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
□	My_Sample_App Category: EMM_Automation	Android	1.4.0	Unlimited	Success	Draft ▼ Active	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

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.

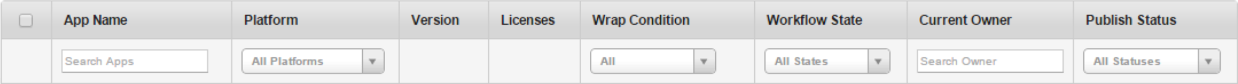
   The Workflow State changes to **Active** in the list view.
4. To publish the app, select the **Publish** option from the drop-down list under Publish Status column. The **State Change** window appears.
5. Enter an appropriate comment in the **Comments** text box. Click the Publish button to proceed. The system displays the confirmation message stating that published App is now available in Store. Click **OK** to proceed.

11.6.4 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:



□	App Name	Platform	Version	Licenses	Wrap Condition	Workflow State	Current Owner	Publish Status
	Search Apps	All Platforms ▾			All ▾	All States ▾	Search Owner	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.

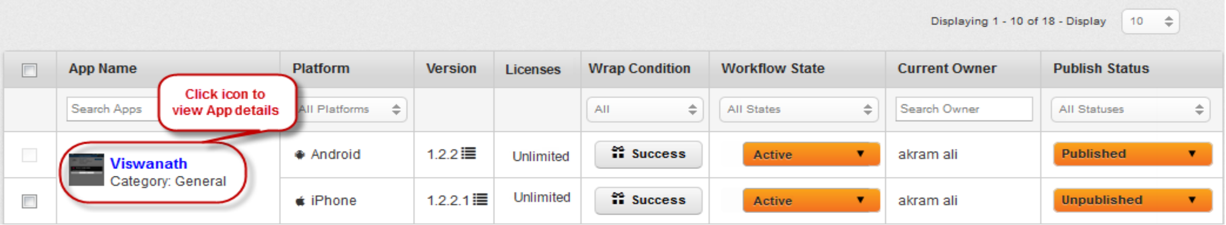
    f. **Status**: Select the current status of the app from the drop-down list. By default, it is set to All Statuses. You can modify to Published or Unpublished.

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.

11.6.5 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.



Displaying 1 - 10 of 18 - Display 10

□	App Name	Platform	Version	Licenses	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	Unlimited	Success	Active	akram ali	Published
□		iPhone	1.2.2.1	Unlimited	Success	Active	akram ali	Unpublished

Click icon to view App details

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]

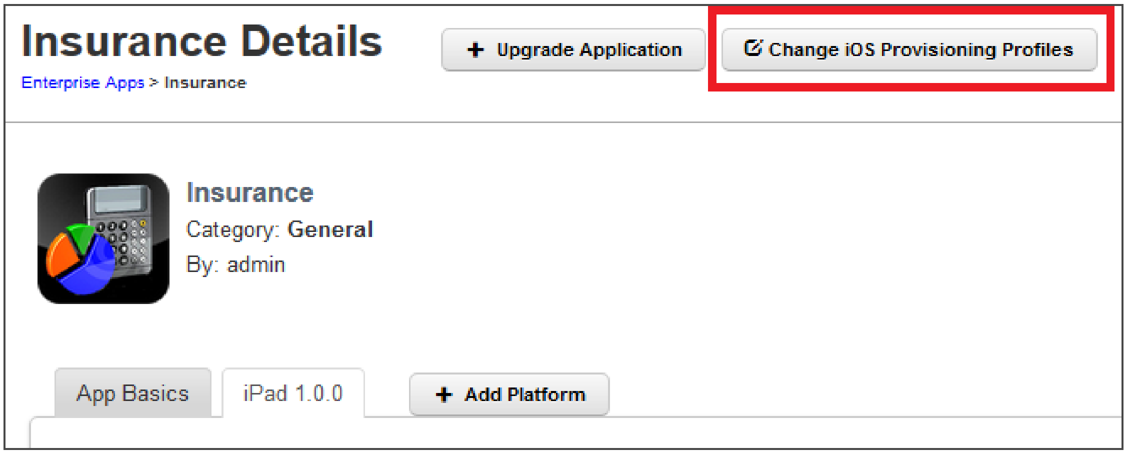
6. Click the **Save and Exit** button to save the updated details. In the confirmation message that appears, click **OK** to continue.

11.6.5.1 Changing iOS Provision Profiles

While editing app details, an administrator can also add or edit iOS mobile-provision profiles.

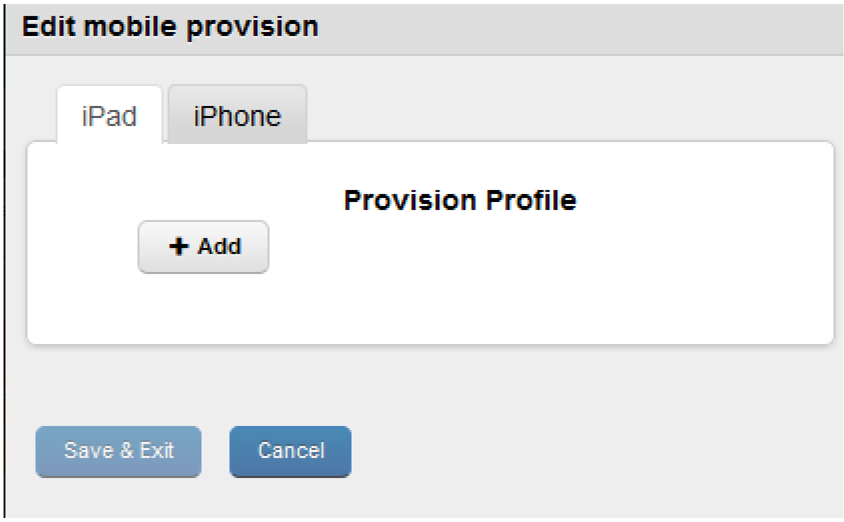
To change mobile-provision profiles, follow these steps:

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.

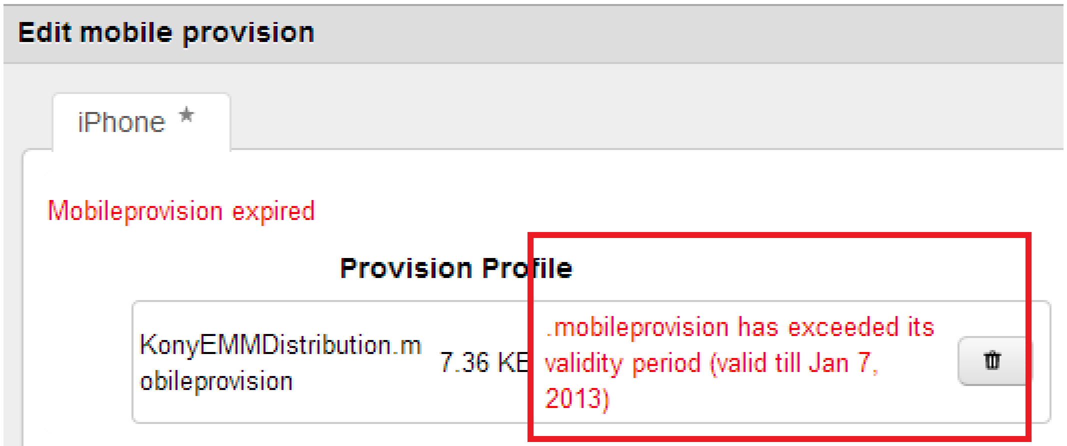
The following tables lists error messages:

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 `<com.kone.x.Test>`, then the user upload wildcard mobile-provision profile must be <com.kone.x.*>For example, if the app bundle ID is `<com.kone.Test>`, then the user upload wildcard mobile-provision profile must be `<com.kone.*>`	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:



Edit mobile provision

Mobileprovision expired

Provision Profile

KonyEMMDistribution.mobileprovision 7.36 KB .mobileprovision has exceeded its validity period (valid till Jan 7, 2013)

11.6.6 Upgrading Enterprise App Details

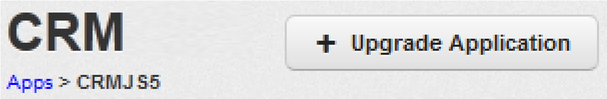
You may wish to upgrade the added application details if new functionality have been added in your app, and binary file is modified etc. This process upgrades the app version.

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.

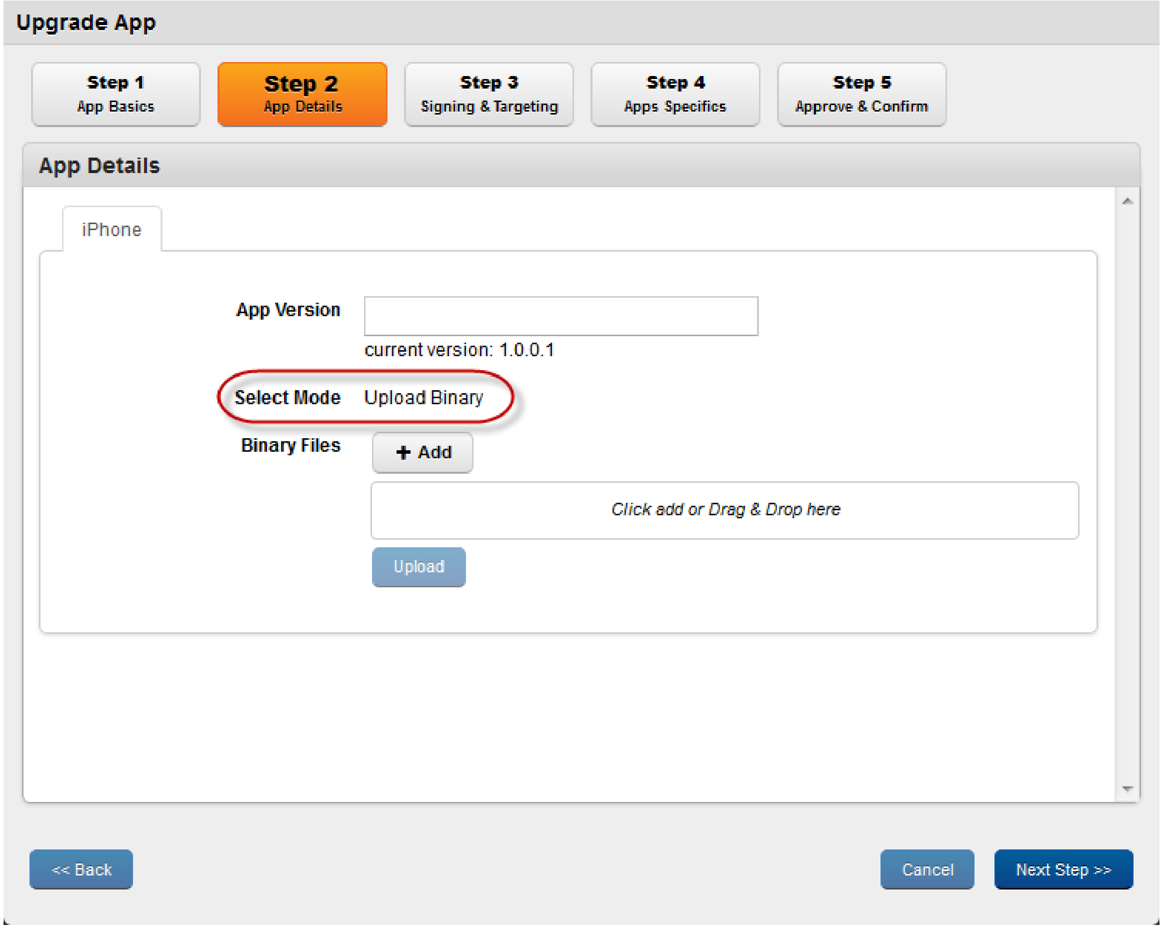
   Upgrade App Window appears.

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

App Details

App Version

current version: 1.0.0.1

Select Mode Upload Binary

Binary Files

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.

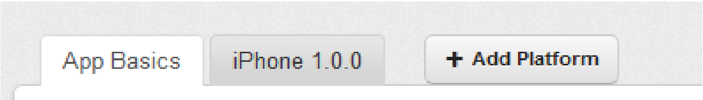
11.6.7 Adding a New Platform

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.

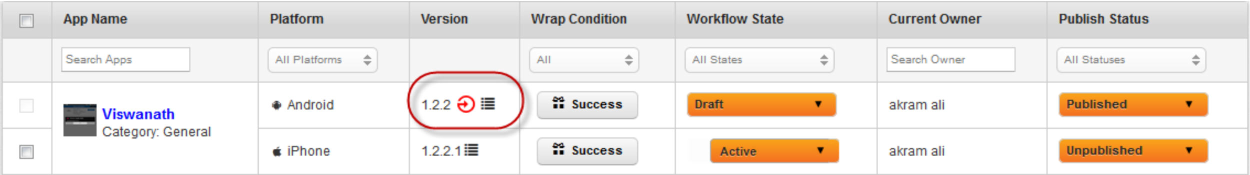
   

   Add Platform window appears.

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.

11.6.8 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.

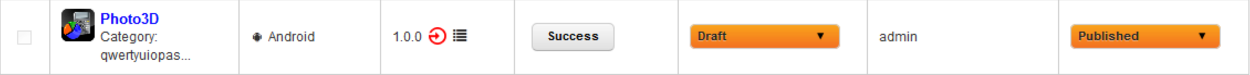


☐	App Name	Platform	Version	Wrap Condition	Workflow State	Current Owner	Publish Status
	Search Apps	All Platforms		All	All States	Search Owner	All Statuses
☐	Viswanath Category: General	Android	1.2.2	Success	Draft ▼	akram ali	Published ▼
☐		iPhone	1.2.2.1	Success	Active ▼	akram ali	Unpublished ▼

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.

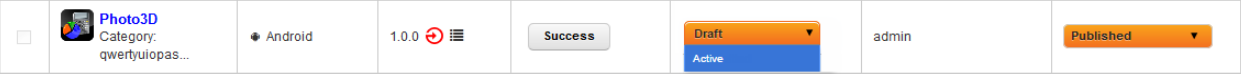
The state must be changed to Approved and published again for the changes to take effect.

To publish the App again, follow these steps:



□	Photo3D Category: qwertyuiopas...	Android	1.0.0	Success	Draft ▼	admin	Published ▼

The current State is **Draft** and the current Status is **Published.**



□	Photo3D Category: qwertyuiopas...	Android	1.0.0	Success	Draft ▼ Active	admin	Published ▼

1. Select the State as **Submitted** from the drop down menu.

   State Change window appears.

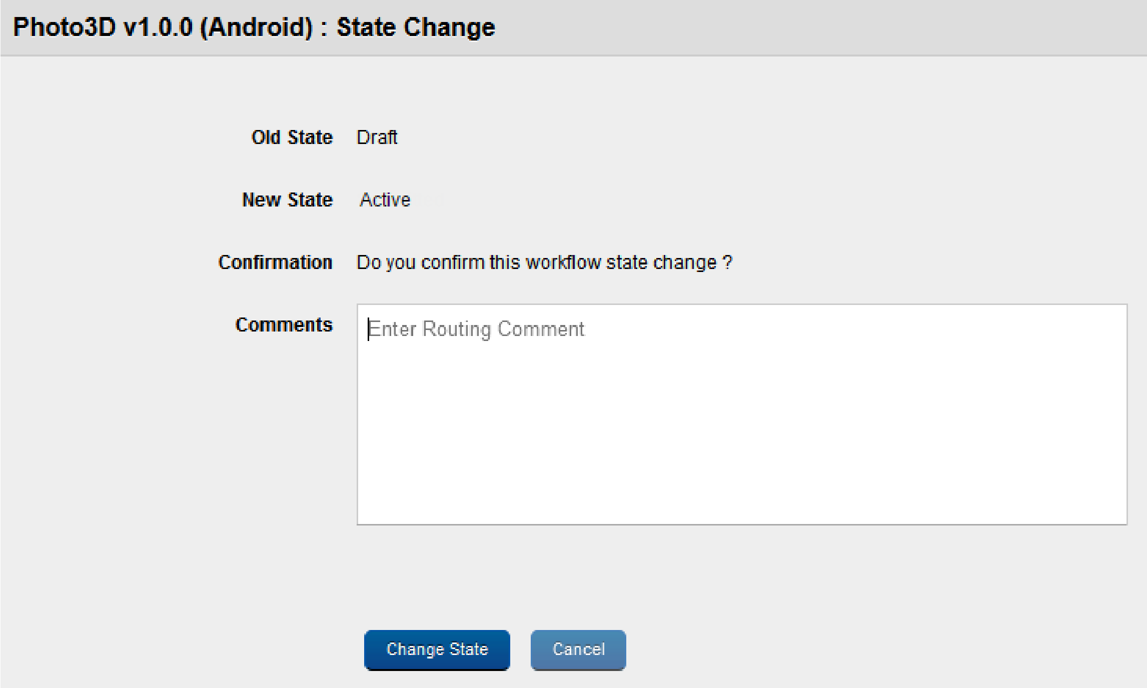


Photo3D v1.0.0 (Android) : State Change

Old State Draft

New State Active

Confirmation Do you confirm this workflow state change ?

Comments Enter Routing Comment

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.

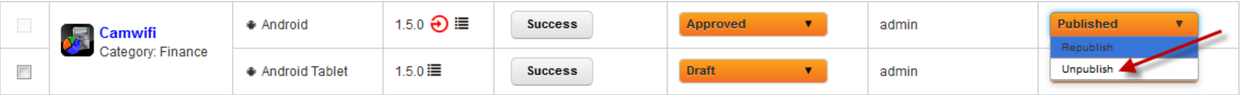
   The Stale icon next to app version is removed. The current State is **Active** and the current Status is **Published.**

11.6.9 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.

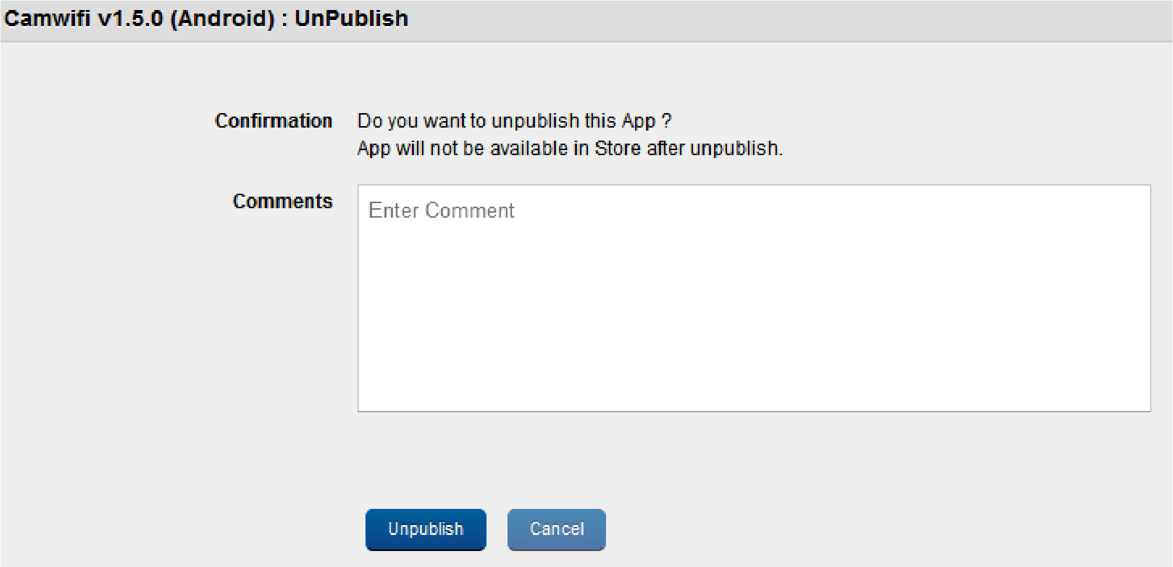
To unpublish the App, follow these steps:



□	Camwifi Category: Finance	Android	1.5.0	Success	Approved ▼	admin	Published ▼
□		Android Tablet	1.5.0	Success	Draft ▼	admin	

1. Select the status as Unpublish from the drop-down menu.

   Unpublish window appears.



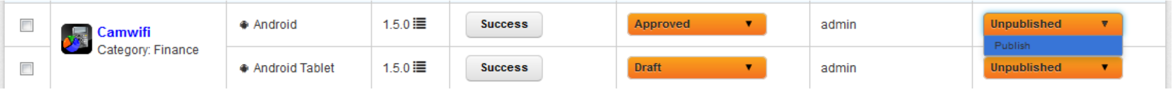
Camwifi v1.5.0 (Android) : UnPublish

Confirmation Do you want to unpublish this App ?
App will not be available in Store after unpublish.

Comments Enter Comment

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.



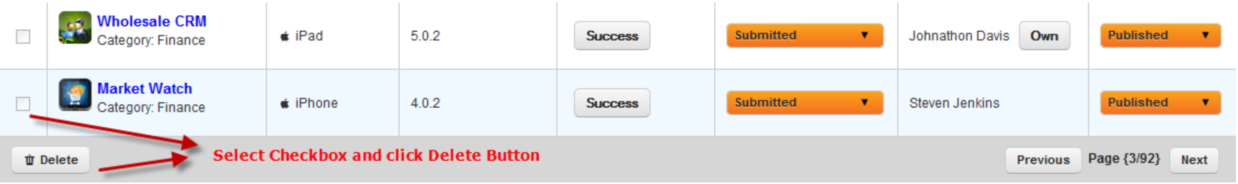
□	Camwifi Category: Finance	Android	1.5.0	Success	Approved ▼	admin	Unpublished ▼ Publish
□		Android Tablet	1.5.0	Success	Draft ▼	admin	Unpublished ▼

4. The App Status changes to **Unpublished.**

   The Unpublished status can be reverted to Published.

11.6.10 Deleting an App

If an app is no longer required, you can delete it.



□	Wholesale CRM Category: Finance	iPad	5.0.2	Success	Submitted ▼	Johnathon Davis Own	Published ▼
□	Market Watch Category: Finance	iPhone	4.0.2	Success	Submitted ▼	Steven Jenkins	Published ▼

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.

11.7 VPP Apps

The Apple’s Volume Purchase Program (VPP) helps businesses to quickly find, buy in bulk and distribute apps to their employees to meet their business needs. EMM currently supports VPP for iOS 7+ devices only.

For information on configuring VPP Apps section in the Application Settings page, click here.

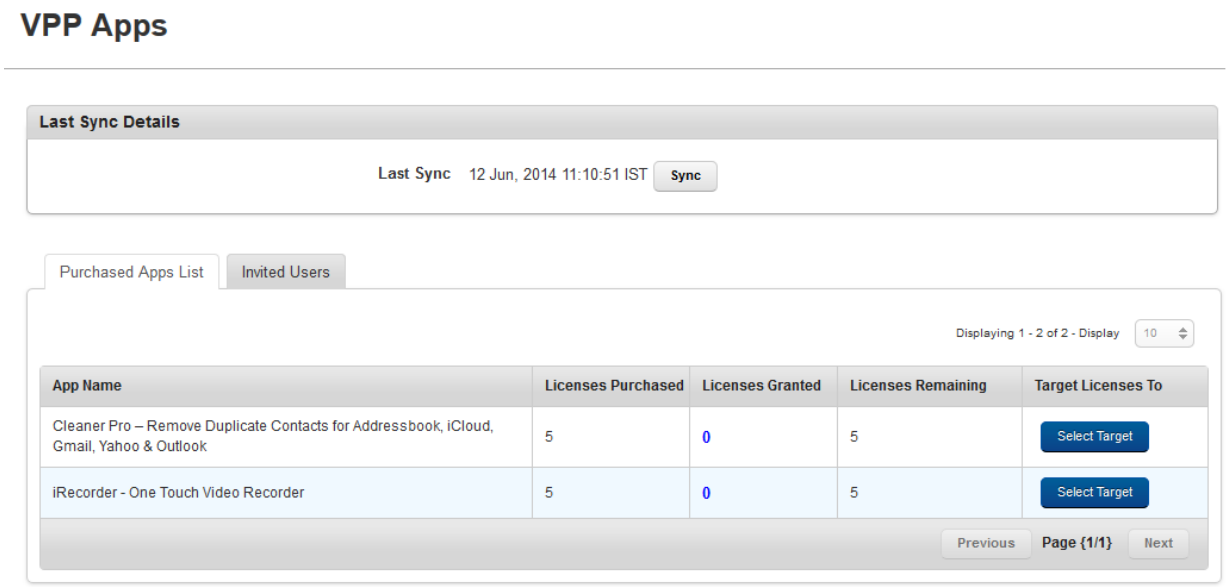
11.7.1 Invitation Process

To begin using Apple's VPP, you must receive an email from EMM inviting you to become associated with the program. The administrator sends invitations to users and groups (each user in a group receives an invitation). The list of invited users are updated in the Invited Users tab

Details of all targeted users are sent to the Apple Server for registration. For more information, see Targeting Users

When you receive your invitation email, you will be asked to click on a designated URL link while on your iOS7+ device. You will need to provide your device Apple ID and password to be authenticated with the server. On acceptance of terms and conditions, you are associated with VPP. Your credentials are associated with your Apple ID that is used for creating a VPP.

From the **App Management** section, click **VPP Apps** from the left panel. The **VPP Apps List** page appears with the Purchased App List tab by default. This page displays a list of purchased apps along with licenses purchased, granted, and remaining.



VPP Apps

Last Sync Details

Last Sync 12 Jun, 2014 11:10:51 IST

Displaying 1 - 2 of 2 - Display 10

App Name	Licenses Purchased	Licenses Granted	Licenses Remaining	Target Licenses To
Cleaner Pro – Remove Duplicate Contacts for Addressbook, iCloud, Gmail, Yahoo & Outlook	5	0	5	Select Target
iRecorder - One Touch Video Recorder	5	0	5	Select Target

An administrator can manage both the purchased apps and invited users from the **VPP Apps List** screen.

11.7.2 Granting Licenses

Once a user is associated to the VPP, licenses are granted for all the apps targeted to that user. Before granting licenses, the system checks with Apple whether there are any licenses available for that app. If the licenses are available, the system grants licenses purchased from VPP to associated users, and pushes apps to iOS 7+ devices automatically. Associated Users can download and install targeted VPP apps seamlessly. The number of licenses granted column is modified accordingly. For more details, see Purchased Apps List tab.

When a user is targeted, if a user is associated with same apple ID on multiple iOS devices , the system grants licenses and installs the app on the users' associated iOS 7+ devices.

Once the licenses are granted, the pushed apps from VPP are listed as paid apps in users iOS device's purchased history.

Even if a user does not install an app, the license is still granted to the user.

The VPP Apps page has the following sections:

- Purchased App List tab
- Invited Users tab

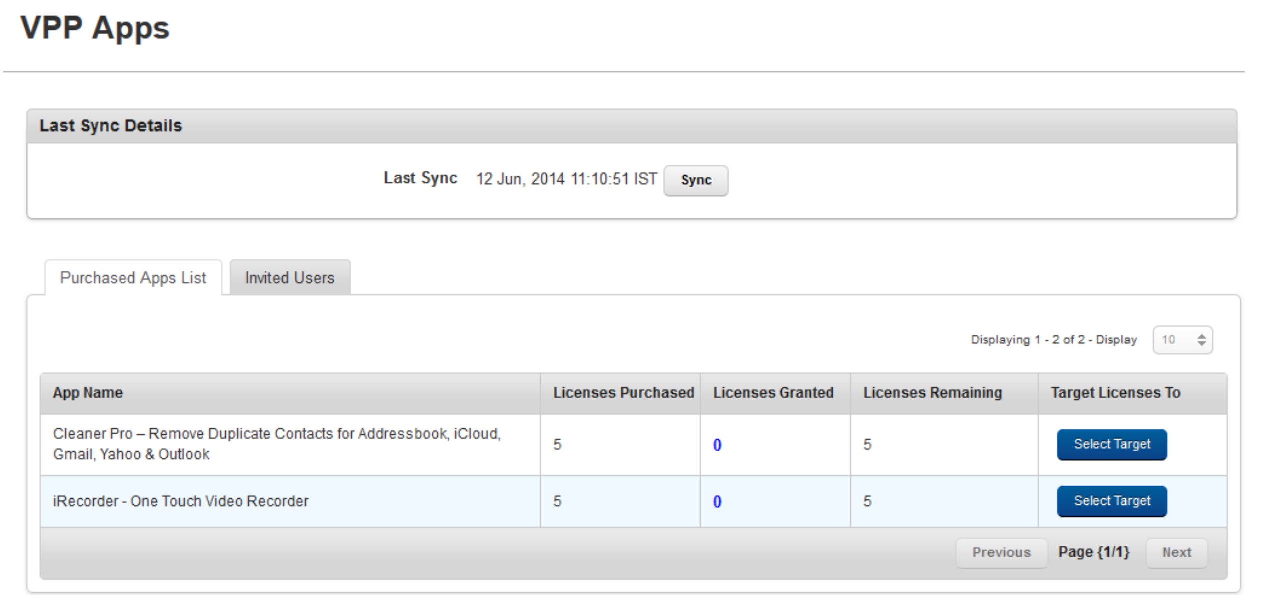
11.7.3 Purchased App List tab

The **Purchased Apps List** tab displays the list of apps purchased, only from the Apple VPP portal by the VPP Facilitator. The App Details and Invited Users details are updated with every sync.

Last Sync detail

Displays the last sync date and time details. Click the **Sync Now** button to start the sync immediately to get current status of purchased apps list.

> ***Note:*** App details and invited user details are updated only with every sync. For any delay in getting the latest status, an administrator can initiate the sync by clicking the **Sync Now** button.



VPP Apps

Last Sync Details

Last Sync 12 Jun, 2014 11:10:51 IST

Displaying 1 - 2 of 2 - Display 10

App Name	Licenses Purchased	Licenses Granted	Licenses Remaining	Target Licenses To
Cleaner Pro – Remove Duplicate Contacts for Addressbook, iCloud, Gmail, Yahoo & Outlook	5	0	5	Select Target
iRecorder - One Touch Video Recorder	5	0	5	Select Target

The **Purchased App List** tab view displays the following columns:

Columns	Description
App Name	Displays the name of app purchased through VPP.
Licenses Purchased	Displays the number of licenses purchased for a specific app through VPP.
Licenses Granted	Displays the number of licenses of an app granted to users.
Licenses Remaining	Displays the number of licenses of an app available to be granted.
Target	Click the Select Target button to grant licenses.

11.7.3.1 Targeting Licenses to Associated Users

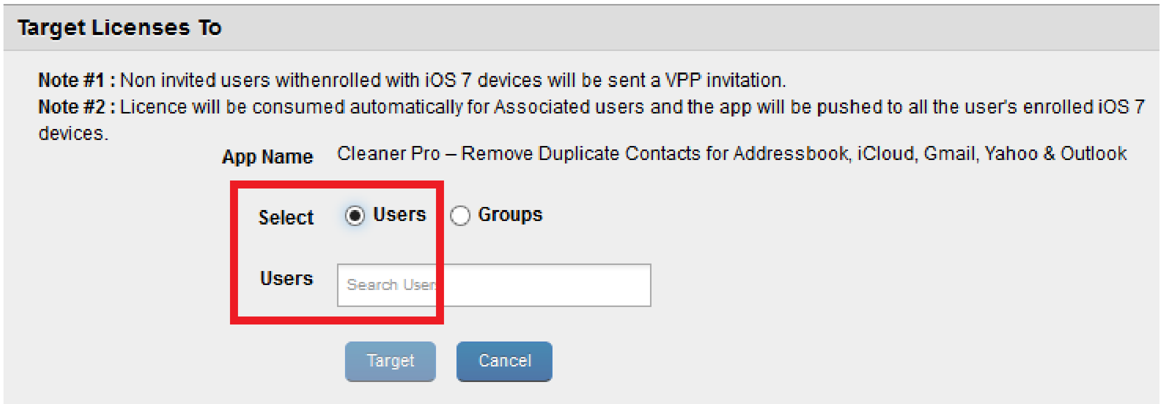
Purchased Apps can only be targeted to Users associated with VPPs. Admin can target apps to a specific set of users or groups in EMM.

> ***Note:*** Super administrators can target VPP apps to any user, group, or domain. Administrators with limited access can only target users, groups, and domains they have access to.

To target associated users, follow these steps:

1. In **Purchased Apps List tab > Target** column, click the **Select Target** button for one of the apps. The system displays the **Target Licenses To** dialog.

2. Select either **Users** or **Groups**. The system displays text fields based on the selected options.



Target Licenses To

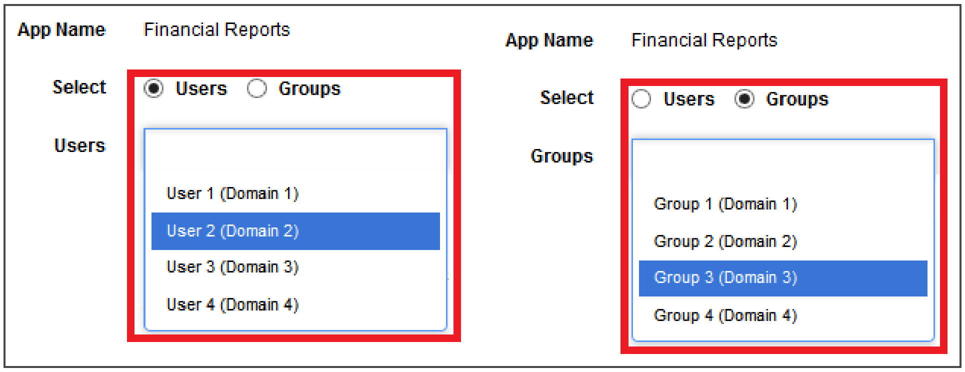
Note #1 : Non invited users withenrolled with iOS 7 devices will be sent a VPP invitation.
Note #2 : Licence will be consumed automatically for Associated users and the app will be pushed to all the user's enrolled iOS 7 devices.

App Name Cleaner Pro – Remove Duplicate Contacts for Addressbook, iCloud, Gmail, Yahoo & Outlook

Select ● Users ○ Groups

Users Search User

3. Click in the **Users** text field to select multiple users. The users are displayed with domains.



App Name Financial Reports

Select ● Users ○ Groups

Users

User 1 (Domain 1)
User 2 (Domain 2)
User 3 (Domain 3)
User 4 (Domain 4)

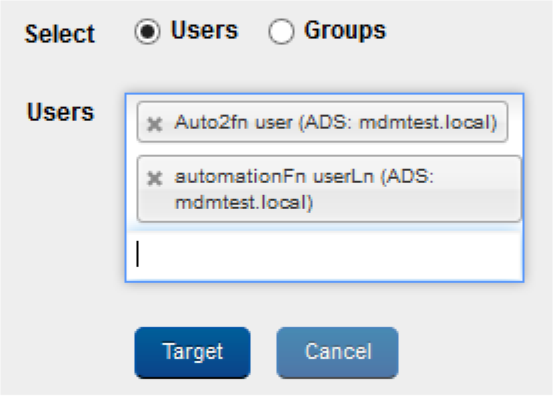
App Name Financial Reports

Select ○ Users ● Groups

Groups

Group 1 (Domain 1)
Group 2 (Domain 2)
Group 3 (Domain 3)
Group 4 (Domain 4)

The selected users are displayed in the text filed.



Select ● Users ○ Groups

Users
Auto2fn user (ADS: mdmtest.local)
automationFn userLn (ADS: mdmtest.local)

4. Click **Target**.

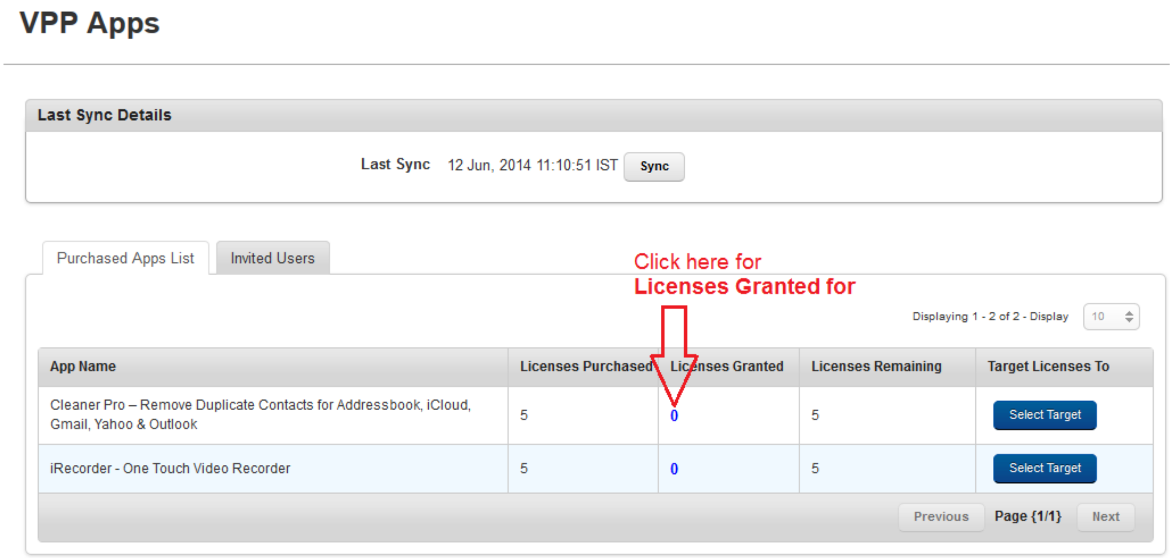
   The system sends a VPP invitation to non invited users enrolled with iOS 7+ devices. If the targeted users are already associated, the system grants Licenses automatically to them and pushes the app to their iOS 7+ devices.

   If admin wants to cancel the target, he must choose **Cancel**.

11.7.3.2 Recalling Licenses

The Licenses Granted dialog displays the list of Users who are granted with app licenses. Admin can recall granted licenses from associated users.

1. In **Purchased Apps List tab > Licenses Granted** column, click one of the numbers shown below.



VPP Apps

Last Sync Details

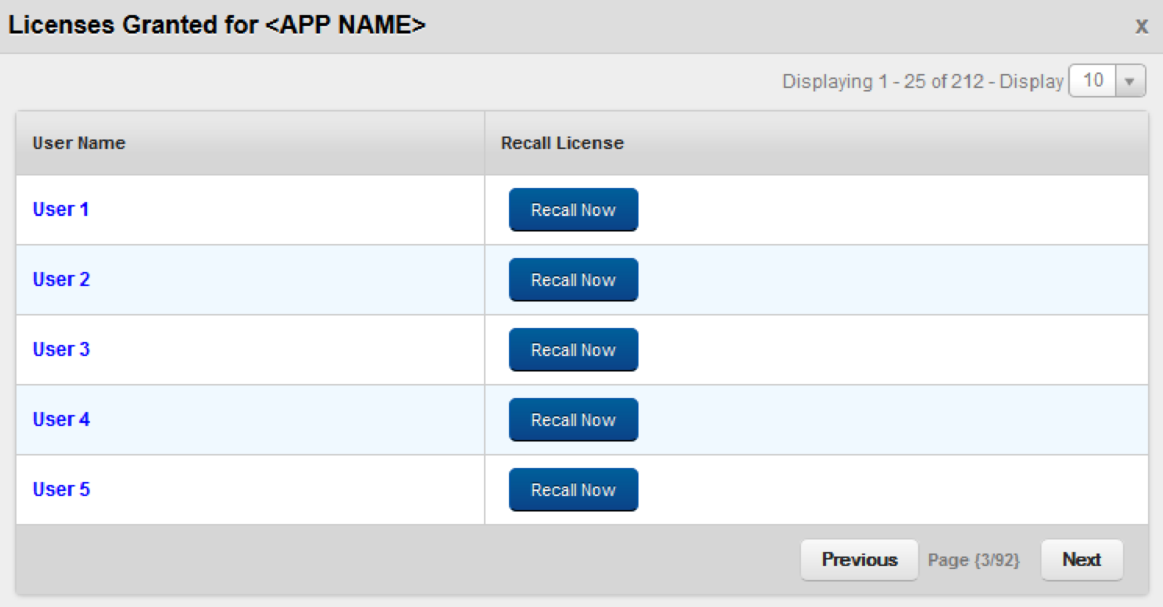
Last Sync 12 Jun, 2014 11:10:51 IST

Click here for
Licenses Granted for

Displaying 1 - 2 of 2 - Display 10

App Name	Licenses Purchased	Licenses Granted	Licenses Remaining	Target Licenses To
Cleaner Pro – Remove Duplicate Contacts for Addressbook, iCloud, Gmail, Yahoo & Outlook	5	0	5	Select Target
iRecorder - One Touch Video Recorder	5	0	5	Select Target

The system displays the **Licenses Granted** dialog.



Licenses Granted for <APP NAME>

Displaying 1 - 25 of 212 - Display 10

User Name	Recall License
User 1	Recall Now
User 2	Recall Now
User 3	Recall Now
User 4	Recall Now
User 5	Recall Now

- **Username**: Displays name of User that is granted the app license.
- **Recall License**: Recall Now button helps to redeems the app licenses against that user.

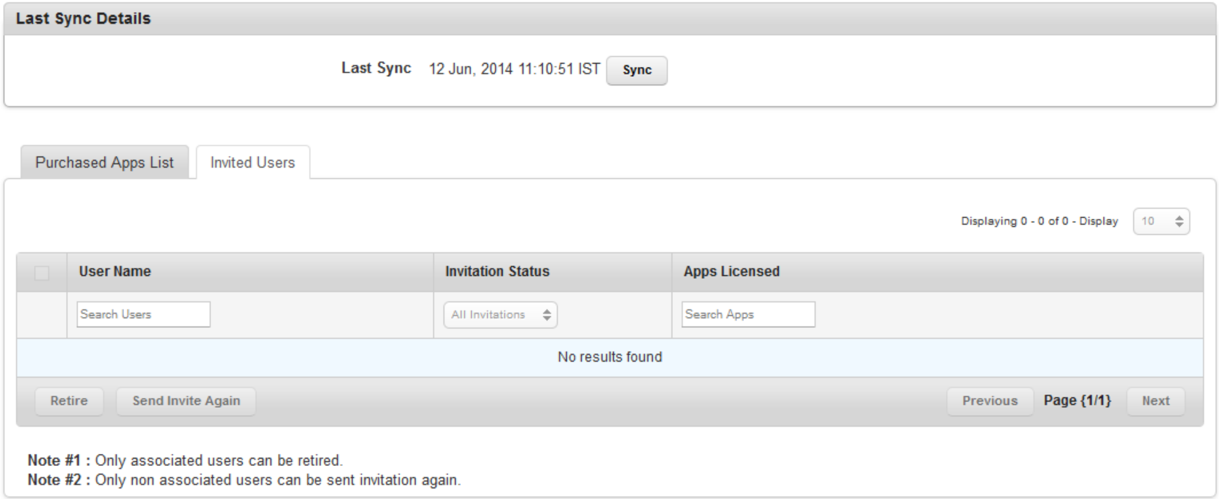
2. Click the **Recall Now** button.
   The system displays a confirmation message. Once confirmed, the app license is redeemed and the number of licenses granted column is modified accordingly. The page returns to the Purchased App List page with the updated details. By default EMM will delete recalled apps from users' devices.

   The user can still download the app from Apple and use it for a 30-day grace period as per Apple.

11.7.4 Invited Users tab

The **Invited Users** tab allows admin to invite users and groups, and retire users, and also sends invitation again to users who are previously invited but not associated. If users who are not in administrators purview are invited, the administrator can only view those users and can not invite or associate or retire those users.

VPP Apps



Last Sync 12 Jun, 2014 11:10:51 IST

Displaying 0 - 0 of 0 - Display 10

User Name	Invitation Status	Apps Licensed
No results found		

Note #1 : Only associated users can be retired.
Note #2 : Only non associated users can be sent invitation again.

The **Invited Users** tab view displays the following columns:

Columns	Description
User Name	Displays the names with domain of users and users from groups who are invited and associated with VPP.
Invitation Status	Displays the invitation status as Invited, Associated or Retired
Apps Licensed	Displays the list of apps granted to an associated user.

11.7.4.1 Retiring a User from VPP

Only associated users can be retired. Once the user is retired, the system recalls all the licenses granted against that user automatically.

Users can pay for the app within that period if they want to use the app later.

To retire a user from VPP, follow these steps:

The admin can choose one or more users and retire them by using the **Retire** action.

1. In the **Invited Users** tab, select the check box next to User Name column.
2. Click the **Retire** button. The system prompts you to confirm the same.

11.7.4.2 Resending an Invitation

Invitations can be sent to only non-associated users. Admin may need to send invitations to users due to several reasons such as an user deleted an invitation or user not responded to an invitation.

To resend an invitation, follow these steps:

1. In the **Invited Users** tab, select the check box next to User Name column.
2. Click the **Send Invite Again** button. The system prompts you to confirm the same.

12. 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 though 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.

12.1 Files Overview

Files are content that is uploaded, targeted, and distributed among groups or users. The following rules apply to the files system:

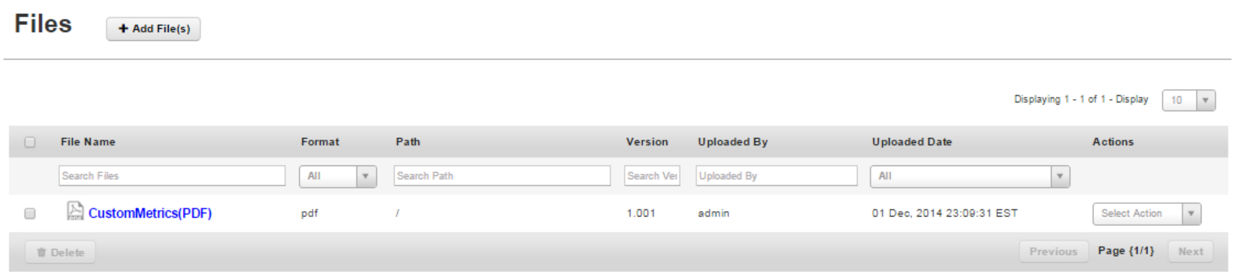
- A file can be part of only one folder. If a file is copied into another folder, the copied file will be treated as a separate file.
- The Files list page shows all files as part of the system, and a user can search for these files. Within folders, all files and folders are shown in a hierarchical view. 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.

12.2 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.

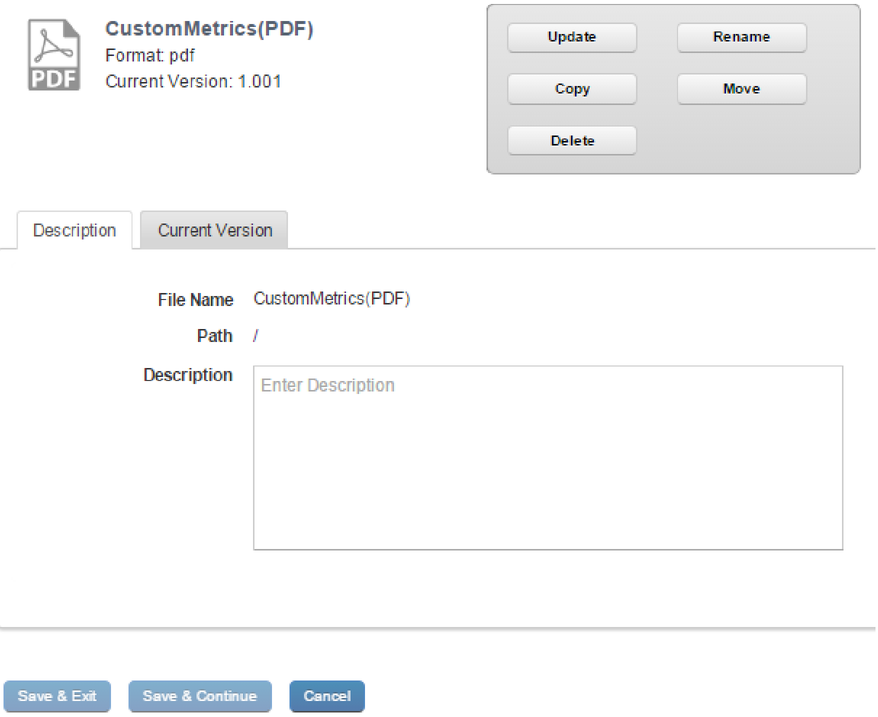
- **Format**: Displays the format of the file.
  - **All**: Search for files based on their specific format. This list contains all allowed file formats.
- **Path**: Displays the location of the file .
  - **Search Path**: If you know the file's path, you can search for the path using this feature.
- **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).



□	File Name	Format	Path	Version	Uploaded By	Uploaded Date	Actions
	Search Files	All	Search Path	Search Ver	Uploaded By	All	
□	CustomMetrics(PDF)	pdf	/	1.001	admin	01 Dec, 2014 23:09:31 EST	Select Action

12.2.1 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

File Name CustomMetrics(PDF)
Path /
Description Enter Description

- **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.

12.3 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.

12.3.1 How to Add a New File

To add a new file, follow these steps:

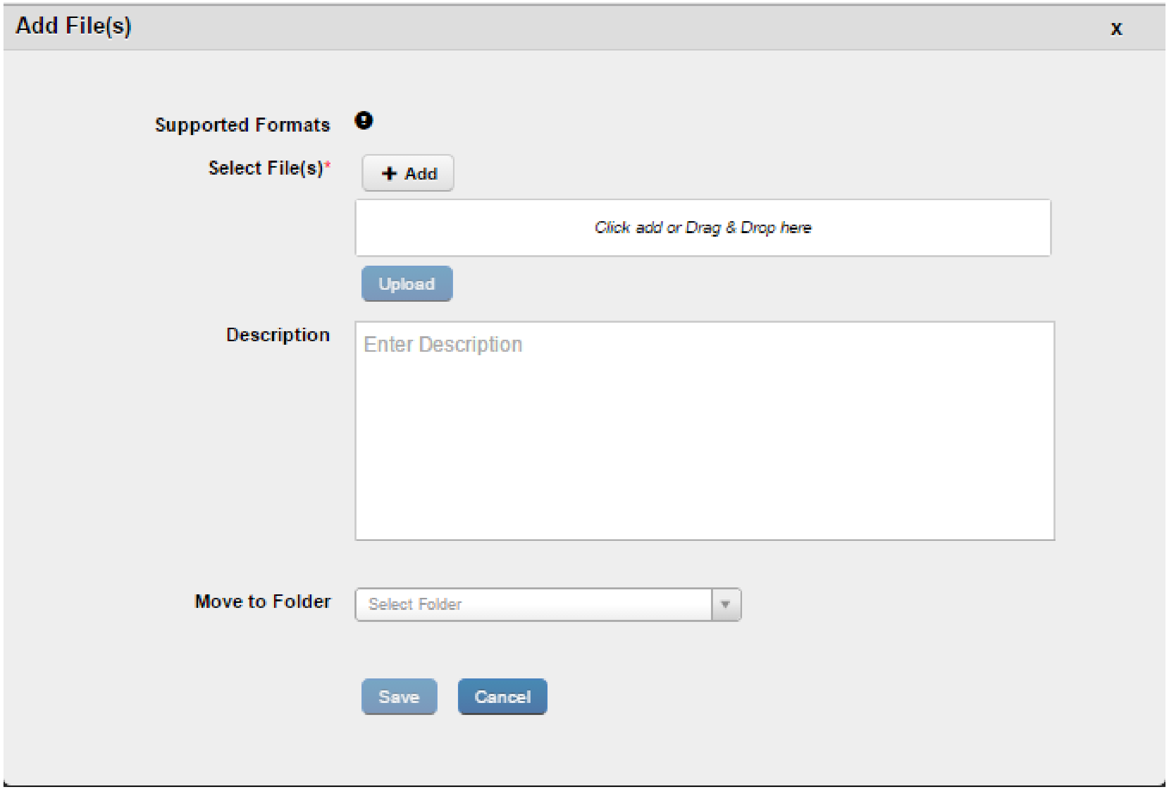
1. In the EMM Management Console, under **Content Management**, click **Files**. The Files page appears.
2. Click **Add File(s)**. The Add File(s) dialog appears.
3. Select file(s). Click to add, or drag and drop.
4. **Click Add**. The Open Dialog appears.
5. Navigate to the file you want to upload, 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.



12.3.2 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**.

12.3.3 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**.

12.3.4 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**.

12.3.5 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**.

12.3.6 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.

12.3.7 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**.

12.3.8 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.

12.3.9 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.

12.3.10 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 Verizon** 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.

12.4 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 polices 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

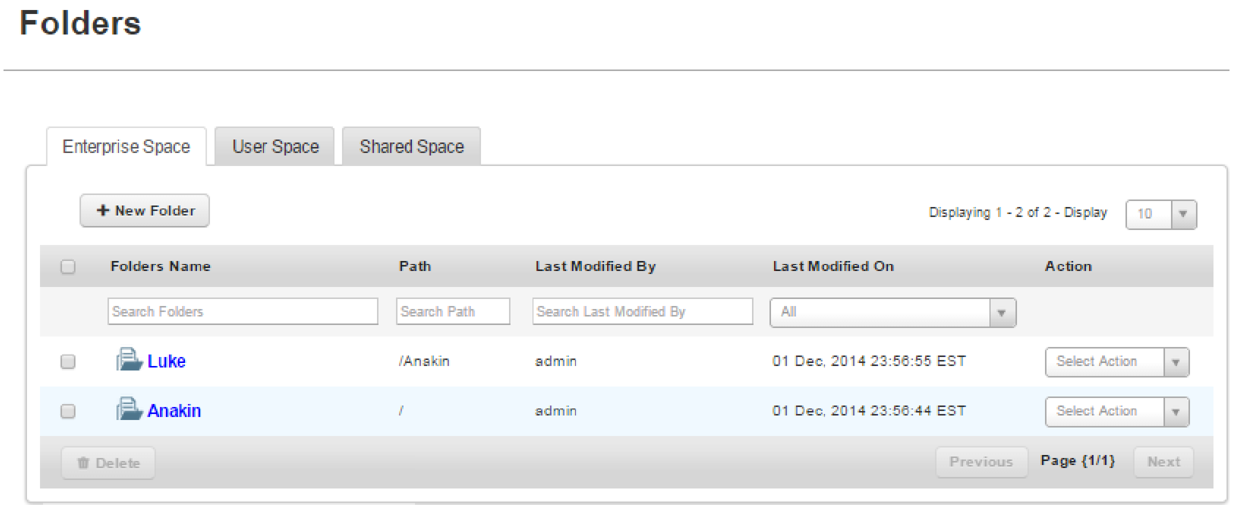
12.5 Folders User Interface

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.

12.5.1 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

Displaying 1 - 2 of 2 - Display 10

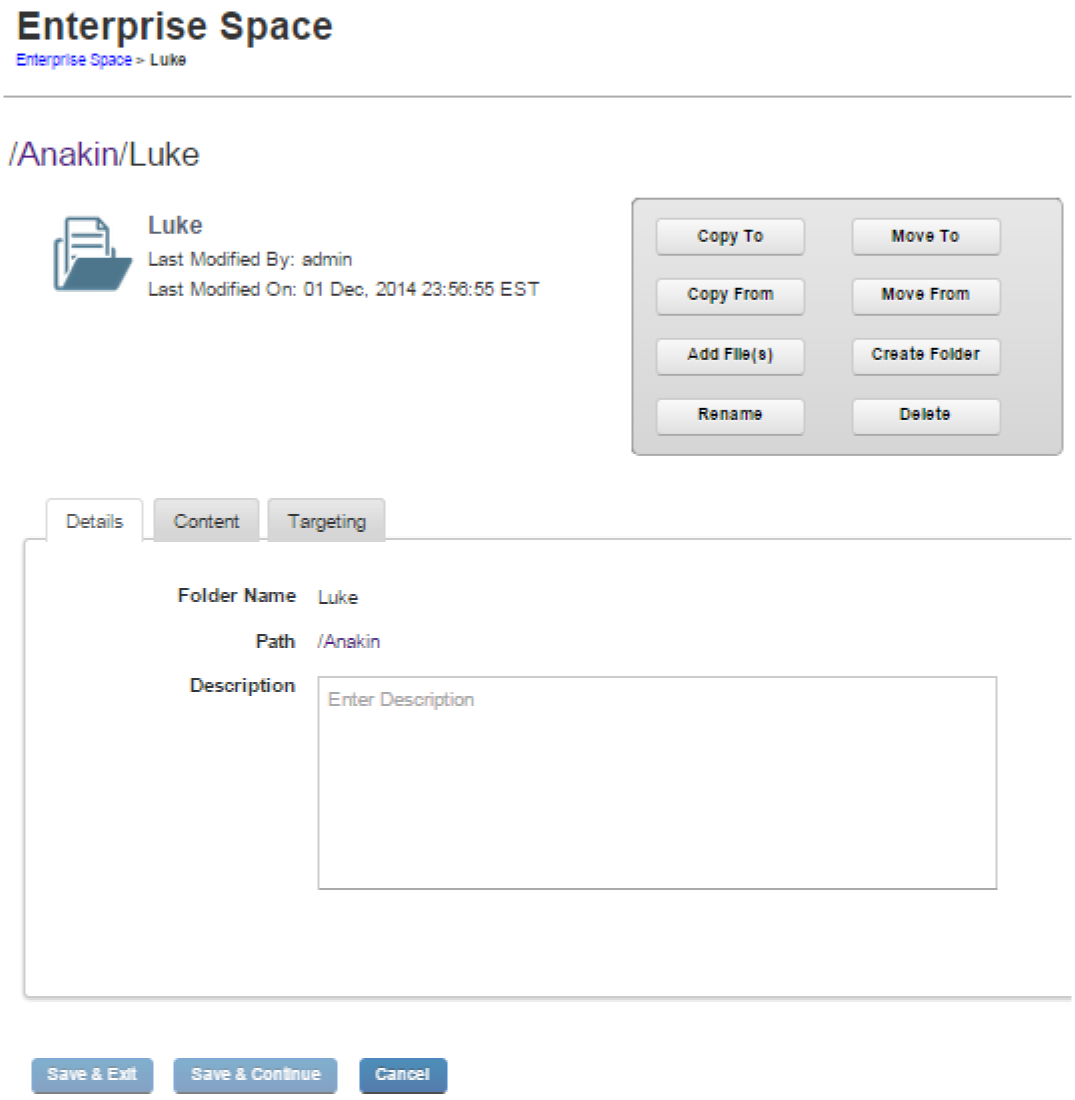
□	Folders Name	Path	Last Modified By	Last Modified On	Action
	Search Folders	Search Path	Search Last Modified By	All	
□	Luke	/Anakin	admin	01 Dec, 2014 23:56:55 EST	Select Action
□	Anakin	/	admin	01 Dec, 2014 23:56:44 EST	Select Action

- **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.

12.5.2 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

Folder Name: Luke

Path: /Anakin

Description: Enter Description

For Enterprise Space folders, a user can perform the following actions.

> ***Important:*** The following actions are not applicable to SharePoint repository folders.

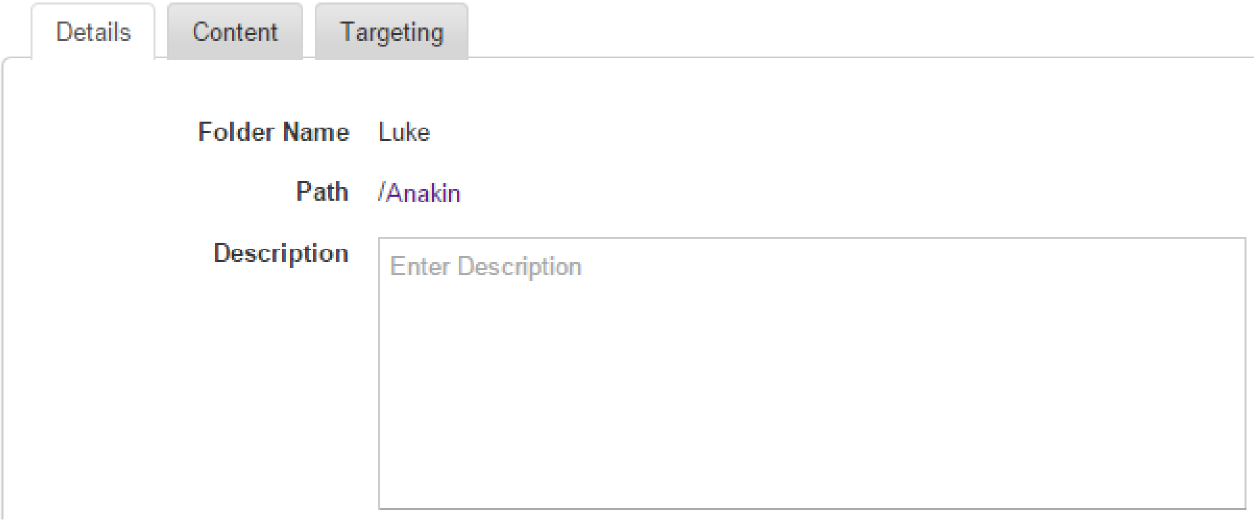
- **Copy to** - A user can copy a folder to a destination a user specifies. All internal files and folders of the folder are also copied to the new destination. If a folder with same name exists in the destination folder, the new folder will be renamed with a suffix (1). The latest version of the file 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.

12.5.2.1 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.



Folder Name Luke

Path /Anakin

Description Enter Description

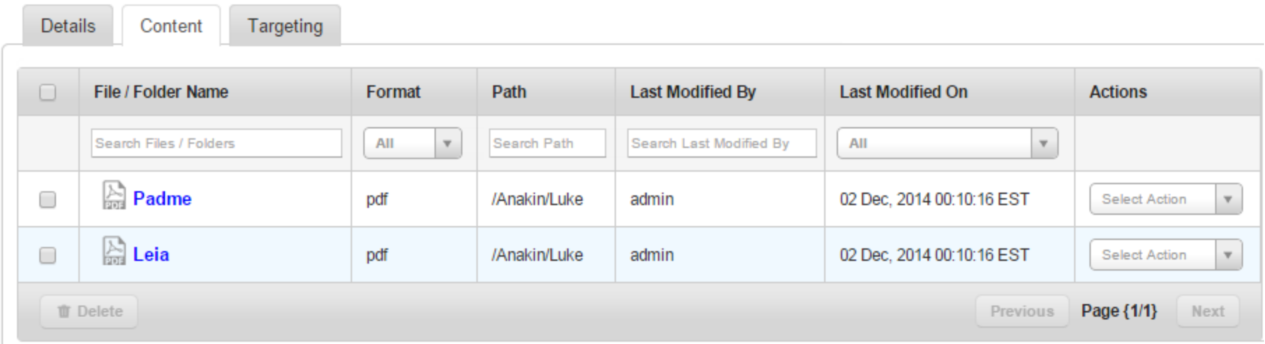
12.5.2.2 Content Tab

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.



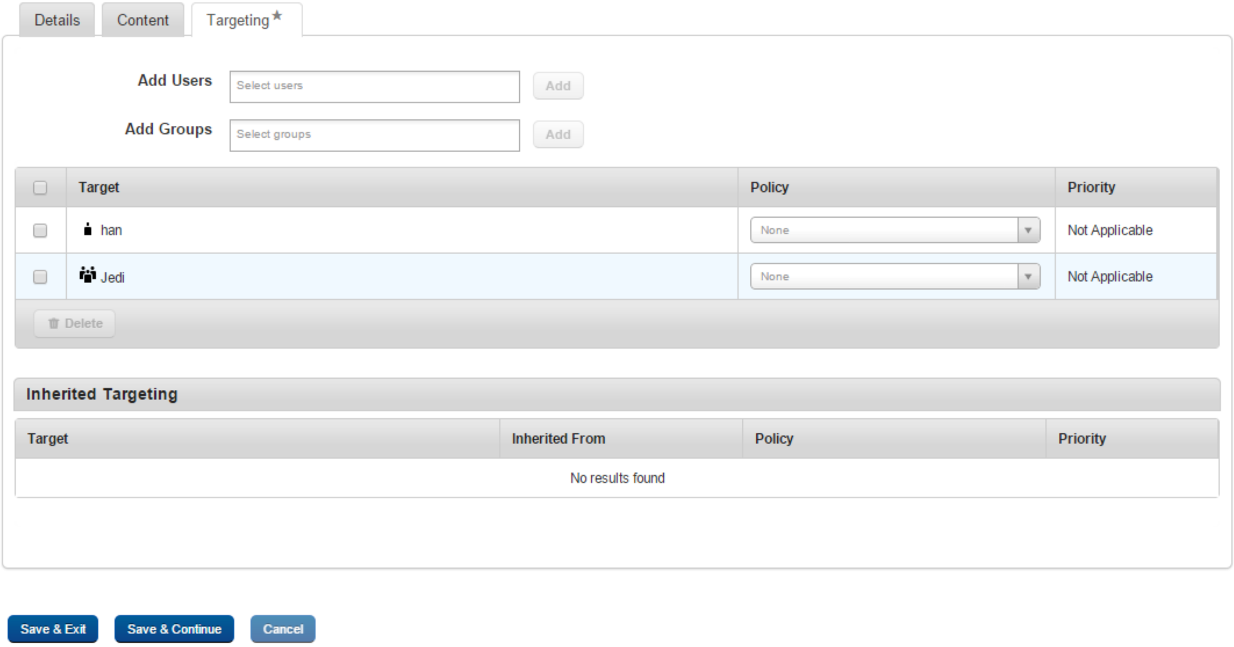
□	File / Folder Name	Format	Path	Last Modified By	Last Modified On	Actions
	Search Files / Folders	All ▾	Search Path	Search Last Modified By	All ▾	
□	Padme	pdf	/Anakin/Luke	admin	02 Dec, 2014 00:10:16 EST	Select Action ▾
□	Leia	pdf	/Anakin/Luke	admin	02 Dec, 2014 00:10:16 EST	Select Action ▾

12.5.2.3 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.



Add Users: Select users

Add Groups: Select groups

□	Target	Policy	Priority
□	han	None	Not Applicable
□	Jedi	None	Not Applicable

Inherited Targeting

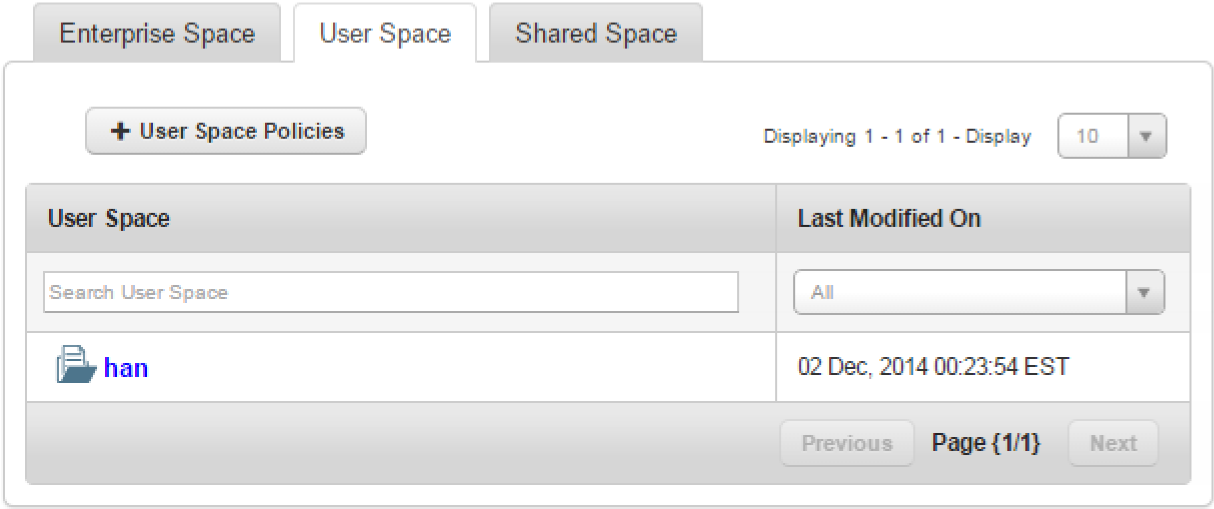
Target	Inherited From	Policy	Priority
No results found			

12.5.3 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.

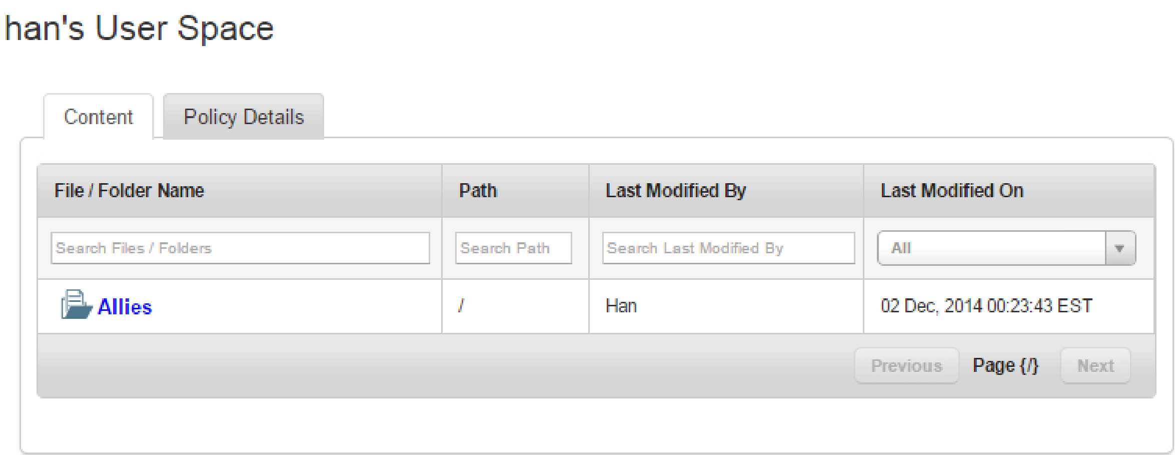


User Space	Last Modified On
Search User Space	All
han	02 Dec, 2014 00:23:54 EST

12.5.3.1 User Space

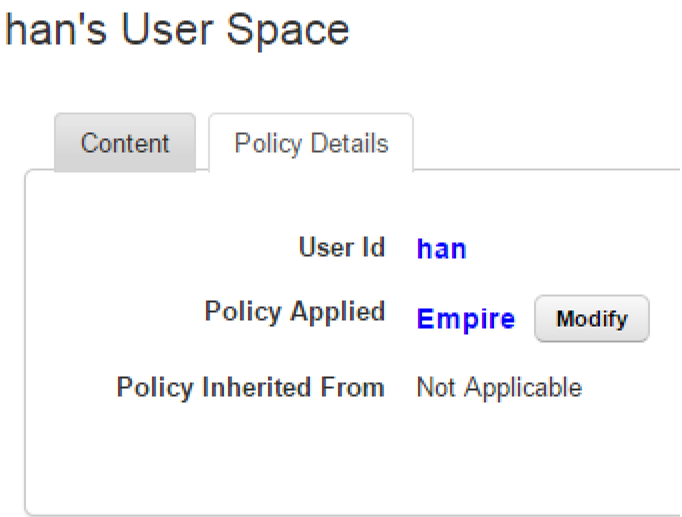
When you click on any of the user's folder, the associated user space page appears.

- **Content**: Displays available content details.



File / Folder Name	Path	Last Modified By	Last Modified On
Search Files / Folders	Search Path	Search Last Modified By	All
Allies	/	Han	02 Dec, 2014 00:23:43 EST

- **Policy Details**: Displays applicable policy.



User Id han
Policy Applied Empire
Policy Inherited From Not Applicable

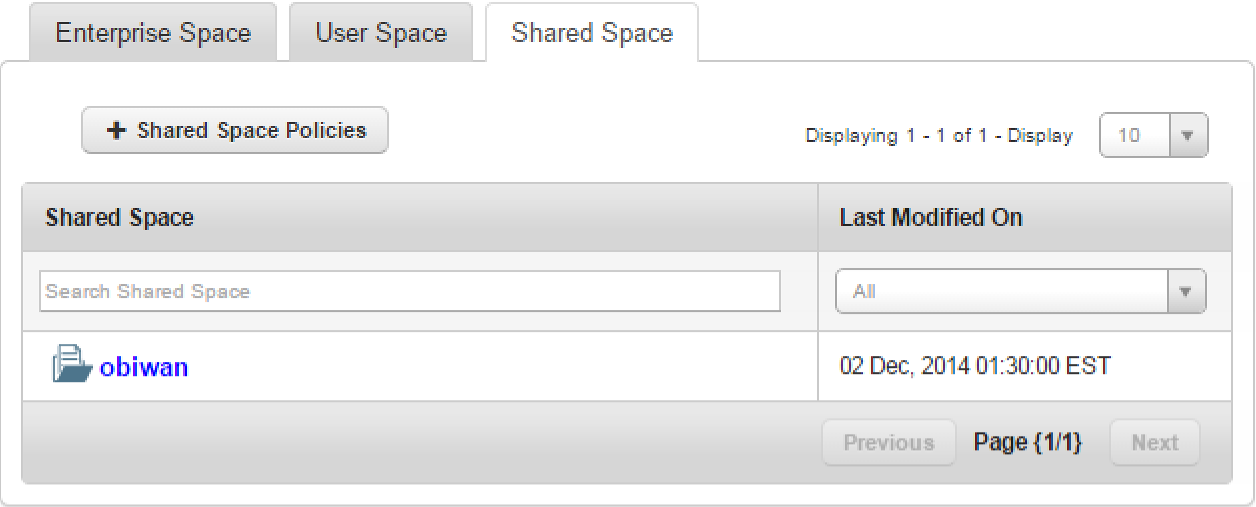
  - **Modify**: Use this button to change the policy that is applied on the folder.

You can view policies applied on users by an administrator in the policy details tab. Only an administrator can modify these policies.

12.5.4 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.



Shared Space	Last Modified On
obiwan	02 Dec, 2014 01:30:00 EST

- **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 .

12.6 Applying Actions to Folders

12.6.1 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.

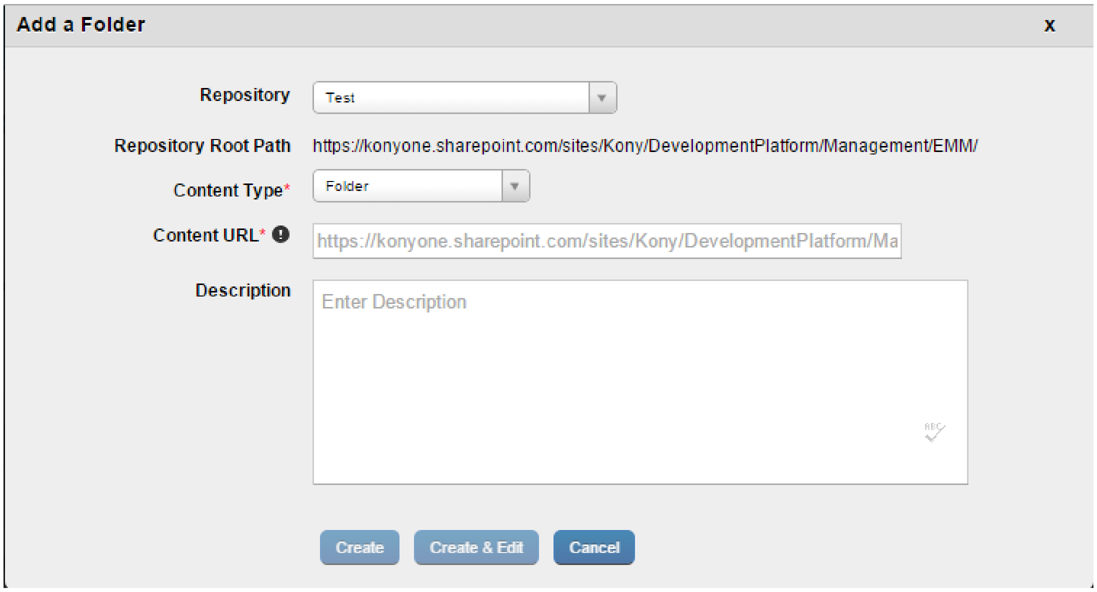
12.6.2 How to Create a New Folder From a SharePoint Repository

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.



Add a Folder

Repository: Test

Repository Root Path: https://konyone.sharepoint.com/sites/Kony/DevelopmentPlatform/Management/EMM/

Content Type*: Folder

Content URL*: https://konyone.sharepoint.com/sites/Kony/DevelopmentPlatform/Ma

Description: Enter Description

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.

12.6.3 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.

12.6.4 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.

12.6.5 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.

12.6.6 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.

12.6.7 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**.

12.6.8 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**.

12.6.9 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**.

12.6.10 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.

12.6.11 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.

12.6.12 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**.

12.6.13 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**.

12.6.14 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.

12.6.15 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.

12.6.16 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.

12.6.17 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**.

12.6.18 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**.

12.6.19 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**.

12.6.20 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**.

12.6.21 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.

12.6.22 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.

12.6.23 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**.

12.6.24 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**.

12.6.25 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.

12.6.26 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.

12.7 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 is 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

12.7.1 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.

12.7.2 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.

12.7.3 Android

- **Allow Access in Android**: By default, this is set to **Yes**.

12.7.4 Windows

- **Allow Access in Windows**: By default, this is set to **Yes**.

12.8 Applying Content Policies

12.8.1 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**.

12.8.2 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.

12.8.3 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.

12.8.4 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.

12.8.5 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.

12.8.6 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.

12.8.7 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.

12.8.8 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**.

12.9 Content Repositories

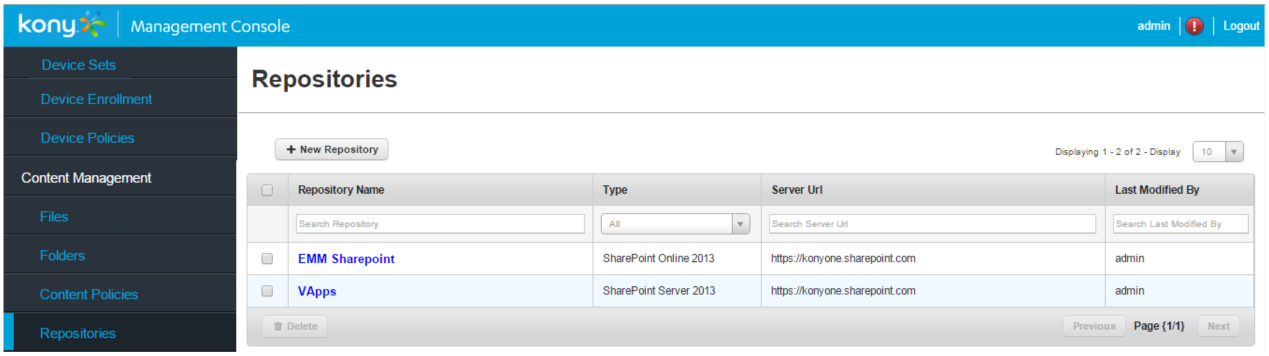
In the Content Management section, before Kony Management Suite 3.5, Enterprise content is uploaded only by an administrator. To extend the enterprise content feature to include files and folders from the enterprise SharePoint, a new Repositories feature is introduced in Kony Management Suite 3.5 GA. 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.

12.9.1 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.



Repositories

Displaying 1 - 2 of 2 - Display 10

☐	Repository Name	Type	Server Url	Last Modified By
	Search Repository	All	Search Server Url	Search Last Modified By
☐	EMM Sharepoint	SharePoint Online 2013	https://konyone.sharepoint.com	admin
☐	VApps	SharePoint Server 2013	https://konyone.sharepoint.com	admin

Page {1/1}

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: • 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.

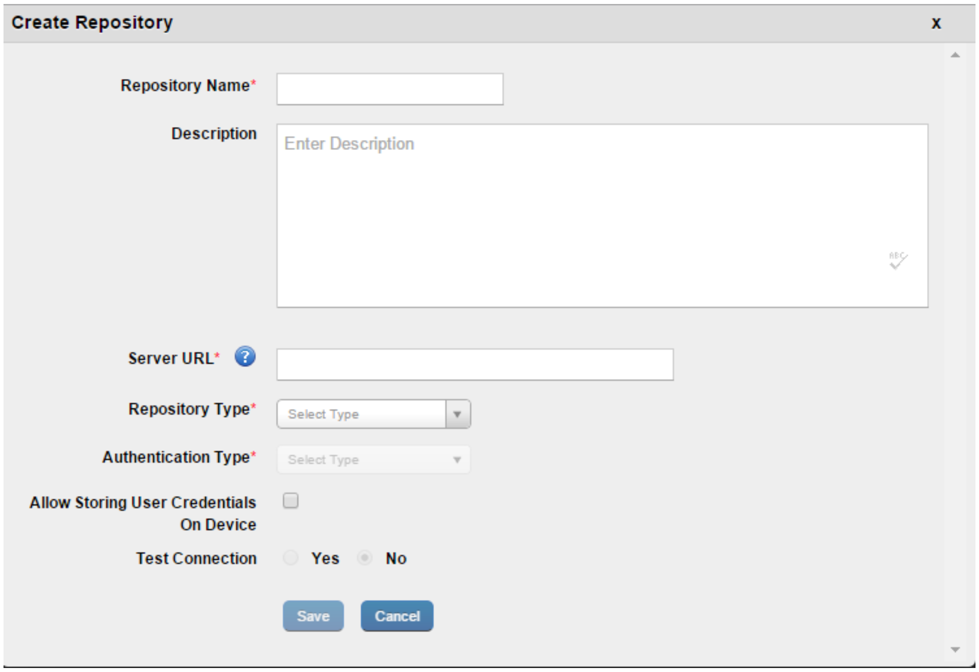
You can do the following from the Repositories page:

- Add a new repository
- Update a repository
- Search for a repository
- Delete a repository

12.9.2 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.



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.

12.9.3 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**.

12.9.4 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.

13. Self Service Console

Self Service Console includes following sections:

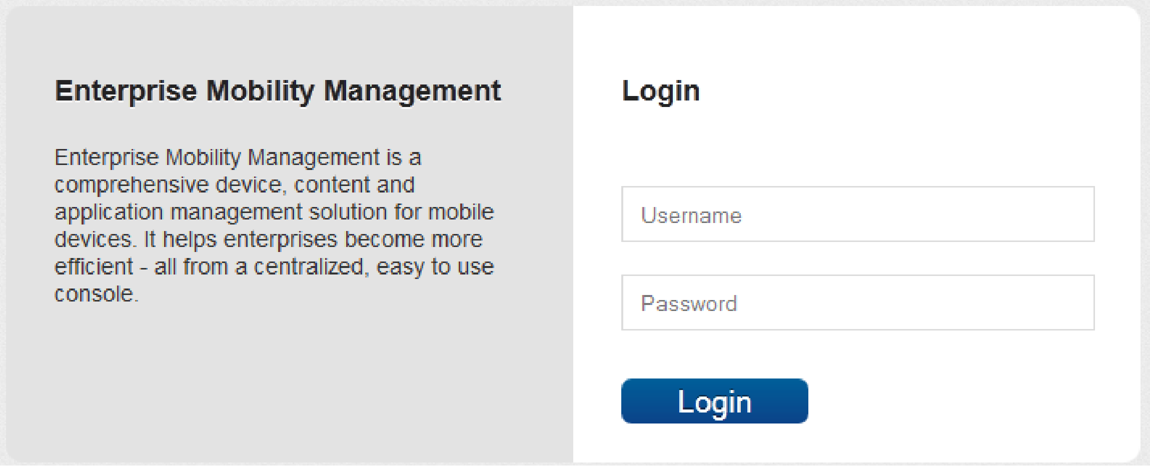
- Home
- Devices
- Content

> ***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.

13.1 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.

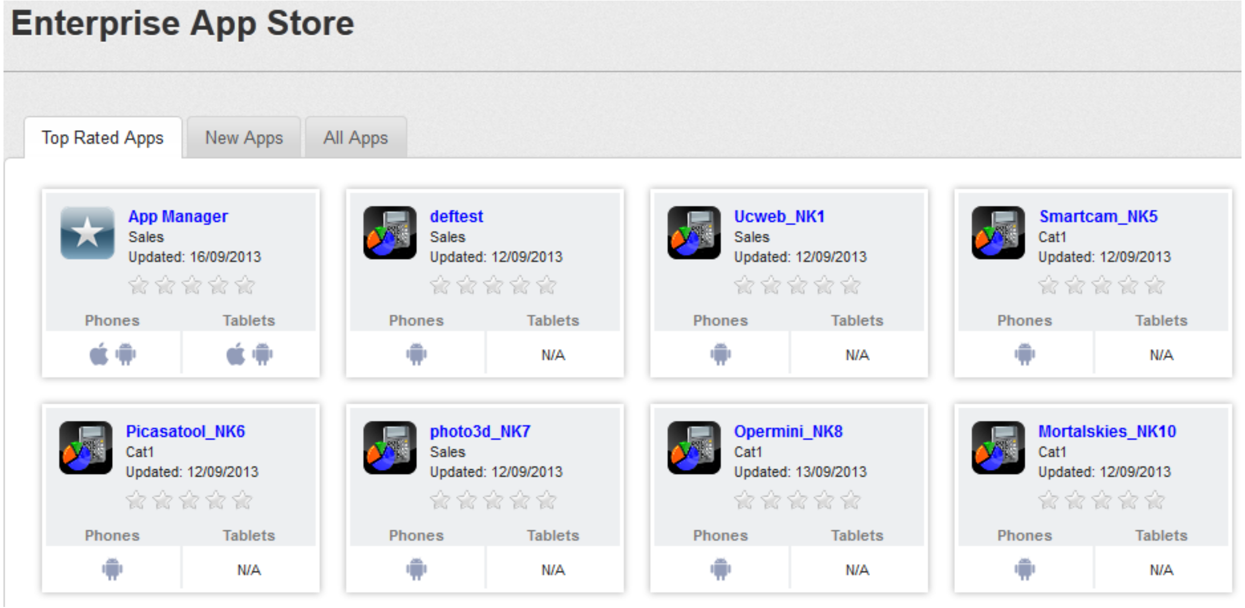
1. Open an Internet browser.
2. Enter the EMM URL in the Address field of the browser. The EMM Console Login screen appears.
3. **User Name**: Enter the user name in the **User name** text field.
4. **Password**: Enter the password in the **Password** text field.
5. Click the **Login** button. After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

13.2 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.



App Manager
Sales
Updated: 16/09/2013

deftest
Sales
Updated: 12/09/2013

Ucweb_NK1
Sales
Updated: 12/09/2013

Smartcam_NK5
Cat1
Updated: 12/09/2013

Picasatool_NK6
Cat1
Updated: 12/09/2013

photo3d_NK7
Sales
Updated: 12/09/2013

Opermini_NK8
Cat1
Updated: 13/09/2013

Mortalskies_NK10
Cat1
Updated: 12/09/2013

The Enterprise App Store page appears with three tabs.

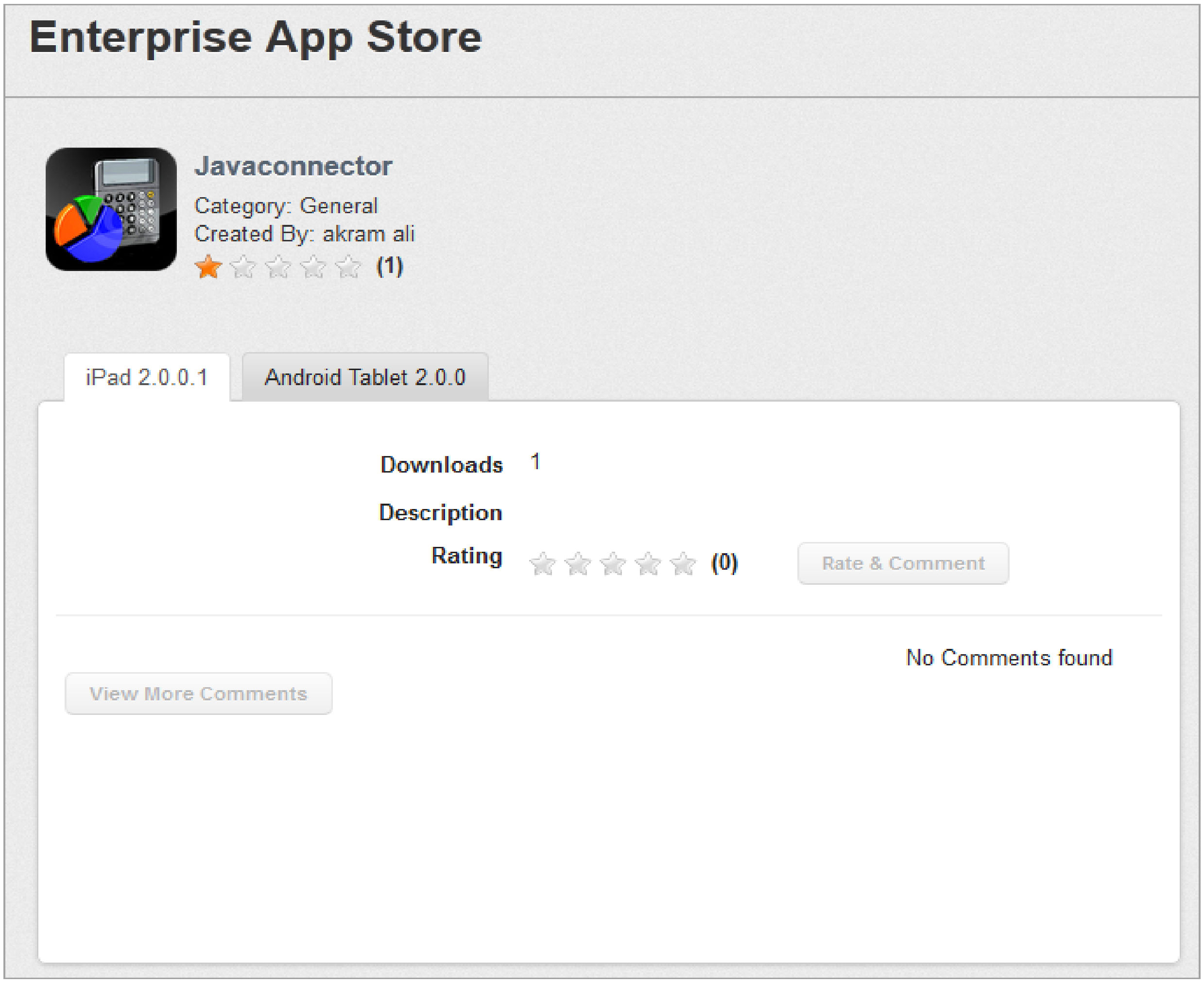
- Top Rated Apps
- New Apps
- All Apps

By default, Top Rated Apps tab is set to active.

13.2.1 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)

Downloads 1

Description

Rating ☆☆☆☆☆ (0)

No Comments found

- Rate and Comment your App

To rate and comment your app, follow these steps:

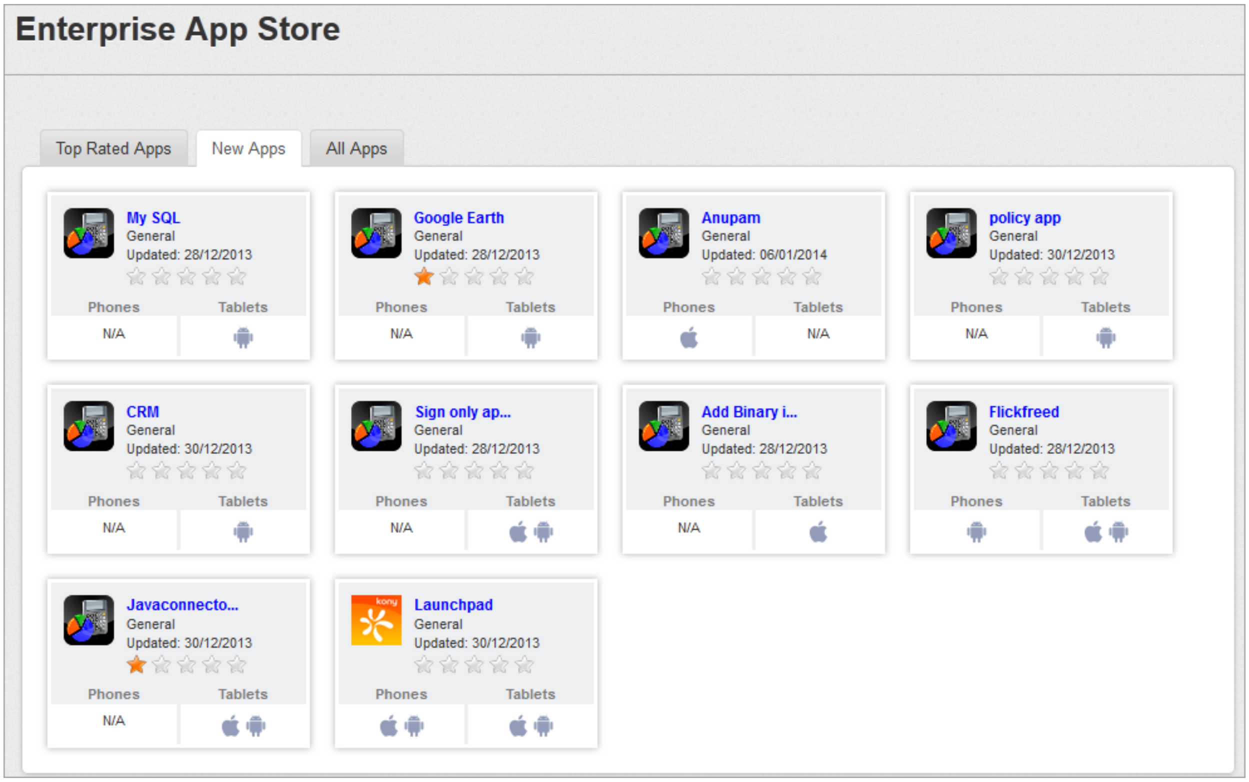
1. **Description**: Enter the comments in the Description text box.
2. **Rating**: Select the number of star icons to rate the app.
3. Click the **Rate and Comment** button to save the details.

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.

13.2.2 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:

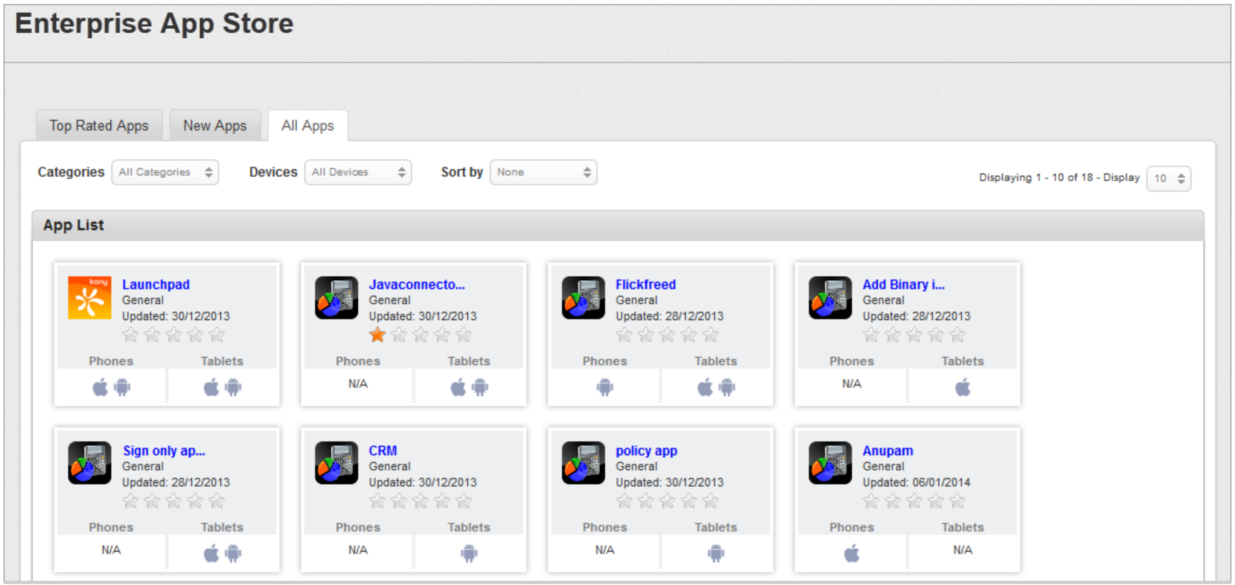
1. **Description**: Enter the comments in the **Description** text box.
2. **Rating**: Select the number of star icons to rate the app.
3. Click the **Rate and Comment** button to save the details.

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.

13.2.3 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.



Categories: All Categories
Devices: All Devices
Sort by: None
Displaying 1 - 10 of 18 - Display: 10

You can perform the following activities from the All Apps page:

- Searching for Enterprise Apps
- Rate and Comment your App

13.2.4 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.

13.2.5 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.

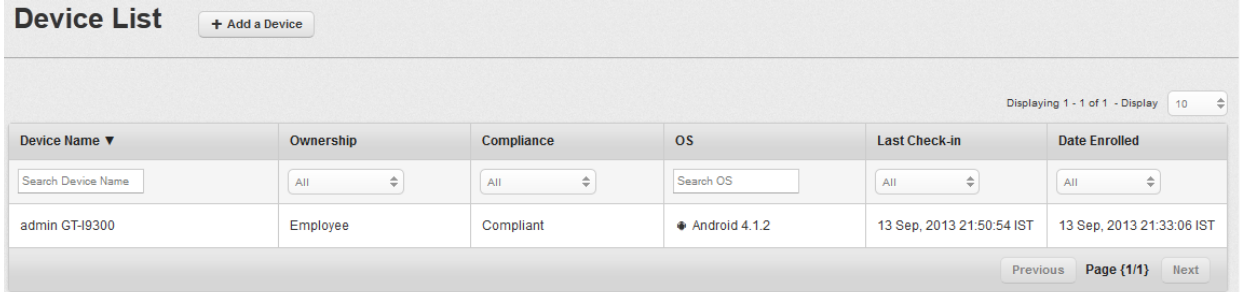
Click the **View More Comments** button to view other review comments posted by other users.

13.3 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 , Check Compliance Status, Date Enrolled, Last Check-in etc. .

The Devices section pertains to role based device enrollment. 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 enrolled 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 List

Displaying 1 - 1 of 1 - Display 10

Device Name ▼	Ownership	Compliance	OS	Last Check-in	Date Enrolled
Search Device Name	All	All	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

Page {1/1}

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, Enrolled, Registered, Deactivated, Retired, Lost, or Control Removed.
Ownership	Displays the owner name, for example, Corporate owned, Employee owned or Shared.
Compliance	Displays, if the device is compliant or non-compliant to the EMM console.

Columns	Description
OS	Displays the operating system to which the device supports.
Last Check-in	Displays when the device was last checked in to EMM Console, for example, Today, Yesterday or Last 7 Days.
Date Enrolled	Displays when the device was enrolled to EMM Console, for example, Today, Yesterday or Last 7 Days.

You can perform the following activities from this page:

- Adding a New Device
- Searching for an Enrolled Device

13.3.1 Adding a New Device

This process falls under Device based Enrollment. These devices are enrolled to Mobile Device Management Server.

The Add a Device window includes three steps to enroll a new device to EMM.

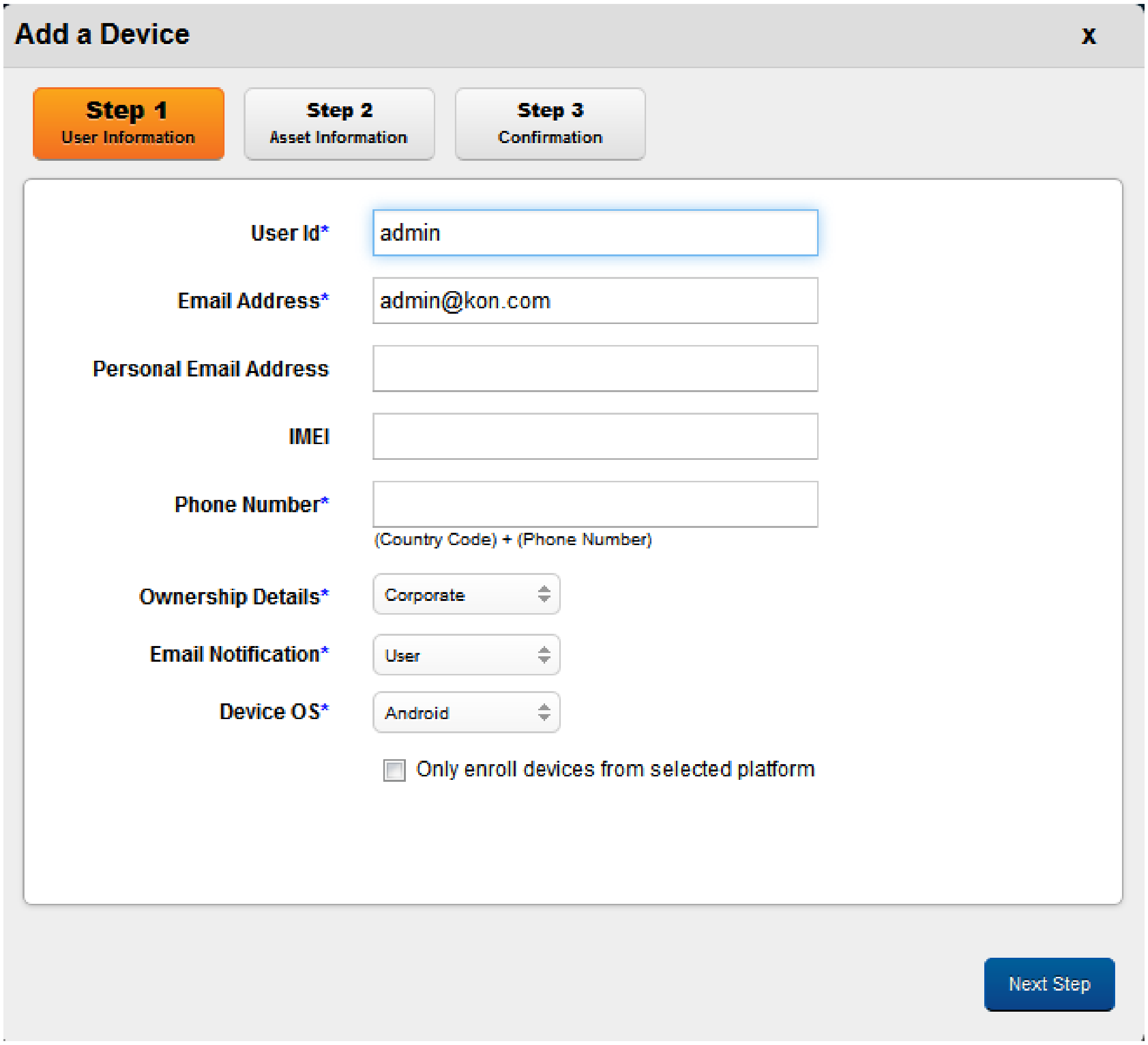
- Step 1: User Information
- Step 2: Asset Information
- Step 3: Confirmation

Step 1: **User Information**

To add a new device, follow these steps:

Device List
+ Add a Device

1. To open the Add a Device window, click the **+ Add a Device** button next to the Device List label at the top of the page.



Add a Device

User Id*: admin

Email Address*: admin@kon.com

Personal Email Address:

IMEI:

Phone Number*:

(Country Code) + (Phone Number)

Ownership Details*: Corporate

Email Notification*: User

Device OS*: Android

□ Only enroll devices from selected platform

The **Add a Device** window appears.

2. Enter the following details under Step One:
3. **User ID**: This field pre-populates from the Active Directory or local database.

   The User Names are populated through Active directory or local database and as per enrolled user id; the respective email id is populated in to Email Address field.
4. **Email Address**: As per enrolled User name, the corresponding email address is populated in the **Email Address** field.

The enrollment request and registration instructions are sent to the user on this email address.

5. **Personal Email Address**: Enter your personal email address for communication through email.
6. **IMEI**: Enter the Mobile Equipment Identity number.

   If you enter wrong IMEI, you receive warning message stating that only digits with at least 15 characters should be entered.
7. **Phone Number:** Enter your Phone number.

   If you enter wrong phone number, you receive warning message stating that at least 11 characters should be entered.
8. **Ownership Details**: Select the appropriate ownership details from the drop-down list under which device falls, for example, Corporate, Employee or Shared.

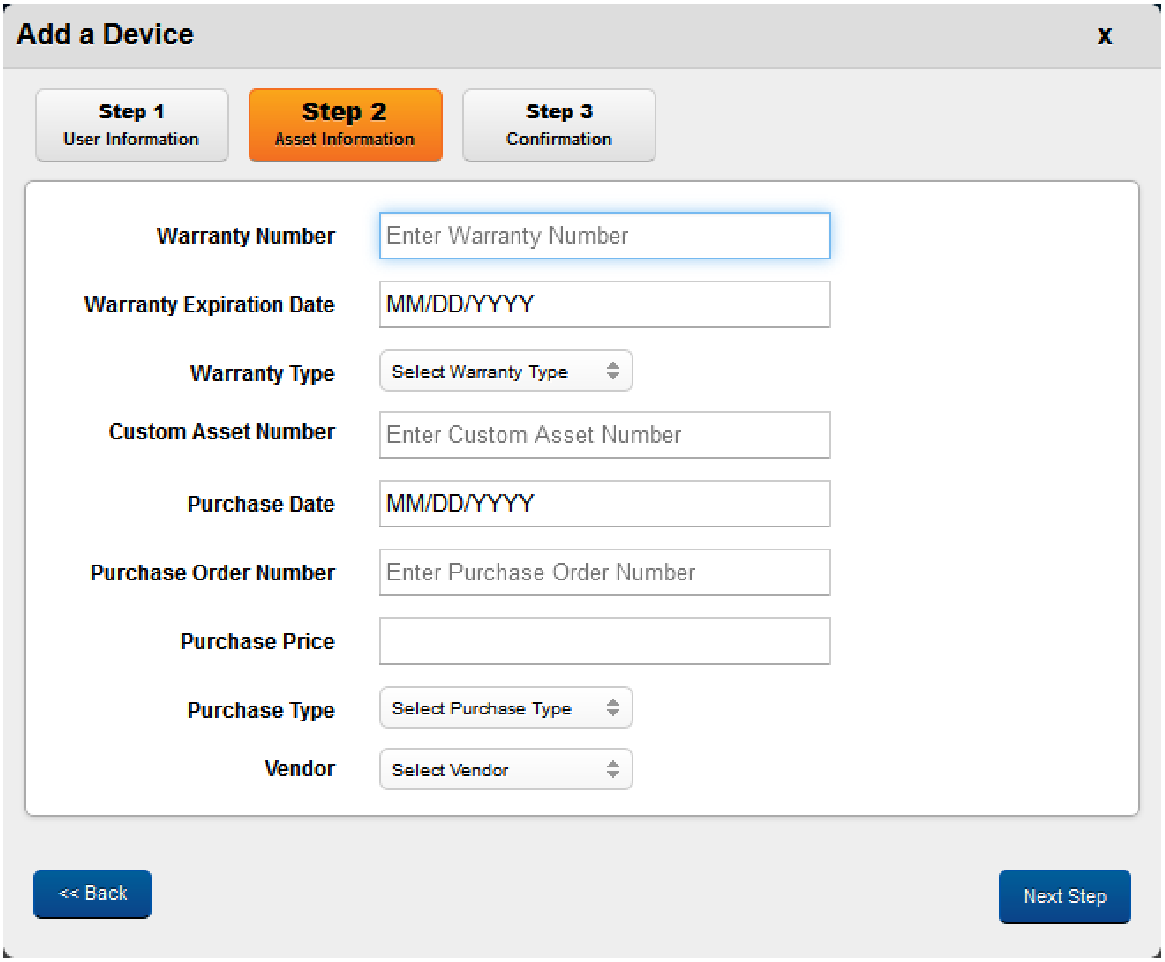
   This pertains to ownership of the device. The device can be owned by an employee, or Corporate, or shared between an employee and the Corporate.
9. **Email Notification**: Select the appropriate option for email notification, for example, User or Admin and User.

   Email notifications are sent to individual User or User Groups regarding enrollment of the device and what further actions are required to accomplish the task.
10. **Device OS**: Select the appropriate Operating system, to which device supports, for example, Android, iPhone, iPad, or Windows.
11. Click the **Next Step** button to open **Step 2** window.

    > ***Note:*** If you wish to enroll devices from the selected platform only, then select the check box" Only enroll devices from selected platform."

Step 2: Asset Information

1. Enter the following details in Step Two:



Add a Device

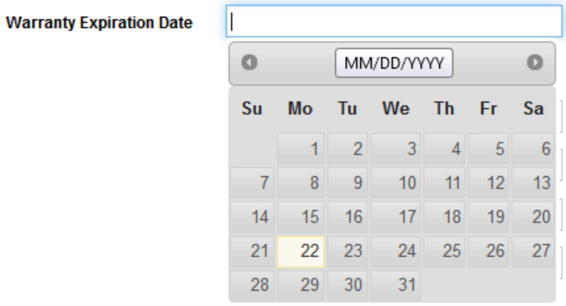
Warranty Number	Enter Warranty Number
Warranty Expiration Date	MM/DD/YYYY
Warranty Type	Select Warranty Type
Custom Asset Number	Enter Custom Asset Number
Purchase Date	MM/DD/YYYY
Purchase Order Number	Enter Purchase Order Number
Purchase Price	
Purchase Type	Select Purchase Type
Vendor	Select Vendor

a. **Warranty Number**: Enter the valid warranty number.

   Unique identification number to identify the warranty type.

b. **Warranty Expiration Date**: Enter the cursor in the **Warranty Expiration Date** field. The Calendar window with current month and current date as active appears. Select the required date. The date is populated in the text field.

   Warranty expiration pertains to a service plan offered under which routine preventive and maintenance are done from the date of purchase until the stipulated time frame. After this period, the warranty expires.



Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

c. **Warranty Type**: Select the appropriate warranty from the **Select Warranty Type** drop-down list.

There are three warranty types respectively, the Manufacturer Warranty, Seller Warranty and the Extended Warranty.

d. **Custom Asset Number**: Enter the valid custom asset number in the **Enter Custom Asset Number** text field.

This number is given by company to define asset information.

e. **Purchase Date**: Enter the cursor in the **Purchase Date** field.

Calendar window with current month and current date as active appears. Select the required date. The date is populated in the text field. Be aware that the purchase date cannot be a future date.

f. **Purchase Order No**: Enter the purchase order number of the device in the **Enter Purchase Order Number** text field.

A purchase order number is an alphanumeric code that is assigned to a particular request to buy something. PO numbers are used internally to track purchases.

g. **Purchase Price**: Enter valid purchase price for the device.

If you enter wrong purchase price, you receive a warning message stating that valid purchase price should be entered.

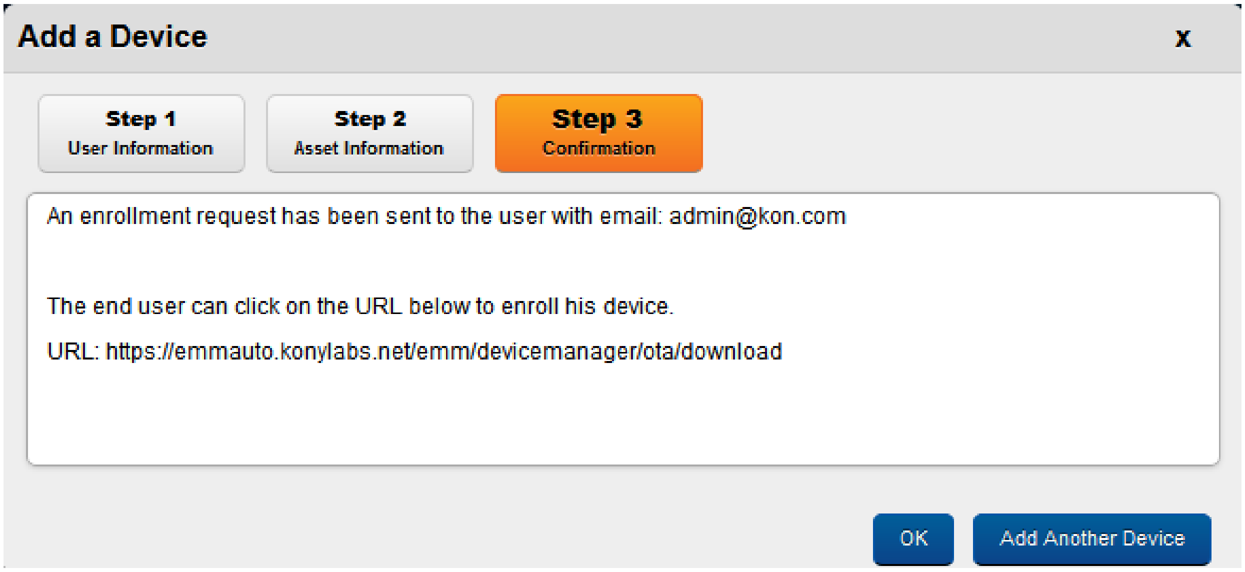
h. **Purchase Type**: Select Purchase Type as **Single Purchase** or **Volume Purchase** from the **Select Purchase Type** drop down list.

   There are two types, Single purchase and Volume purchase.

2. Click the **Back** button to navigate to **Step 1**.
3. Click the **Submit** button to open **Step 3** window.

Step 3: Confirmation

Step Three window displays confirmation message stating that the enrollment request and registration instructions are sent at the specified email address of the administrator.



An enrollment request has been sent to the user with email: admin@kon.com

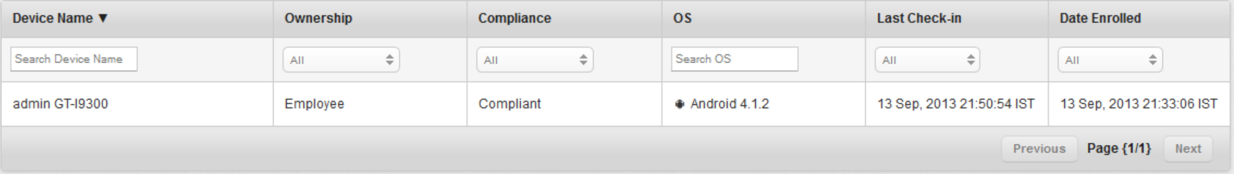
The end user can click on the URL below to enroll his device.

URL: https://emmauto.konylabs.net/emm/devicemanager/ota/download

1. Click the **OK** button to proceed.
2. Click the **Add Another Device** button to open **Step One** window to enroll a new device with EMM.

13.3.2 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
Search Device Name	All	All	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

1. Enter or select details for following search filters:
    a. **Device Name**: Enter partial or a complete device name in the **Search Devices** text field.

    b. **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.

    c. **Compliance**: Select the compliance type from the drop-down list.

       Provides a list of compliance (Policies) details of the device, for example, Compliant or Non-Compliant.

    d. **OS**: Enter desired operating system name in the **Search OS** text field.

    e. **Last Check-in**: 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.

    f. **Date Enrolled**: Select the date on which the device is enrolled to EMM from the drop-down list.

Provides a list of dates the policy was enrolled, 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.

13.4 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.

13.5 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:

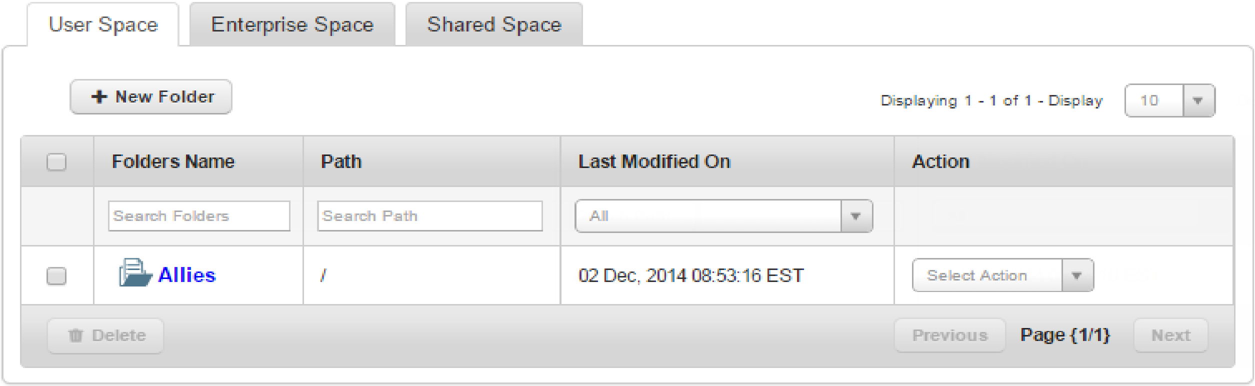
- Create a new folder
- Delete a folder
- Add content to a folder
- Modify content in a folder
- Share content with other users

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.

13.5.1 User Space

User space contains details of content uploaded by a user.



□	Folders Name	Path	Last Modified On	Action
	Search Folders	Search Path	All	
□	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.

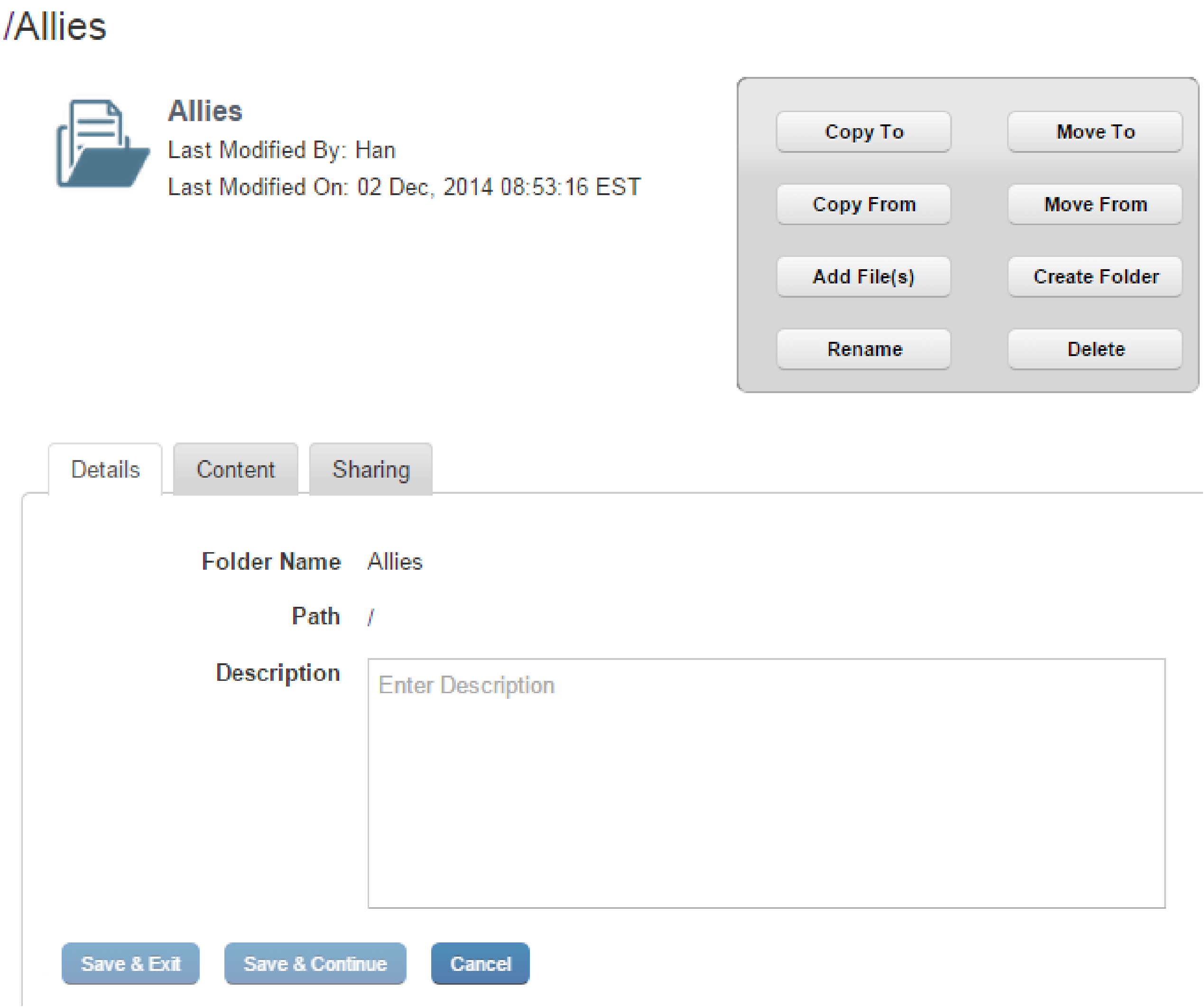
- **Action**: A list of actions you can take on the folder.
  - **Select Action**: Options are Copy To and Move To.
- **Delete**: You can delete a folder.
- **Previous**: Clicking this button will take you to the previous page.
- **Next**: Clicking this button takes you to the next page.

13.5.1.1 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

Folder Name Allies

Path /

Description Enter 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.

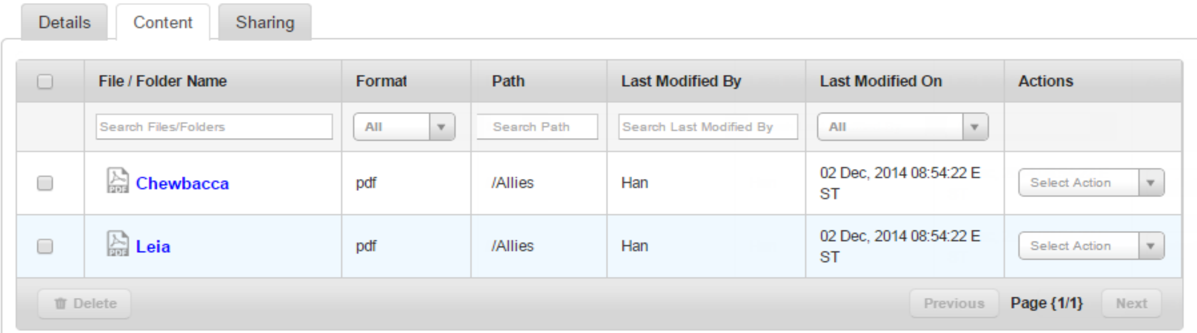
Details Tab

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.



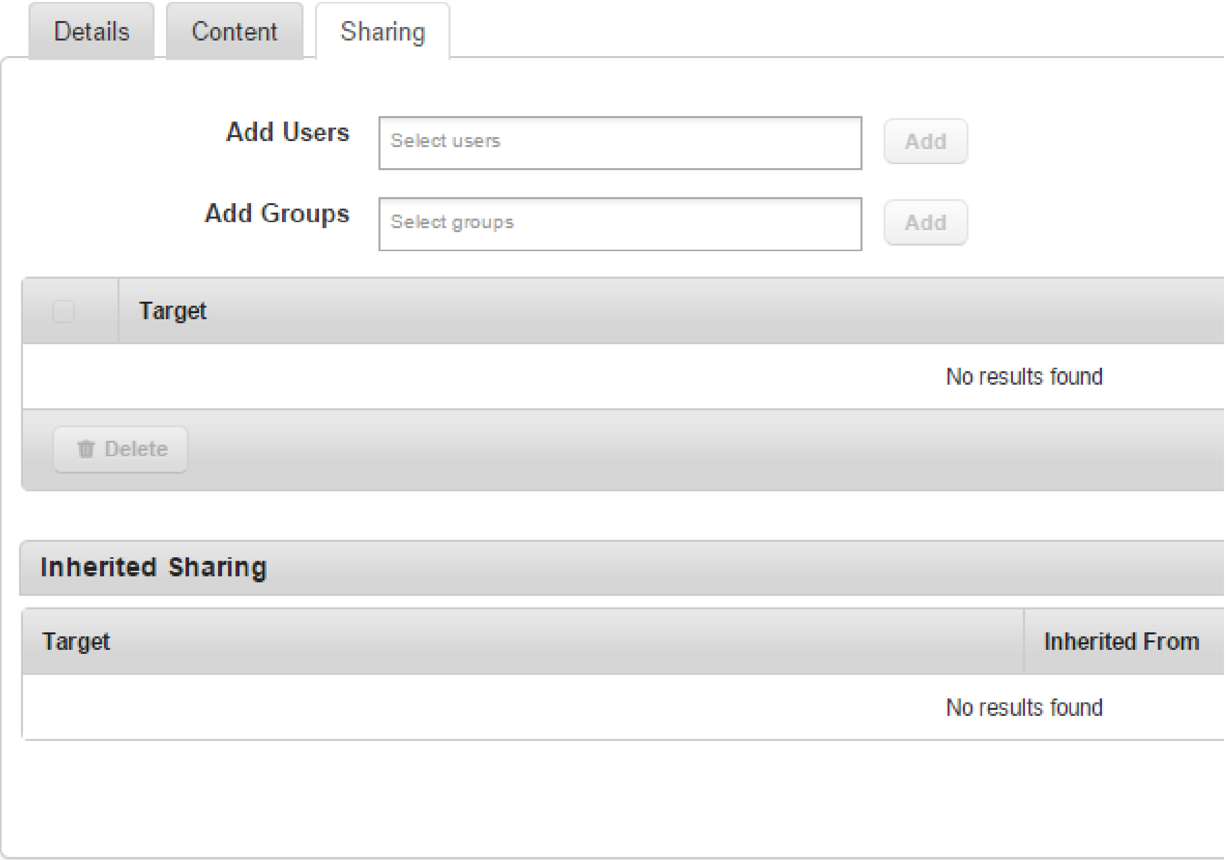
□	File / Folder Name	Format	Path	Last Modified By	Last Modified On	Actions
	Search Files/Folders	All ▾	Search Path	Search Last Modified By	All ▾	
□	Chewbacca	pdf	/Allies	Han	02 Dec, 2014 08:54:22 EST	Select Action ▾
□	Leia	pdf	/Allies	Han	02 Dec, 2014 08:54:22 EST	Select Action ▾

- **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.



□	Target
	No results found

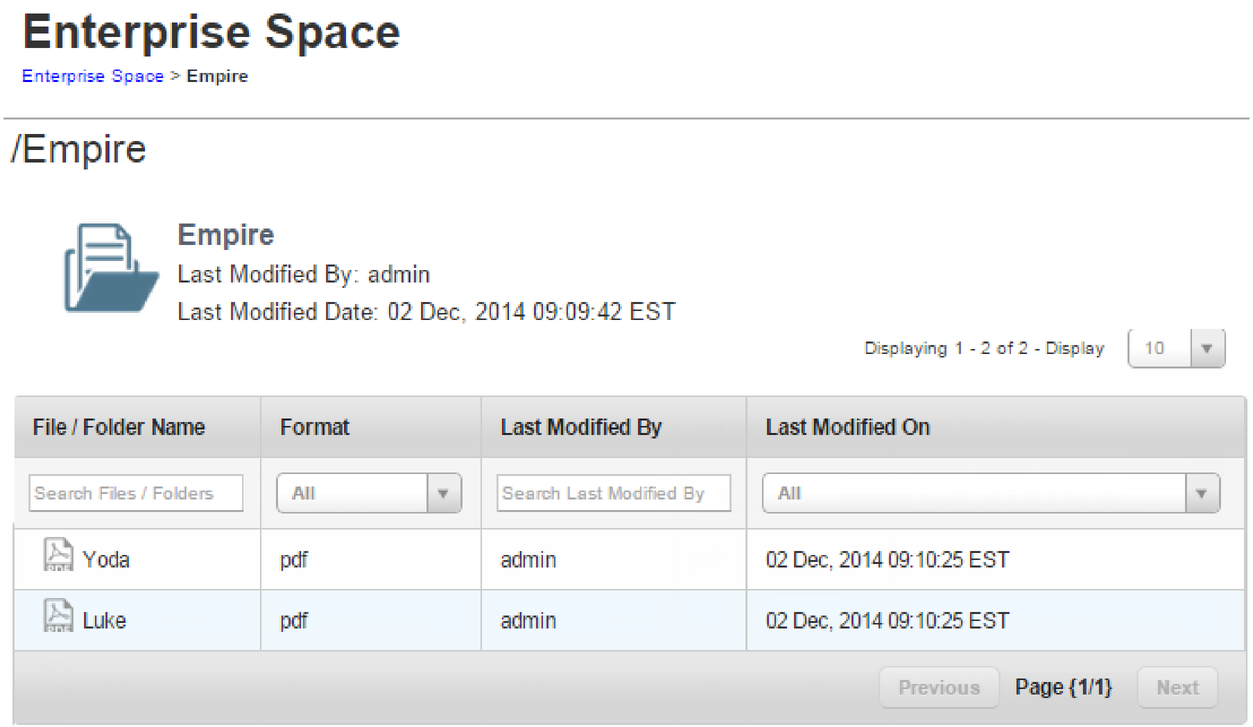
Target	Inherited From
No results found	

- **Add Users**: Enter names of uses 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.

13.5.2 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 10

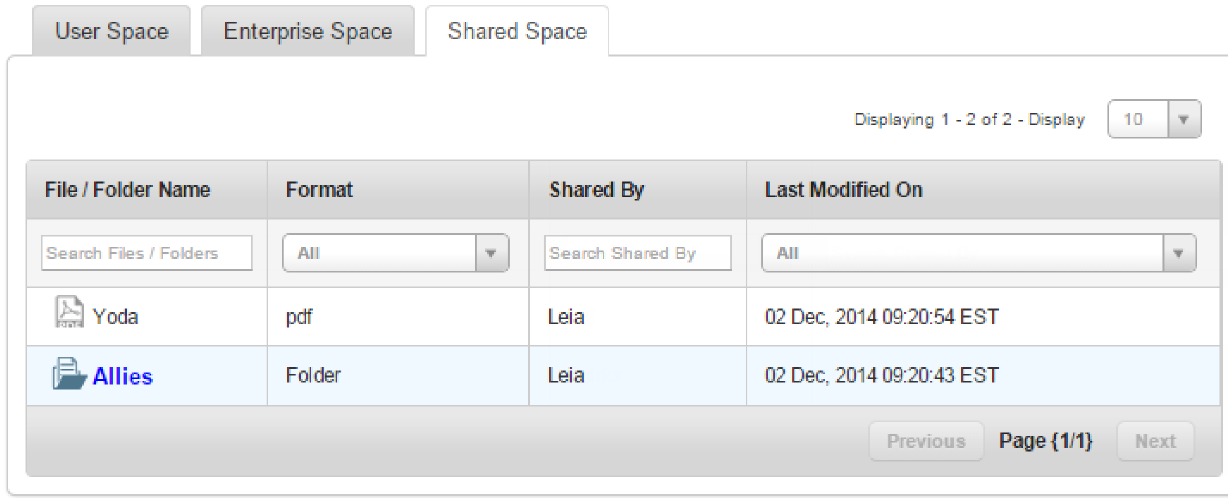
File / Folder Name	Format	Last Modified By	Last Modified On
Search Files / Folders	All	Search Last Modified By	All
Yoda	pdf	admin	02 Dec, 2014 09:10:25 EST
Luke	pdf	admin	02 Dec, 2014 09:10:25 EST

- **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.

13.5.3 Shared Space

The Shared Space contains files and folders shared with the user by other users from their user space.



File / Folder Name	Format	Shared By	Last Modified On
Search Files / Folders	All	Search Shared By	All
Yoda	pdf	Leia	02 Dec, 2014 09:20:54 EST
Allies	Folder	Leia	02 Dec, 2014 09:20:43 EST

- **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.

13.6 Applying Features of the Self-Service Console

13.6.1 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.

13.6.2 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.

13.6.3 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.

13.6.4 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.

13.6.5 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.

13.6.6 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**.

13.6.7 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**.

13.6.8 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**.

13.6.9 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 fle name appears.

7. Click the file name to select the file, and then click **Move**.

8. A **Move From Successful** message appears. Click **OK**.

13.6.10 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.

13.6.11 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.

13.6.12 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**.

13.6.13 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.

13.7 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 exits. 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.

13.8 Applying Actions to Files

13.8.1 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**.

13.8.2 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**.

13.8.3 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**.

13.8.4 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**.

13.8.5 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**.

13.8.6 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.

13.8.7 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.

13.8.8 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.

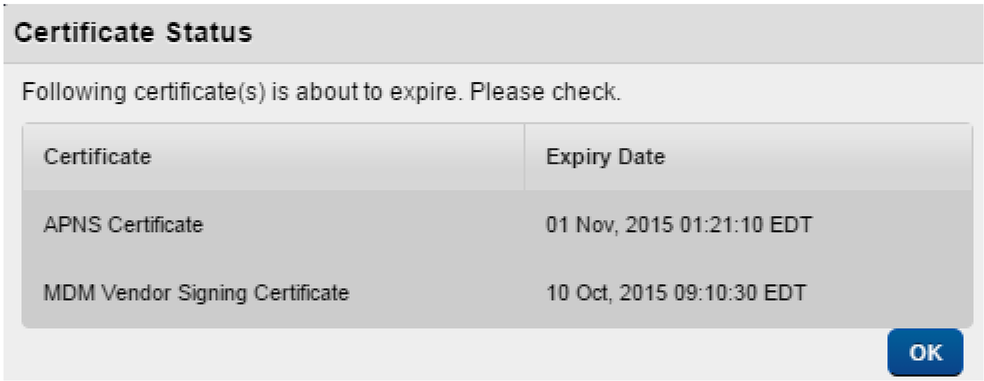
7. Click **Add**. Content is shared with the user/group, and details appear in the Target section.

8. Click **Save & Exit**.

14. Dashboard

The Dashboard is a visual summary of information. System administrators can use the dashboard to get a comprehensive graphical view of total enrolled 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.



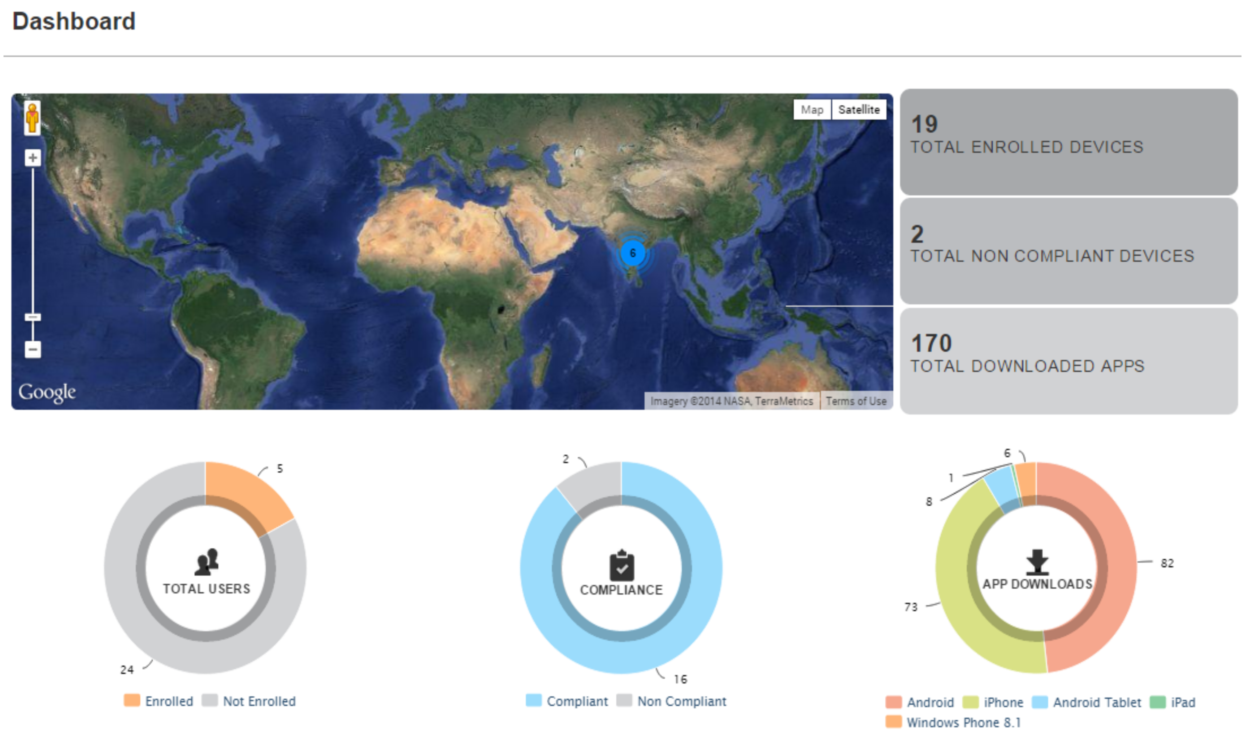
Certificate Status

Following certificate(s) is about to expire. Please check.

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.



The following table describes the components of the Dashboard:

Component	Description
Map	The Map displays the actual location of the total enrolled devices, total non-compliant devices and the total number of downloaded apps. You can view the location details in map or satellite format.
Total Enrolled Devices Label	This label displays the total number of the enrolled devices to EMM. For example, the label in above image indicates that total 19 devices are enrolled 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, Enrollment Summary Chart, Compliance Summary Chart, and App Downloads Summary Chart.

You can perform the following activities from the Dashboard:

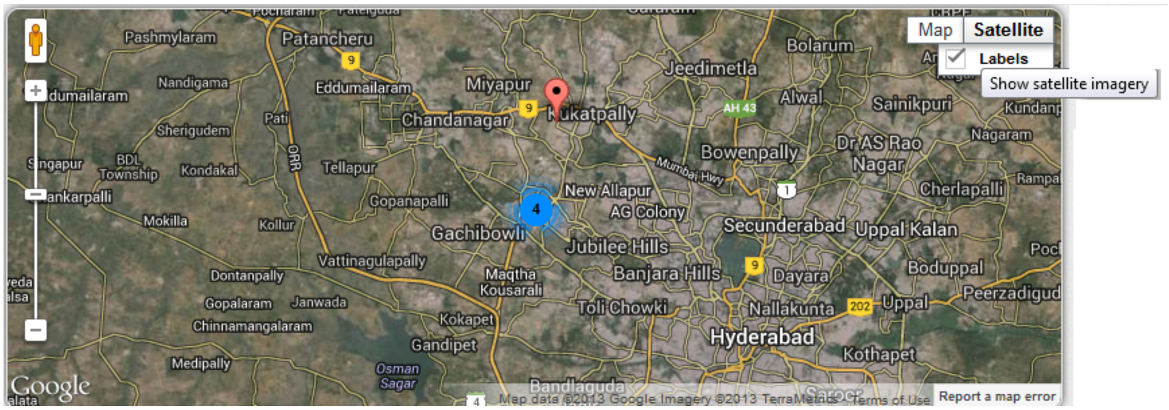
- Using the Map View
- Viewing the Enrollment Summary Chart
- Viewing the Compliance Summary Chart
- Viewing the App Downloads Summary Chart

14.1 Using the Map View

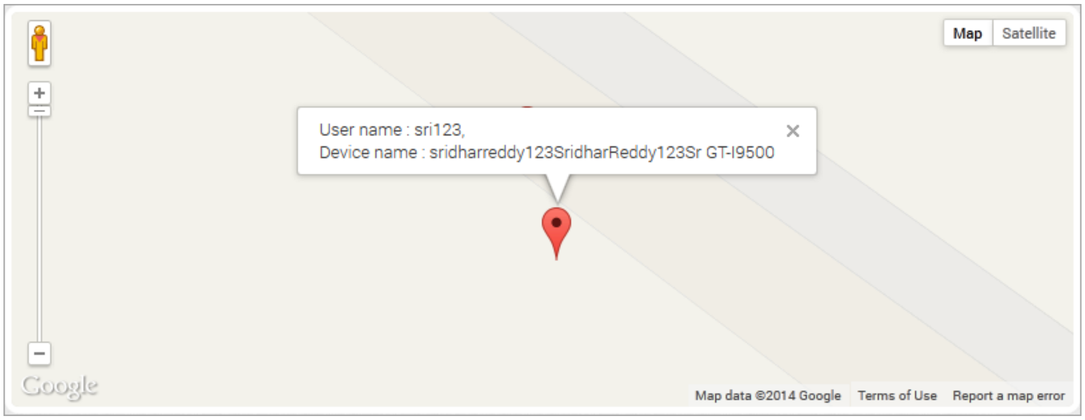
This window displays the location details on a map. You can also view it in satellite format. You can freely scroll through the area through hand tool. You can use the zoom tool to change the size of the visible area.

The view menu gives the following options:

- **Setting Labels**: Select the Labels option to view the labels for geographical locations.



- **Orient grid North**:The screen rotates such that the top of the screen points north. Not the geographical north is taken as reference, but the north of the currently selected grid.
- **Go to Target:**
  - Click the red icon on map to view the User Name and the Device Name. Double-click the red icon to open the Device details page.


User name : sri123,
Device name : sridharreddy123SridharReddy123Sr GT-I9500

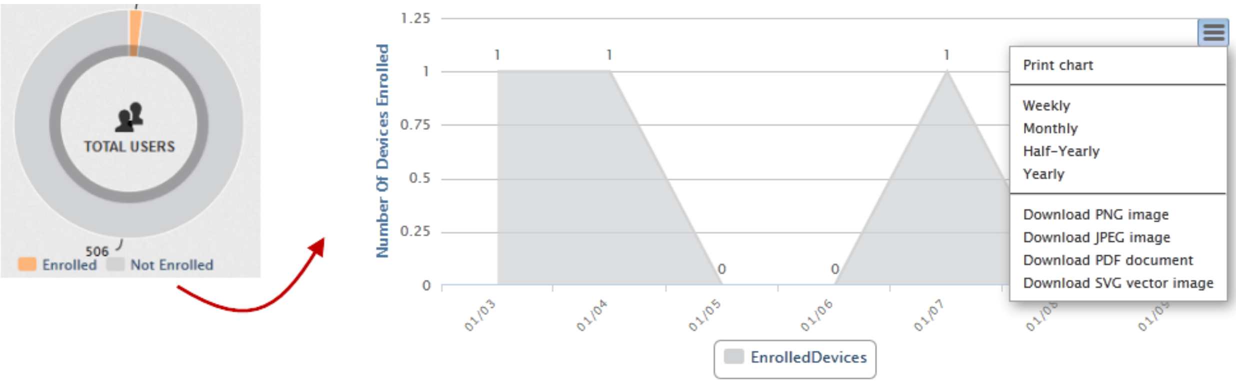
  - Click the **Total Enrolled Devices** label to open the **Device List** page.
  - Click the **Non Compliant Devices** label to open the **Device List** page.

> *Important:* There may be a mismatch between the number shown on maps and actual enrolled devices for several reasons:
> • If location tracking is disabled for certain devices
> • If there is any delay in retrieving the location data
> Windows devices should not be shown in the maps.

> *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.

14.2 Viewing the Enrollment Summary Chart

Enrollment Summary Chart displays the number of Users with enrolled devices versus Users with not enrolled devices. Click the pie chart to view Enrollment Summary chart.



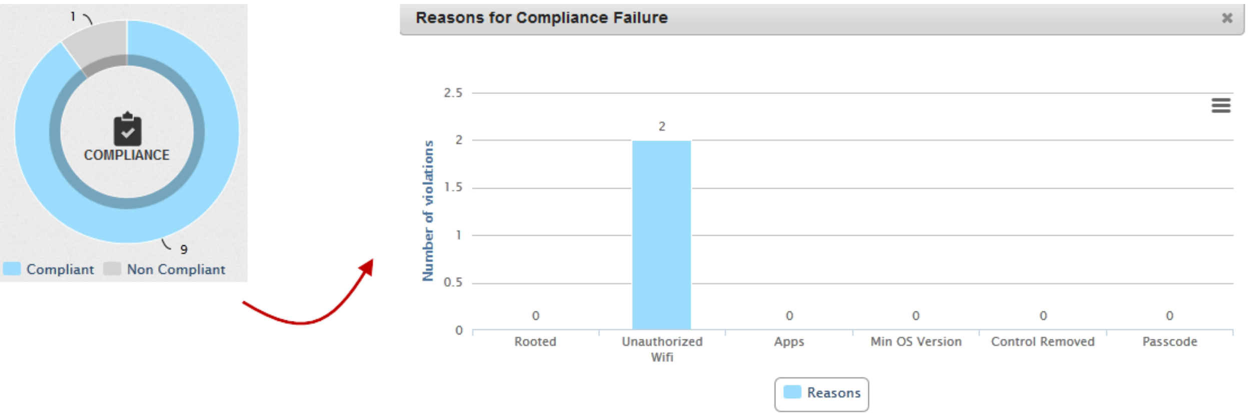
The Enrollment Summary chart includes the following components:

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

Components	Description
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 • Print the chart. • Download the chart in PNG, JPEG or SVG vector format. • Download the chart in PDF format.
Chart Details	• 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.

14.3 Viewing the Compliance Summary Chart

Compliance Summary chart displays the number of devices in compliance versus not in compliance in the pie graph.Click the pie chart to view Compliance Summary chart.



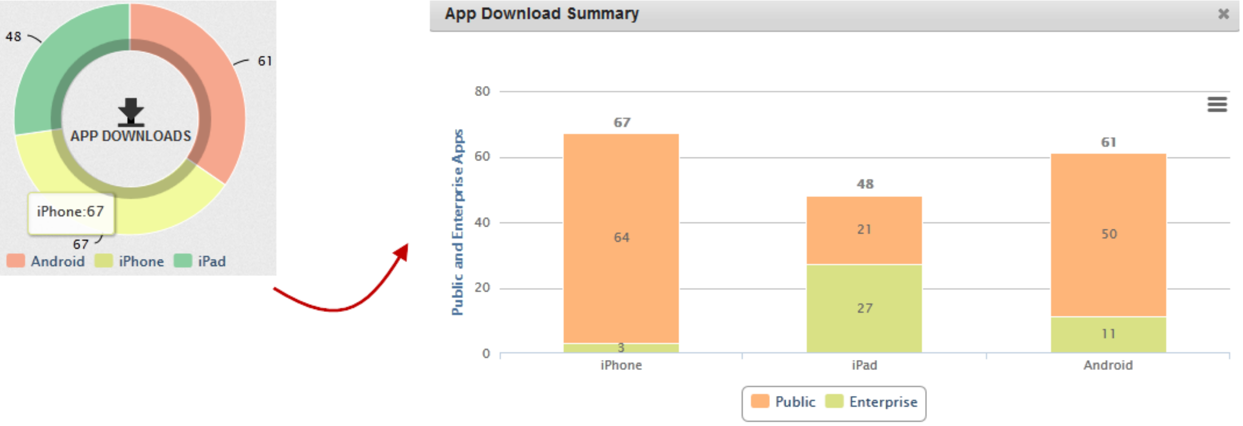
The Compliance Summary chart includes the following components:

Components	Description
Color Codes	The color codes indicates the distribution of each item (represented by a slice)
Chart Details	Double-click the pie chart to view the Reasons for Compliance Failure chart details. • Click the Chart Context menu to ○ Print the chart. ○ Download the chart in PNG, JPEG or SVG vector format. ○ Download the chart in PDF format. • The X axis represents the reasons. • The Y axis represents the number of violations.

14.4 Viewing the App Downloads Summary Chart

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	Double click the pie chart to view the Reasons for Compliance Failure chart details. • Click the Chart Context menu to ○ 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.

t also counts apps pushed through the app policy even though apps are not downloaded on a levice.

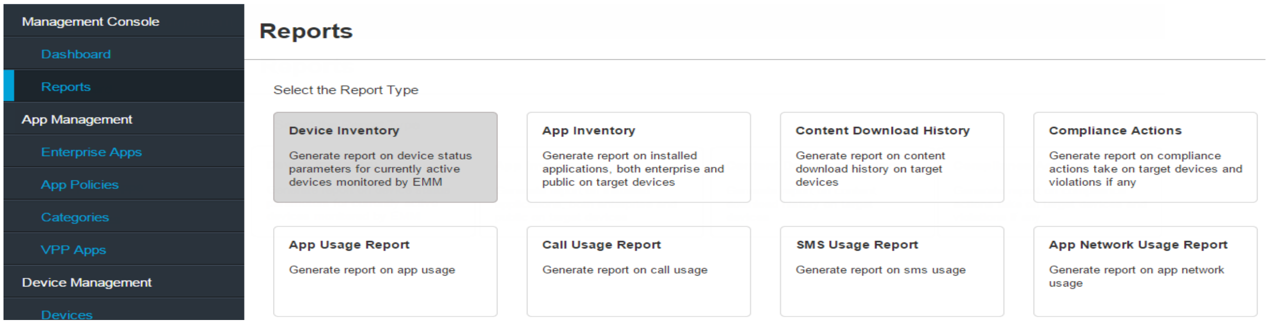
f a user clicks the Cancel button, it increments the download count

14.5 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.


Management Console
Dashboard
Reports
App Management
Enterprise Apps
App Policies
Categories
VPP Apps
Device Management
Devices
Reports
Select the Report Type
Device Inventory
Generate report on device status parameters for currently active devices monitored by EMM
App Inventory
Generate report on installed applications, both enterprise and public on target devices
Content Download History
Generate report on content download history on target devices
Compliance Actions
Generate report on compliance actions take on target devices and violations if any
App Usage Report
Generate report on app usage
Call Usage Report
Generate report on call usage
SMS Usage Report
Generate report on sms usage
App Network Usage Report
Generate report on app network usage

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.

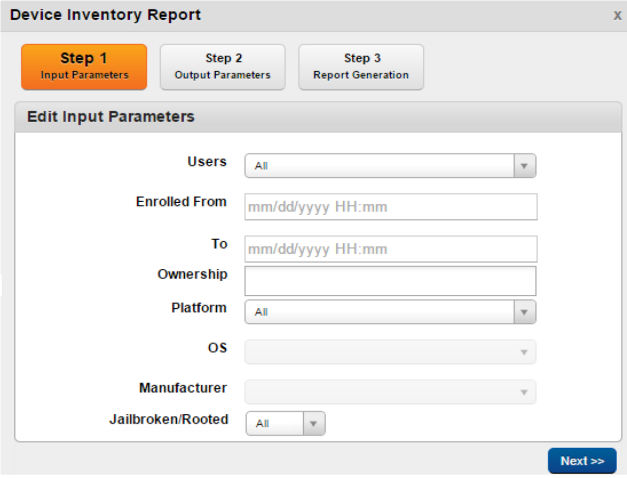
14.5.1 Device Inventory Report

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.



Device Inventory Report

Edit Input Parameters

Users: All

Enrolled From: mm/dd/yyyy HH:mm

To: mm/dd/yyyy HH:mm

Ownership:

Platform: All

OS:

Manufacturer:

Jailbroken/Rooted: All

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**.

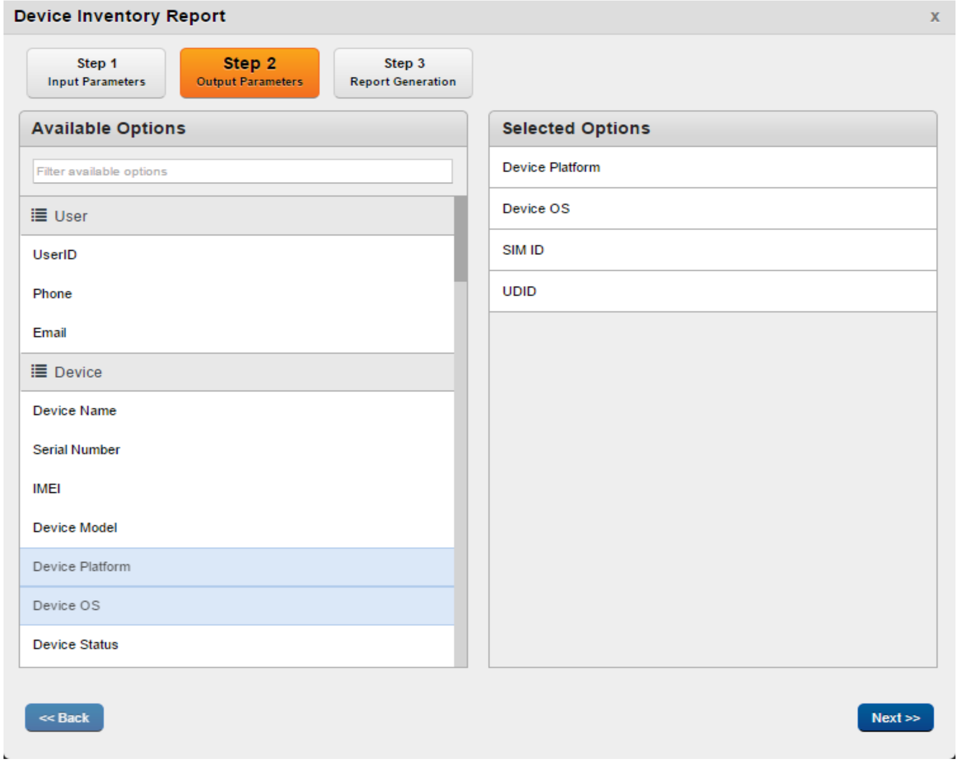
9. From the **Platform** list, select the platforms for which you want the Device Inventory Report. Based on the platform you select, OS and Manufacturer field options change.

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.

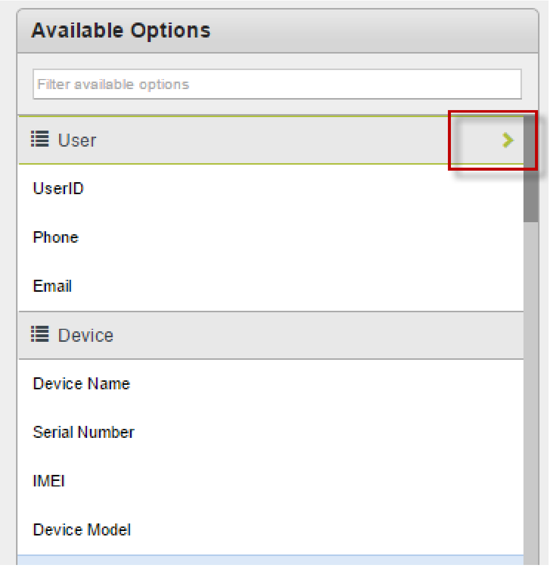


The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

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.



Available Options

Filter available options

User

UserID

Phone

Email

Device

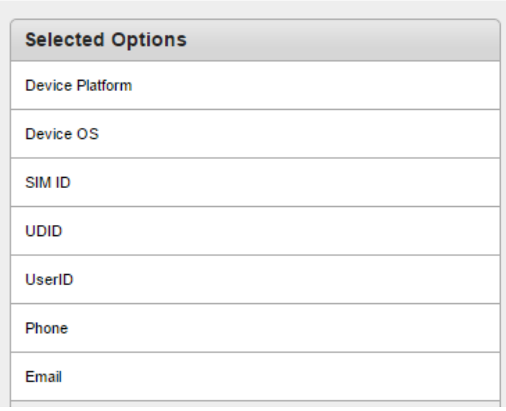
Device Name

Serial Number

IMEI

Device Model

    b. Click the select icon. Selected parameters appear in the selected options column.



Selected Options

Device Platform

Device OS

SIM ID

UDID

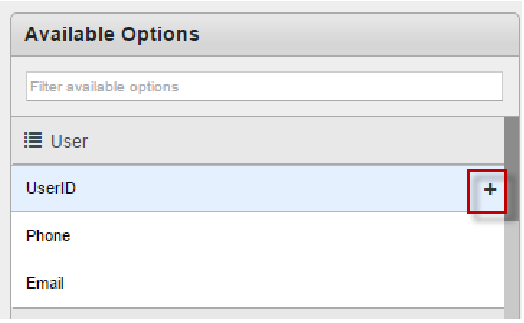
UserID

Phone

Email

16. 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

Filter available options

User

UserID +

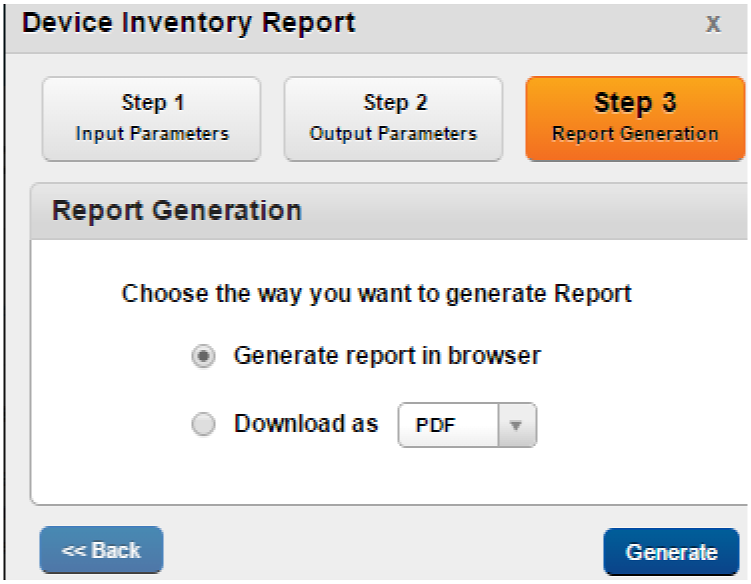
Phone

Email

    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.



Device Inventory Report

Report Generation

Choose the way you want to generate Report

● Generate report in browser

○ Download as PDF

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.

14.5.2 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 atleast 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 **Mode**list, select the EMM enrollment mode type. Options are **EMM**and **MAM/MCM**.
4. From the **App Type** list, select the app type. Options are **All**, **Enterprise App**, **Personal App**, and **Managed App**.
5. In the **App Name** field, enter the app name.
6. 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.
7. To create an app inventory report for any specific group, enter the group name in the **Groups** field.
8. To create an app inventory report for any specific user, enter the user name in the **Users** field.

9. 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.

10. From the **OS** list, select the OS version. If the selected platform is **All**, this field is disabled.

11. Click **Next**. The Output Parameters page appears.

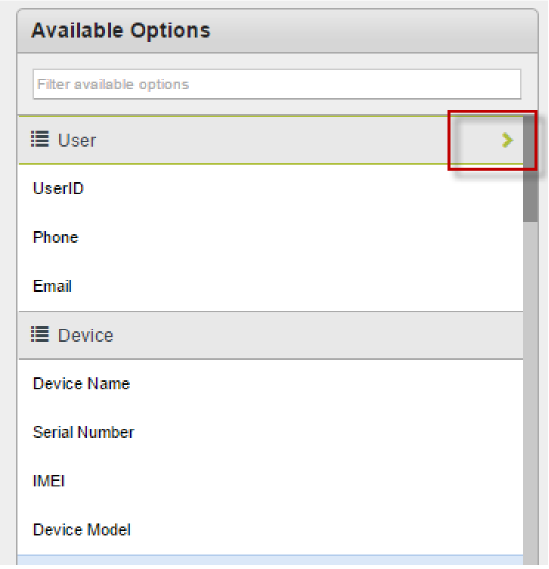
    The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.

12. You can choose other parameters from the available options column. You can do that in two ways:

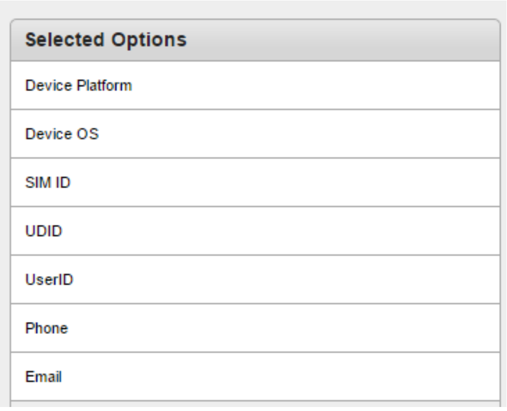
    - Select parameters group
    - Select individual parameter.

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.



Selected Options

Device Platform

Device OS

SIM ID

UDID

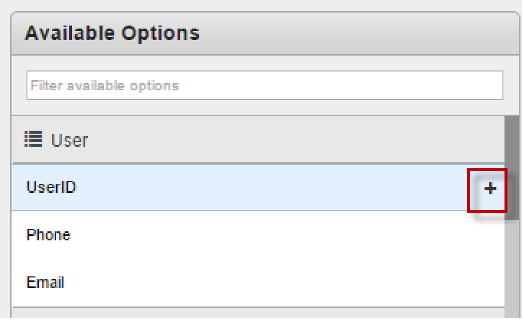
UserID

Phone

Email

14. 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

Filter available options

☰ User

UserID +

Phone

Email

b. Click the plus sign. Selected parameter appears in the selected options column.

15. Click **Next**. The Report Generation page appears.

16. To view the report in a browser, select **Generate report in browser**.

17. To download the report, select **Download as**.

18. If you select Download as, select the file type from the **Download as** list. Options are CSV, PDF, XLS and XLSX.

19. Click **Generate**. The report opens in a new browser or downloads in the format you choose.

14.5.3 Content Inventory Report

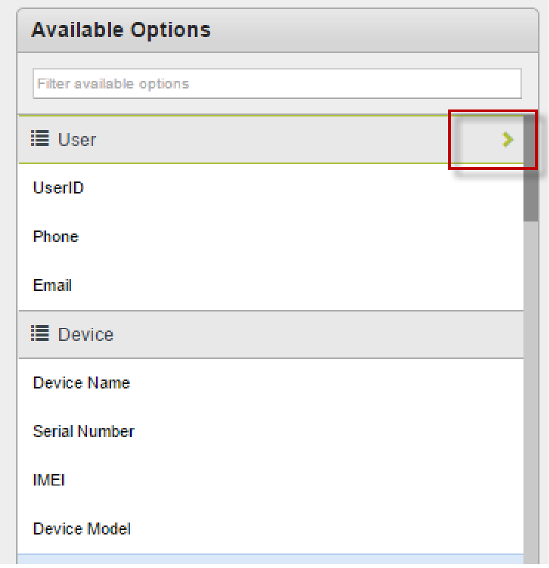
The Content Inventory report generates a report on the content download history on targeted devices in Kony Management Suite console.

To create a Content Inventory report, follow these steps:

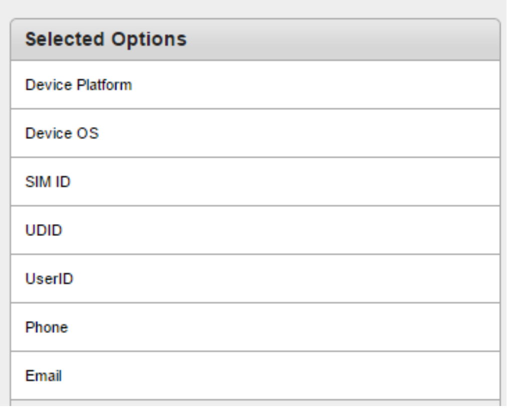
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Content Inventory**. The Content Inventory Report page appears.
3. From the **Target User** list, select **All** or **Specific**. If you select **All**, new fields do not appear. If you select Specific, 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.

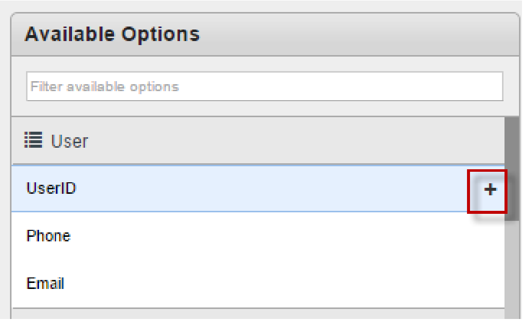


    b. Click the select icon. Selected parameters appear in the selected options column.



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.

14.5.4 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.

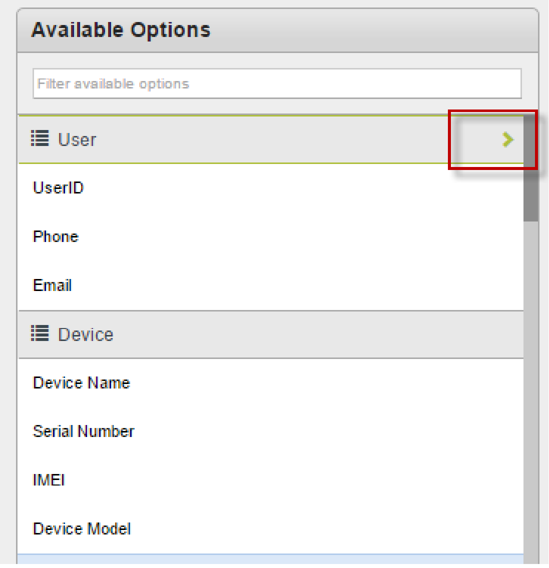
2. Click **Compliance Actions**. The Compliance Actions Report page appears.

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:

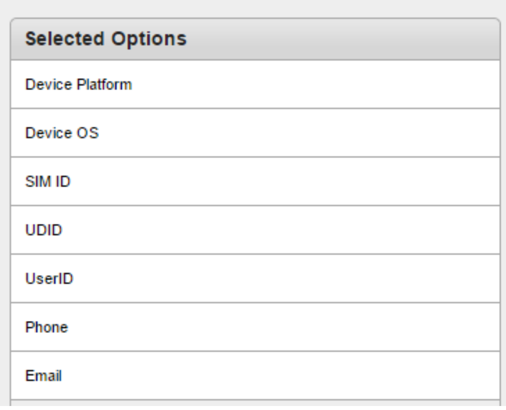
    a. Hover your mouse on the parameters group name. The select icon appears.



Available Options

Filter available options

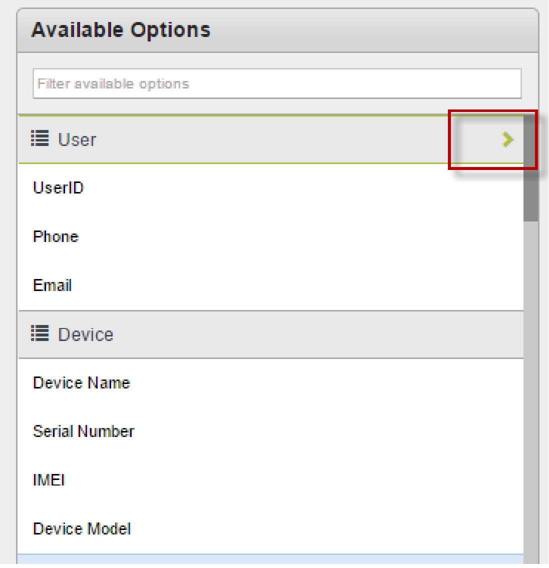
    b. Click the select icon. Selected parameters appear in the selected options column.



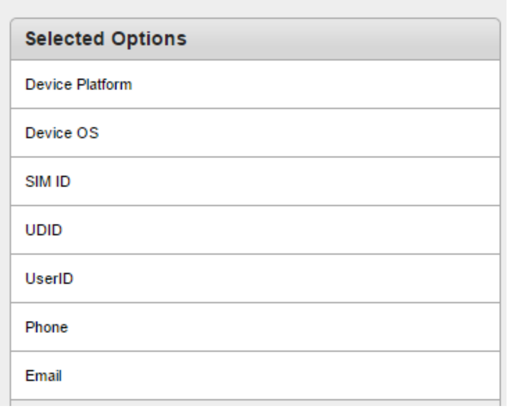
Selected Options

14. To select a parameters group, do the following:

   a. Hover your mouse on the parameters group name. The select icon appears.

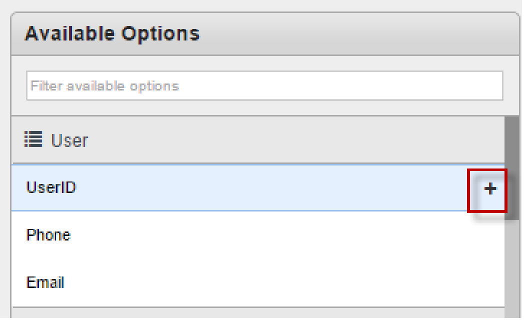


   b. Click the select icon. Selected parameters appear in the selected options column.



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.

14.5.5 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.

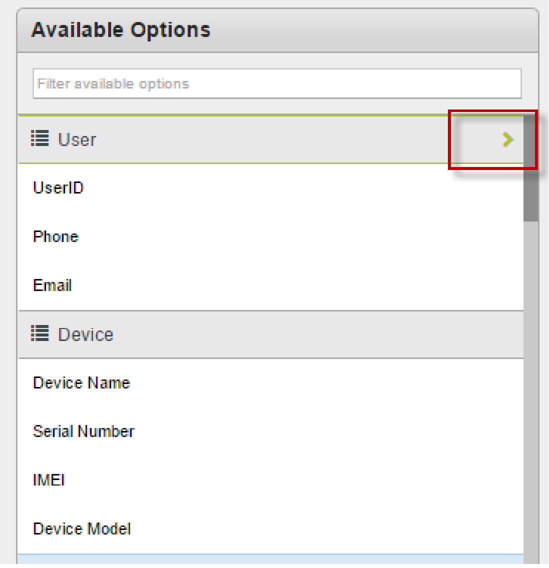
3. From the **Target Users** list, select **All** or **Specific**. If you select All, new fields do not appear. If you select Specific, new fields (Groups and Users) appear.

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.

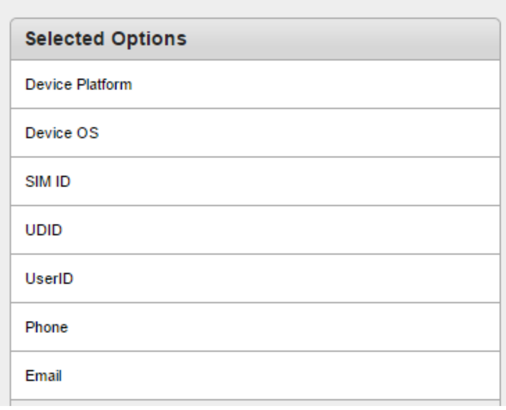
   The Output parameters page displays all parameters in two columns: **Available Options** and **Selected Options**. In the Selected options column, some parameters are selected by default.
10. You can choose other parameters from the available options column. Select one of the following options:
    - Select parameters group
    - Select individual parameter.

11. To select a parameters group, do the following:

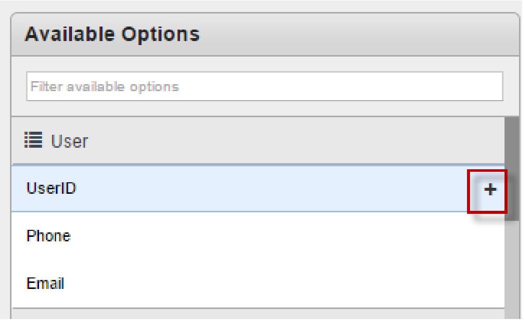
    a. Hover your mouse on the parameters group name. The select icon appears.



    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.

14.5.6 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:

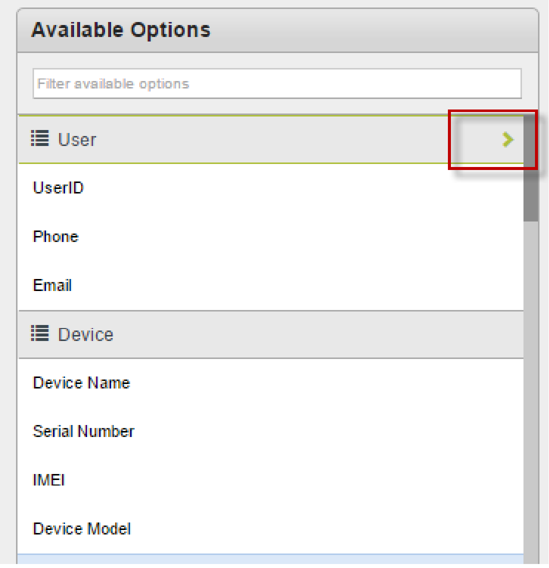
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **Call Usage Report**. The Call Usage Report page appears.

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.

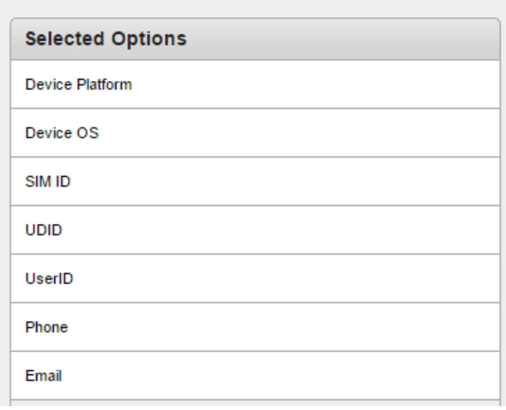
   The Output parameters page displays all parameters in two columns: **Available Options**, and **Selected Options**. In the Selected options column, some parameters are selected by default.
10. You can choose other parameters from the available options column. Select one of the two options:
    - Select parameters group
    - Select individual parameter.

11. To select a parameters group, do the following:

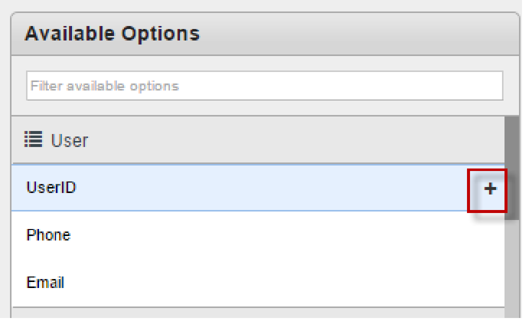
    a. Hover your mouse on the parameters group name. The select icon appears.



    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.

14.5.7 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:

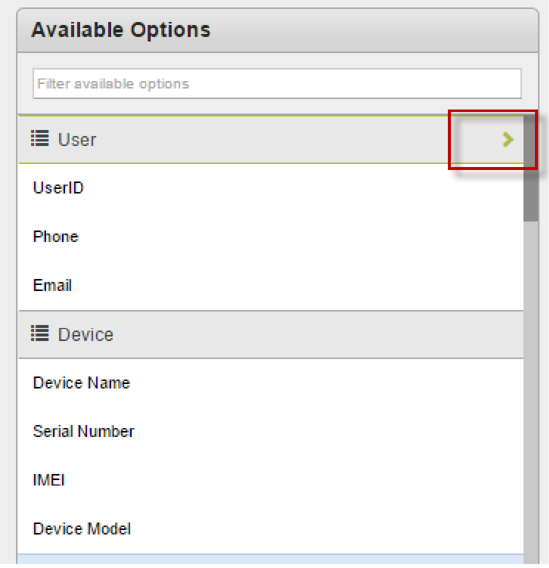
1. In Kony Management Suite Management console, click **Reports**. The Reports page appears.
2. Click **SMS Usage Report**. The SMS Usage Report page appears.

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.



Available Options

Filter available options

User

UserID

Phone

Email

Device

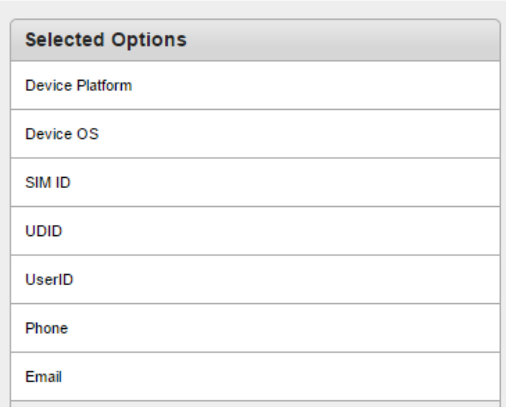
Device Name

Serial Number

IMEI

Device Model

    b. Click the select icon. Selected parameters appear in the selected options column.



Selected Options

Device Platform

Device OS

SIM ID

UDID

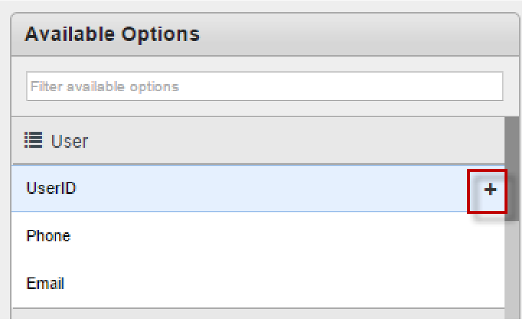
UserID

Phone

Email

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.

14.5.8 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.

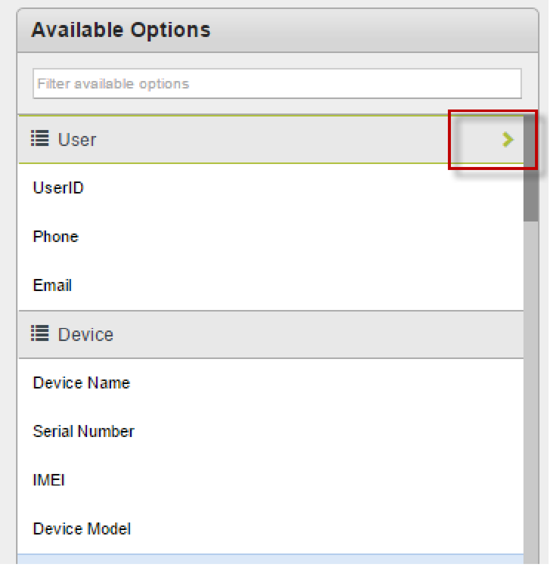
To create an Enterprise App Network Usage Actions report, follow these steps:

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.



Available Options

Filter available options

☰ User ›

UserID

Phone

Email

☰ Device

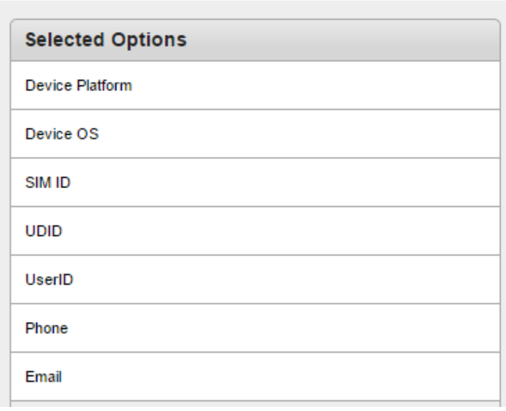
Device Name

Serial Number

IMEI

Device Model

    b. Click the select icon. Selected parameters appear in the selected options column.



Selected Options

Device Platform

Device OS

SIM ID

UDID

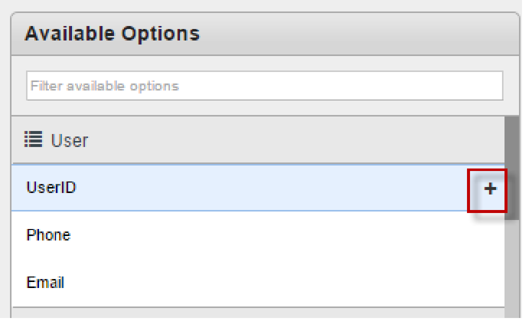
UserID

Phone

Email

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.

14.5.9 User Device Report

The User Device Report generates a report on all users and their devices enrolled in Kony Management Suite console.

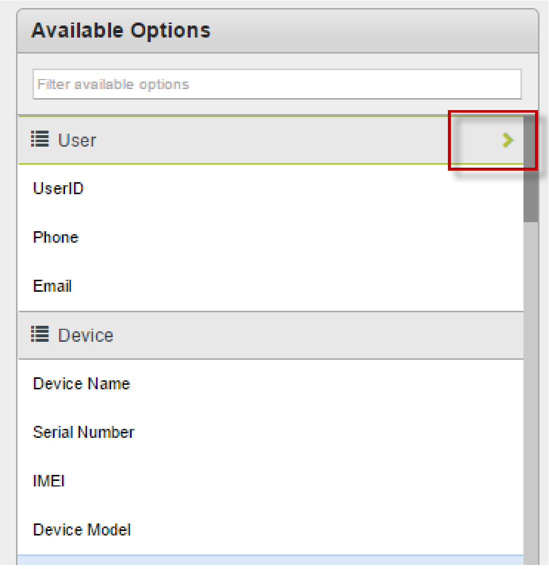
To create a User Device Report, follow these steps:

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.



Available Options

Filter available options

User

UserID

Phone

Email

Device

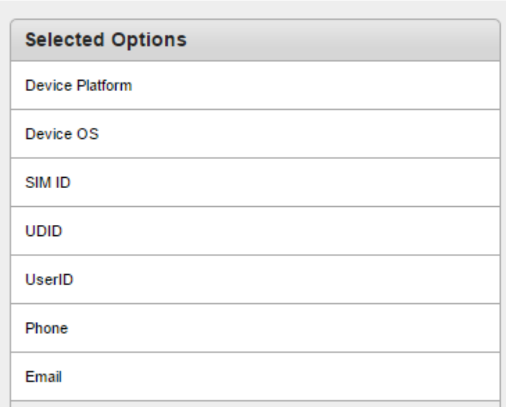
Device Name

Serial Number

IMEI

Device Model

   b. Click the select icon. The selected parameters appear in the selected options column.



Selected Options

Device Platform

Device OS

SIM ID

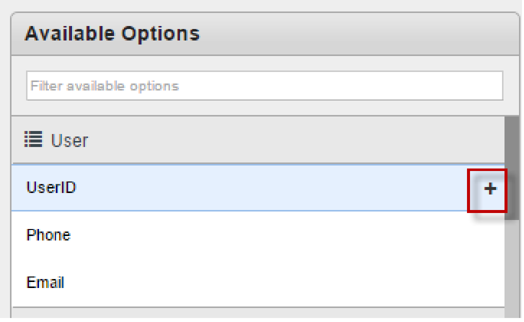
UDID

UserID

Phone

Email

9. 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

Filter available options

User

UserID

Phone

Email

   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.

14.5.10 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.

15. Intelligent EMM (IEMM)

iEMM enables developers to use device management controls during application development. This section elaborates device management information and controls provided to the developers. These controls are provided as REST APIs. These controls support both XML and JSON return types.

> ***Note:*** In EMM 2.5, the service Login to authenticate user access to EMM is an option. You can use HTTP Basic Authentication with each service API call, except `/emminfo` rest all service APIs are required to use SSL.

You can leverage these services through IEMM. The services that can be leveraged include the following.

- EMM Information
- User Authentication
- Device Information
- User Group Information
- Policy Information
  - Query Policy types
  - Query Policies
  - Query Policies as applied and acknowledged by device
- Apply Policy
- Querying Policy Applied Status
- Revert Applied Policy

15.1 EMM Information

This service provides the information, if tenant enabled iEMM services are or not.

15.1.1 URL

```
https://emmserver.com/emm/iemm/services/emminfo
```

15.1.2 Type

GET

15.1.3 Input

15.1.3.1 Input Headers

Accept

This is an optional parameter. The default value is `application/xml`,and possible values are `application/xml` or `application/json`

15.1.4 Output

15.1.4.1 Output Parameters

responseCode

- 1000 = success
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call

description

Refer responseCode.

iemmAvailable

This helps a user to know, if IEMM services are available or not. The possible values are True and False.

15.1.5 Examples

Output:

```
{"description":"success","responseCode":1000,"iemmAvailable":true}
```

15.2 User Authentication

This service is the first service call in series of calling various IEMM services except emminfo service. This service maintains sessions and secret tokens that contain user information.

15.2.1 URL

```
https://emmserver.com/emm/iemm/services/login
```

15.2.2 Type

POST

15.2.3 Input

15.2.3.1 Input Parameters

username

This is a mandatory parameter given by tenant/admin to the particular user.

password

This is a mandatory parameter given by tenant/admin to the particular user.

deviceid

This is a mandatory parameter to authenticate the user.

15.2.3.2 Input Headers

Content-Type

This is a mandatory parameter and allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter whose default value is "`application/xml`", and the possible values are `application/xml or application/json.`

15.2.4 Output

15.2.4.1 Output Parameters

responseCode

- 1000 = success
- 1001 = Error - Missing Username: Username should not be empty
- 1002 = Error - Missing Password: Password should not be empty
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 1005 = Authentication Failed. Invalid username or password
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session time out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEMM services are not available
- 3005 = Error - Device is not enrolled with EMM

description

Please refer responseCode.

token

Encrypted token contains user information.

15.2.4.2 Output Headers

Set-Cookie

This helps in maintaining session and is passed in consecutive services as value of input header parameter “`Cookie`”.

15.2.5 Examples

Input:

```
username=admin&password=admin&deviceid=
fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output:

```
{
   "description":"success",
   "responseCode":1000,

"token":"BA47E3769E65732794B4CD4A742DB555E37F167C87A9AE73A27581E0C18
6039D43800F9C0D8CA8611D0F971A9B3B2B52F9C7D629F59728A8F0F5669091722E9
C"
}
```

15.3 Device Information

This service provides the information about a device enrolled with EMM.

15.3.1 URL

```
https://emmserver.com/emm/iemm/services/deviceinfo
```

15.3.2 Type

POST

15.3.3 Input

15.3.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user.

15.3.3.2 Input Headers

Content-Type

This is a mandatory parameter and allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter, whose default value is `application/xml`, and possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.3.4 Output

15.3.4.1 Output Parameters

responseCode

- 1000 = success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session time out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM

description

Refer responseCode.

token

Encrypted token contains user information.

deviceStatus

This always comes as `“ENROLLED”`

devicePlatform

Device from where this service is called. The possible values are IPHONE and so on.

15.3.4.2 Output Headers

Set-Cookie

This is used to maintain sessions and passed in consecutive services as value of input header parameter `Cookie`

15.3.5 Examples

Input:

```
deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output:

```
{
   "description":"success",
   "responseCode":1000,
   "deviceStatus":"ENROLLED",
   "devicePlatform":"IPHONE"
}
```

15.4 User Group Information

This is a query base service. On the basis of a query parameter, the system responds with the list of groups to the associated user device.

15.4.1 URL

```
https://mdmdev.konylabs.net/emm/iemm/services/usergroup
```

15.4.2 Type

POST

15.4.3 Input

15.4.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user device to get group details.

15.4.3.2 Input Headers

Content-Type

This is a mandatory parameter, and the allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is the output header parameter Set-Cookie value of the previous service.

15.4.4 Output

15.4.4.1 Output Parameters

responseCode

- 1000 = Success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session timed out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM

Description

Please refer responseCode.

15.4.4.2 Output Headers

Set-Cookie

Set-cookie helps to maintain a session passed in consecutive services as a value of the input header parameter cookie

15.4.5 Examples

Input:

```
deviceid=358918050081901
```

Output:

```
Response
               {
                  "description": "Success",
                  "responseCode": 1000,
                  "userGroup":
                  [
                          {
                                  "groupName": "tg1",
                                  "domain": null
                          },
                          {
                                  "groupName": "tg2",
                                  "domain": null
                          }
                  ]
               }
```

15.5 Policy Information

This is a query base service. On the basis of query parameter and corresponding expression, the system responds to the user with relevant output.

15.5.1 URL

```
https://emmserver.com/emm/iemm/services/policy
```

15.5.2 Type

POST

15.5.3 Input

15.5.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user.

query

This is a mandatory parameter and its possible values are:

- policytype
- policy
- devicepolicy

queryexpression

- This is an optional parameter. It helps a user in filtering the output result using simple java expressions. Refer examples for more detail. The Possible values for:
  - for query=policytype
    1. id [int]
    2. name [String]
    3. desc [String]
  - for query=policy
    1. id [int]
    2. name [String]
    3. desc [String]
    4. policyID [int]
    5. state [String]
    6. status [String]
    7. updatorID [String]
    8. creatorID [String]
    9. syncID [String]
  - for query=devicepolicy
    1. id [int]
    2. name [String]

3. desc [String]
4. policyID [int]
5. state [String]
6. status [String]
7. updatorID [String]
8. creatorID [String]
9. syncID [String]

15.5.3.2 Input Headers

Content-Type

This is a mandatory parameter and allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`.

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.5.4 Output

15.5.4.1 Output Parameters

responseCode

- 1000 = success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session time out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM

description

Please refer responseCode.

policies

This comes as output for policytype query. It is an array of policy types existing in EMM. Refer policytype examples for more detail.

policyInstances

This comes as output for policy query or devicepolicy query. It is an array of policies existing in EMM. Refer policy or devicepolicy examples for more detail.

15.5.4.2 Output Headers

Set-Cookie

This helps in maintaining session and passed in consecutive services as value of input header parameter Cookie

15.5.5 Examples

15.5.5.1 policytype

Input:

```
query=policytype&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output:

```
{
   "description":"success",
   "responseCode":1000,
   "policies":[
      {
         "id":1,
         "name":"PASSCODE_POLICY",
         "desc":"Passcode Policy"
      },
      {
         "id":2,
         "name":"DEVICE_RESTRICTIONS",
         "desc":"Device restrictions"
      },
      {
         "id":3,
         "name":"EMAIL_CALENDAR",
         "desc":"Email and Calendar setup"
      },
      {
         "id":4,
         "name":"NETWORK",
         "desc":"Network"
      },
      {
         "id":5,
         "name":"CERTIFICATE_DISTRIBUTION",
         "desc":"Certificate distribution"
      },
      {
         "id":6,
         "name":"WEB_CLIPS",
         "desc":"Webclips"
      },
      {
         "id":8,
         "name":"COMPLAINCE_ACTIONS",
         "desc":"Compliance Actions"
      },
      {
         "id":9,
         "name":"TRACKING_SETTINGS",
         "desc":"Tracking Settings"
      },
      {
         "id":11,
         "name":"MANDATORY_APPS",
         "desc":"App Policy"
      }
   ]
```

```
}
```

Input2

You can use `queryexpression` for the policytype queries.

```
query=policytype&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4&queryexpression=name=="PASSCODE_POLICY"
```

Output2

```
{
   "description":"success",
   "responseCode":1000,
   "policies":[
      {
         "id":1,
         "name":"PASSCODE_POLICY",
         "desc":"Passcode Policy"
      }
   ]
}
```

15.5.5.2 policy

Input1

You can use `queryexpression` for the policy queries.

```
query=policy&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output1

```
{
   "description":"success",
   "responseCode":1000,
   "policyInstances":[
      {
         "policyID":"7502395553198640881",
         "id":1,
         "name":"Name",
         "desc":"",
         "state":"ACTIVE",
         "status":"PUBLISHED",
         "syncID":null,
         "creatorID":"admin",
         "createdTimestamp":"YYYY-MM-DD HH:MM:SS.SS",
         "priority":1,
         "updatorID":"admin",
         "updatedTimestamp":"YYYY-MM-DD HH:MM:SS.SS",
         "publishTimestamp":"YYYY-MM-DD HH:MM:SS.SS"

         "policyDescription":[
            {
               "constraintKey":"ALLOW_SIMPLE_PASSCODE",
               "constraintName":"Allow Simple Passcode",
               "constraintValue":"true"
            },

         ],

      },


[[-- optional element --]]
```

Input 2:

You can use `queryexpression` for the policy queries.

```
query=policy&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4&queryexpressi
on=policyID==7502395553198640881
```

Output 2:

```
{
   "description":"success",
   "responseCode":1000,
   "policyInstances":[
      {
         "policyID":"7502395553198640881",
         "id":1,
         "name":"Name",
         "desc":"",
         "state":"ACTIVE",
         "status":"PUBLISHED",
         "syncID":null,
         "creatorID":"admin",
         "createdTimestamp":"YYYY-MM-DD HH:MM:SS.SS",
         "priority":1,
         "policyDescription":[
            {
               "constraintKey":"ALLOW_SIMPLE_PASSCODE",
               "constraintName":"Allow Simple Passcode",
               "constraintValue":"true"
            },
            {
               "constraintKey":"REQUIRE_ALPHANUMERIC",
               "constraintName":"Require Alphanumeric",
               "constraintValue":"false"
            },
            {
               "constraintKey":"MIN_PASSODE_LENGTH",
               "constraintName":"Minimum Passcode Length",
               "constraintValue":"4"
            },
            {
               "constraintKey":"NUM_OF_SPECIAL_CHARS",
               "constraintName":"Number of Special characters",
               "constraintValue":"0"
            },
            {
               "constraintKey":"PASSCODE_EXPIRATION",
               "constraintName":"Passcode Expiration",
               "constraintValue":"30"
            },
            {
               "constraintKey":"AUTO_LOCK_TIME_LIMIT",
               "constraintName":"Auto-lock Time Limit",
               "constraintValue":"2"
            },
            {
               "constraintKey":"UNIQUE_PASSCODES_BEFORE_REUSE",
               "constraintName":"Unique Passcodes required Before
Reuse",
               "constraintValue":"6"
            },
            {
               "constraintKey":"ERASE_DATA_FAILED_ATTEMPTS",
               "constraintName":"Erase All Data",
               "constraintValue":"9"
            },
            {
               "constraintKey":"IOS_REQUIRE_PASSCODE",
               "constraintName":"Require Passcode",
               "constraintValue":"true"
            }
         ],
         "updatorID":"admin",
         "updatedTimestamp":"YYYY-MM-DD HH:MM:SS.SS",
         "publishTimestamp":"YYYY-MM-DD HH:MM:SS.SS"
      }
   ]
}
```

Input3

You can use `queryexpression` for the policy queries. Queiryexpressions can be made complex using Boolean operators:

- Or (||)
- And (&&)

```
deviceid=358918050081901&query=policy&queryexpression=name=='P2'||name=='P3'%26%26state=='ACTIVE'&&status=='PUBLISHED'
```

Output

```
 {
       "description": "Success",
       "responseCode": 1000,
       "policyInstances":
       [
           {
               "name": "P2",
               "policyID": "7560377597073303607",
               "priority": 2,
               "id": 1,
               "desc": "this is test passcode policy",
               "state": "ACTIVE",
               "status": "PUBLISHED",
               "syncID": null,
               "creatorID": null,
                          "updatorID": null,
               "createdTimestamp": "YYYY-MM-DD HH:MM:SS.SS",
               "updatedTimestamp": "YYYY-MM-DD HH:MM:SS.SS",
               "publishTimestamp": "YYYY-MM-DD HH:MM:SS.SS"
               "policyDescription":
               [
                   {
                       "constraintKey": "AND_REQUIRE_PASSCODE",
                       "constraintName": "Require Passcode",
                       "constraintValue": "false"
                   }
               ],
           }
       ]
    }
```

15.5.5.3 devicepolicy

The devicepolicy method queries policies that are acknowleged by a device.

Input

```
query=devicepolicy&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <policyInstance>
       <description>Success</description>
       <responseCode>1000</responseCode>
       <policyInstances>
       <createdTimestamp>YYYY-MM-DD HH:MM:SS.SS</createdTimestamp>
                   <desc>
                   </desc>
                   <id>2</id>
                   <name>safe_dr</name>
       <policyDescription>
                   <constraintKey>AND_ALLOW_CAMERA</constraintKey>
                   <constraintName>Challenge Code</constraintName>

<constraintValue>false</constraintValue>
       </policyDescription>



       <policyDescription>
             <constraintKey>ANDROID_SAMSUNG_SAFE_EMAIL_
ALLOWACCOUNTADDITION</constraintKey>
              <constraintName>Allow Voice Dialer</constraintName>

<constraintValue>true</constraintValue>
        </policyDescription>
         <policyID>7548037160583064994</policyID>
         <priority>3</priority>
         <publishTimestamp>YYYY-MM-DD HH:MM:SS.SS</publishTimestamp>
         <state>ACTIVE</state>
         <status>PUBLISHED</status>
         <updatedTimestamp>YYYY-MM-DD HH:MM:SS.SS</updatedTimestamp>
        </policyInstances>
    </policyInstance>
```

15.6 Apply Policy

This service is used to apply a policy on the device. This takes precedence over the policy applied using a device set configuration in EMM.

This service accepts a coma separated list of policy IDs defined in the EMM server.

15.6.1 URL

```
https://emmserver.com/emm/iemm/services/policy
```

15.6.2 Type

POST

15.6.3 Input

15.6.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user.

query

This is a mandatory parameter. The possible values are:

- applypolicy

devicesetID

This is a optional parameter to verify whether a device is part of a device set.

policyid

This is a mandatory parameter and its comma-separated values of policy id should be applied on a device. Refer examples for more details.

15.6.3.2 Input Headers

Content-Type

This is a mandatory parameter, and allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.6.4 Output

15.6.4.1 Output Parameters

responseCode

- 1000 = success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session time out
- 3001 = Unexpected error occurred

- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM
- 3006 = Error - Invalid Policy passed
- 3007 = Error - Device does not belong to provided Device Set
- 4001 = Policy already exists on device
- 4002 = Error - Improper Policy: PolicyID not exist.
- 4003 = Error - Unpublished Policy provided

description

Please refer responseCode.

requestID

A unique identifier for requested applied policy.

policyApplied

This is a Boolean value to check if policy is applied successfully or not. The possible values are true and false.

15.6.4.2 Output Headers

Set-Cookie

Set-cookie helps to maintain sessions and passed in consecutive services as a value of the input header parameter Cookie

15.6.5 Examples

Input:

```
query=applypolicy&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4&policyid
=7502395757865996819,7502560957311238180
```

Output:

```
{
   "description":"success",
   "responseCode":1000,
   "requestID":1041,
   " poicyApplied ":"true"
}
```

15.7 Querying Policy Applied Status

This is a query base service. On the basis of query parameter, the system responds to the user device with the status of a policy.

15.7.1 URL

```
https://emmserver.com/emm/iemm/services/policy
```

15.7.2 Type

POST

15.7.3 Input

15.7.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user.

query

This is a mandatory parameter, and possible values are:

- policystatus

requestid

When a policy is applied, the system returns a requestID. This requestID needs to be passed to get the status of a policy applied on device or not.

15.7.3.2 Input Headers

Content-Type

This is a mandatory parameter and its allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.7.4 Output

15.7.4.1 Output Parameters

responseCode

- 1000 = Success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session timed out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call

- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM
- 3008 = Error - Invalid/Missing RequestId

description

Please refer responseCode.

policystatus

A Boolean value to returns according to policy applied on device.

15.7.4.2 Output Headers

Set-Cookie

This helps in maintaining session and passed in consecutive services as value of input header parameter Cookie

15.7.5 Examples

Input:

```
query=policystatus&requestId=1001
```

Output:

```
{
   "description":"success",
   "responseCode":1000,
   " isAcknowledged":true
}
```

15.8 Revert Applied Policy

This service reverts an applied policy on a device.

15.8.1 URL

```
https://emmserver.com/emm/iemm/services/policy
```

15.8.2 Type

POST

15.8.3 Input

15.8.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user.

query

This is a mandatory parameter. The possible values are as follows:

- revertpolicy

requestid

This is an optional parameter. With every applied policy service, it returns with one requestid. Passing that requestid in the service device returns to the state maintained before applying that policy.

By default it reverts all the policies applied through services and maintains the state as it was at the time of the enrollment.

15.8.3.2 Input Headers

Content-Type

This is a mandatory parameter and allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml,` and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.8.4 Output

15.8.4.1 Output Parameters

responseCode

- 1000 = success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 2001 = Error: Authenticated Token is missing
- 2002 = Error: Device ID should not be empty
- 2003 = Session time out
- 3001 = Unexpected error occurred
- 3003 = Error - Improper Service Call: Please check URL and provide correct service call
- 3004 = IEmm Services are not available
- 3005 = Error - Device is not enrolled with EMM

- 4004 = Error - Existing device policies are empty
- 4005 = Policies already reverted for given requestid

description

Refer responseCode.

requestID

A unique identifier for requested applied policy.

policiesRevert

A Boolean value to check, if the policy is reverted successfully or not. The possible values are TRUE and FALSE.

15.8.4.2 Output Headers

Set-Cookie

This helps in maintaining the session and passed in consecutive services as value of input header parameter `Cookie`

15.8.5 Examples

Input:

```
query=revertpolicy&deviceid=fbf43e35aeb2fb9eaedf0dddf26250d4
```

Output:

```
{
   "description":"success",
   "responseCode":1000,
   "policiesRevert":true
}
```

15.9 User Custom Attributes

On the basis of the query parameter, the system responds with the list of custom attributes targeted to a user.

15.9.1 URL

```
https://emmserver.com/emm/iemm/services/userCustomAttributes
```

15.9.2 Type

POST

15.9.3 Input

15.9.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user device to get custom attribute details.

15.9.3.2 Input Headers

Content-Type

This is a mandatory parameter. The allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is the output header parameter Set-Cookie value of the previous service.

15.9.4 Output

15.9.4.1 Output Parameters

responseCode

- 1000 = Success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 1009 = Error - Missing Device ID: Device ID should not be empty
- 4006 = Error: Invalid Input

description

Please refer responseCode.

15.9.4.2 Output Headers

Set-Cookie

This helps to maintain a session and pass consecutive services as values of input header parameter Cookie.

15.9.5 Examples

With a valid deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/userCustomAttributes?d=3
5724653771877
```

Output:

```
Response
               {"afdsa":"dsfafdsa","a1":"A1VALUE"}
```

Without a valid deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/userCustomAttributes?d=3
572465377187
```

Output:

```
Response
       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error: Invalid Input</description>
```

```
<responseCode>4006</responseCode>
```

```
</emmExceptionHandler>
```

Without a deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/userCustomAttributes
```

Output:

```
Response
       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error: - Missing Device ID: Device ID should not be
empty</description>
```

```
<responseCode>1003</responseCode>
```

```
</emmExceptionHandler>
```

15.10 User Group Custom Attributes

On the basis of the query parameter, the system responds with the list of custom attributes targeted to a user group.

15.10.1 URL

```
 https://mdmdev.konylabs.net/emm/iemm/services/usergroup
```

15.10.2 Type

POST

15.10.3 Input

15.10.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user device to get custom attribute details.

Grpid - Group ID

This is a mandatory parameter to authenticate a user device to get custom attribute details.

15.10.3.2 Input Headers

Content-Type

This is a mandatory parameter. The allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is output header parameter Set-Cookie value of the previous service.

15.10.4 Output

15.10.4.1 Output Parameters

responseCode

- 1000 = Success
- 1003 = Error - Missing Device ID: Device ID should not be empty

- 1010 = Error - Group Id Cannot be Empty
- 1011 = Error - Group Not Found
- 3005 = Error - Device is not enrolled with EMM
- 4006 = Error: Invalid Input

description

Please refer responseCode.

15.10.4.2 Output Headers

Set-Cookie

This helps to maintain a session and pass consecutive services as values of input header parameter Cookie.

15.10.5 Examples

With a valid groupID and a valid deviceID

Input:

```
https://emmserver.net:
446/emm/iemm/services/
groupCustomAttributesgrpid=
7616473680459072146&d=357246053771877
```

Output:

```
Response
               {"afdsa":"dsfafdsa","a1":"A1VALUE"}
```

With a valid groupID and without a valid deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/groupCustomAttributes?
grpid=7616473680459072146
```

Output:

```
Response
       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error - Missing Device ID: Device ID should not be
empty</description>
```

```
<responseCode>1003</responseCode>
```

```
</emmExceptionHandler>
```

Without a groupID and without a deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/groupCustomAttributes
```

Output:

```
Response
       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error - Missing Device ID: Device ID should not be
empty</description>
```

```
<responseCode>1003</responseCode>
```

```
</emmExceptionHandler>
```

With an invalid groupID and an invalid deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/groupCustomAttributes
```

Output:

Group is not part of the enrolled user.

15.11 App Custom Attributes

On the basis of the query parameter, the system responds with the list of custom attributes targeted to a child application.

15.11.1 URL

```
https://emmserver.com/emm/iemm/services/appCustomAttributes
```

15.11.2 Type

POST

15.11.3 Input

15.11.3.1 Input Parameters

- appProfileID - App Profile ID
- v - Version of the App
- platform - Platform Name

15.11.3.2 Input Headers

Content-Type

This is a mandatory parameter. The allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is the output header parameter Set-Cookie value of the previous service.

15.11.4 Output

15.11.4.1 Output Parameters

responseCode

- 1000 = Success
- 4006 = Error: Invalid Input
- 400 = App Id cannot be empty

- 400 = App version cannot be empty
- 400 = App platform cannot be empty
- 400 = App does not exist with given details

description

Please refer responseCode.

15.11.4.2 Output Headers

Set-Cookie

This helps to maintain a session and pass consecutive services as values of input header parameter Cookie.

15.11.5 Examples

With valid app profileid,version, and platform.

Input:

```
https://emmserver.net:
446/emm/iemm/services/
appCustomAttributes?
appProfileId=7616310799201479653&v=1.0.0&platform=ANDROID
```

Output:

```
Response
                              {"afdsa":"dsfafdsa","a1":"A1VALUE"}
```

With invalid app profileid,version, and platform

Input:

```
https://emmserver.net:446/emm/iemm/services/appCustomAttributes?
appProfileId=716310799201479653&v=version&platform=ANDR
```

Output:

```
       <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error: Invalid Input</description>
```

```
<responseCode>4006</responseCode>
```

```
</emmExceptionHandler>
```

Without an AppprofileId

Input:

```
https://emmserver.net:446/emm/iemm/services/appCustomAttributes?v=1.
0.0&platform=ANDROID
```

Output:

```
App ID cannot be empty.
```

With an invalid appprofileid, valid version, and valid platform.

Input:

```
https://emmserver.net:446/emm/iemm/services/
appCustomAttributesappProfileId=3244&v=1.0.0&platform=ANDROID
```

Output:

App does not exist with given details.

15.12 Device Custom Attributes

On the basis of the query parameter, the system responds with the list of custom attributes targeted to a device.

15.12.1 URL

```
https://emmserver.com/emm/iemm/services/deviceCustomAttributes
```

15.12.2 Type

POST

15.12.3 Input

15.12.3.1 Input Parameters

deviceid

This is a mandatory parameter to authenticate a user device to get group details.

15.12.3.2 Input Headers

Content-Type

This is a mandatory parameter, and the allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter. The default value is `application/xml`, and the possible values are `application/xml` or `application/json`

Cookie

This is a mandatory parameter. The value is the output header parameter Set-Cookie value of the previous service.

15.12.4 Output

15.12.4.1 Output Parameters

responseCode

- 1000 = Success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 4006 = Error: Invalid Input

description

Please refer responseCode.

15.12.4.2 Output Headers

Set-Cookie

This helps to maintain a session and pass consecutive services as values of input header parameter Cookie.

15.12.5 Examples

With a valid deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/
deviceCustomAttributes?d=357246053771877
```

Output:

```
Response
               {"afdsa":"dsfafdsa","a1":"A1VALUE"}
```

Without a deviceID

Input:

```
https://emmserver.net:446/emm/iemm/services/deviceCustomAttributes
```

Output:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<emmExceptionHandler>
```

```
<description>Error - Missing Device ID: Device ID should not be
empty</description>
```

```
<responseCode>1003</responseCode>
```

```
</emmExceptionHandler>
```

15.13 User and Device Authentication

This service provides information on the following:

- If a user is locked or not
- If a user is active or not
- Device status
- If a device is rooted/jailbroken or not

This service maintains sessions and secret tokens that contain user and device information.

15.13.1 URL

```
https://emmserver.com/emm/iemm/services/userDeviceInfo
```

15.13.2 Type

POST

15.13.3 Input

15.13.3.1 Input Parameters

d - deviceID

u-User ID

15.13.3.2 Input Headers

Content-Type

This is a mandatory parameter and the allowed value is `application/x-www-form-urlencoded.`

Accept

This is an optional parameter whose default value is “`application/xml`”, and the possible values are `application/xml or application/json.`

Cookie

This is an mandatory parameter. The value is an output header parameter Set-Cookie value of the previous service.

15.13.4 Output

15.13.4.1 Output Parameters

responseCode

- 1000 = success
- 1003 = Error - Missing Device ID: Device ID should not be empty
- 1012 = Error - User does not exist
- 1014 = Error - Missing user ID. User ID should not be empty
- 1015 = User is deleted from EMM
- 3005 = Error - Device is not enrolled with EMM

15.13.4.2 Output Headers

Set-Cookie

Set-cookie helps in maintaining session and is passed in consecutive services as a value of input header parameter "`Cookie`".

15.13.5 Examples

15.13.5.1 With invalid deviceID

Input:

```
https://user.konylabs.net:446/emm/iemm/services/userDeviceInfo?d=10&
u=uday
```

Output:

```
{"description":"Error - Device is not enrolled with
EMM","responseCode":"3005"}
```

15.13.5.2 Without deviceID

Input:

```
https://user.konylabs.net:446//emm/iemm/services/userDeviceInfo?u=ud
ay
```

Output:

```
{"description":" Error - Missing Device ID: Device ID should not be
empty ","responseCode":"1003"}
```

15.13.5.3 Without userID

Input:

```
https://user.konylabs.net:446/emm/iemm/services/userDeviceInfo?d=
353490061504094
```

Output:

```
{"description": “Error - Missing User ID: User ID should not be
empty”,"responseCode": “1014”,}
```

15.13.5.4 Invalid userID

Input:

```
https://user.konylabs.net:446/emm/iemm/services/userDeviceInfo?d=
353490061504094&u=1234
```

Output:

```
{"description":" User doesn't exist ","responseCode":"1012"}
```

15.13.5.5 Device enrolled with a different user

Input:

```
https://user.konylabs.net:446/emm/iemm/services/userDeviceInfo?d=
353490061504094&u=admin
```

Output:

```
{"description":" Success ","responseCode":"1000"
“result” : {“error”:”Device not enrolled against given user” ,
 “userDeviceInfo”:null}
}
```

15.13.5.6 User and Device Information

Input:

```
https://user.konylabs.net:446/emm/iemm/services/userDeviceInfo?d=
353490061504094&u=user1
```

Output:

```
{"description":" Success ","responseCode":"1000"
“result” : {“error”:null ,“userDeviceInfo”:{
“deviceStatus” : “ENROLLED”,
“deviceRooted” : false,
“userActive” : true,
“userLocked” : false
}}
}
```

16. 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.

16.1 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: - **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 entreprise 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.

16.2 Push Messages

The following table displays the push messages:

Push Messages	Scenarios
Your device has been blocked by EMM Admin. You will be logged out.	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.
Your device has been deactivated by EMM Admin. You will be logged out.	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.
Your account has been deactivated by EMM Admin. You will be logged out.	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.
This device is Deactivated. You will not have access to any enterprise resources.Contact your IT Admin in case you have any queries.	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.
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.	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.

Push Messages	Scenarios
Your device is purged by EMM Admin. You will be logged out.	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.
This device is Resumed. You will have access to enterprise resources. Contact your IT Admin in case you have any queries.	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.
This device is Retired. You will not have access to any enterprise resources. Contact your IT Admin in case you have any queries.	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.
This device is Suspended. You will not have access to any enterprise resources.Contact your IT Admin in case you have any queries.	The admin performs the **Suspended Wipe** operation to temporally 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.
Your device has been sent the Block corporate email command. In case you have any queries, contact your IT Admin.	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.

Push Messages	Scenarios
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.	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.
Dear ${userName}, You have successfully enrolled your ${deviceModel} device. In case of any queries, please contact your IT Admin.	A user device is enrolled with the EMM server. A push notification to confirm device enrollment is sent to the user.
Dear ${userName}, You have successfully enrolled your ${deviceModel} device with device code ${deviceCode}. In case of any queries, please contact your IT Admin.	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.
Your Mail+ is Configured.Accept to start using emails.	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.
You are required to Install ${appName} on this device. Check your pending actions to do the same.	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.

Push Messages	Scenarios
Your device enrollment mode has been changed to ${enrollmode} by EMM Admin. Please login to continue. In case of any queries, Contact your IT Admin.	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).
The folder ${foldername} is now shared with you by ${sharedbyname}. You now have access to all its contents.	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.
The folder ${foldername} is no longer shared with you by ${sharedbyname}.	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.
The file ${filename} is shared with you by ${sharedbyname}. You now have access to read the file.	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.
The file ${filename} is no longer shared with you by ${sharedbyname}.	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.
The folder ${foldername} is now available to you with all its contents.	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.

Push Messages	Scenarios
The folder ${foldername} 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 ${filename} has an updated version ${versionnum} 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 ${appname} 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 ${appname} 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.	The current scenario: - 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. 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.
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 ${appname} (${appversion}) 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 ${appname} (${appversion}) 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 `<app name> with <app version>`.

16.3 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 '{}' 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.	The system displays the following error messages, if the authentication settings is configured with **OpenID2** for the following scenarios: 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 occured 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
This device is blocked for you and you cannot access your apps on the same. Contact your EMM Admin for more information.	The error appears for the MAM mode devices while login to the Enterprise store, if the EMM admin has blocked the device.
Your access to corporate resources is suspended. Contact your administrator in case of any further queries.	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.
There are no users with the given email id. Provide a valid email id.	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.

Store Messages	Scenarios
Device enrollment failed	The error message can appear at multiple places during enrollment: 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	The error appears during a device enrollment, if the device does not have a valid enrollment request.
Wipe has been initiated for this device. You are not permitted to login until it is completed.	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: - The EMM admin can initiate wipe for any wrong failed attempts or - The **User** device mode changes from EMM to MAM (for iOS and Windows). In this scenario, the system displays the error message.
IOError writing file to output stream	The error message is displayed in the following scenarios: 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 enrollmnet 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: 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 enrollmnet request flag. It is found that the device information data is null.
Invalid Device id	The error message is displayed in the following scenarios: 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.	Scenario: The error message occurs, while authenticating a user with the given username and password: - The user credentials are expired due to a policy defined by the EMM admin. 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.

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-Agen**t, 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
Device Enrollment Successful. Enterprise Store installation is triggered and may take some time. Once it is installed, login into Enterprise Store using your credentials.	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.
Device Enrollment Successful. For full EMM functionality, please inform your Administrator to update the Enterprise Certificate.	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.

Store Messages	Scenarios
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}.	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.
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	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.

Store Messages	Scenarios
Your access to corporate resources is suspended. Contact your administrator in case of any further queries.	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.
It is observed that Future Enrollment is denied for this Device,thus Un-enroll has been initiated, Contact your admin.	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.
Enter a device code.	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.
Enter a different device code.	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.

17. Frequently Asked Questions

My wrapping is failing when I build an Android application with Kony Visualizer V8 SP2 plug-in and try to wrap the application with Kony Management-GA-8.2. How do I fix this?

Kony Management 8.2.0 wrapping script supports AAPT. If you build an Android application with Visualizer SP2, the application is not wrapped in Kony Management. This is because Visualizer V8 SP2 uses Gradle version 3.0.x which by default uses APPT2. Android applications built with AAPT2 do not work with AAPT. To solve the issue, you must disable AAPT2 in Kony Visualizer.

To disable AAPT2 in Kony Visualizer, do the following:

1. In your Visualizer project, navigate to **Project Settings** > **Native** > **Android**.
2. In the **Android** tab, navigate to the **Manifest Properties & Gradle Build Entries** section.
3. Click the **Gradle Entries** tab.
4. In the **gradle.properties entries:** section, enter the following text.
   ```
   android.enableAapt2=false
   ```
5. Click **Finish**.

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.

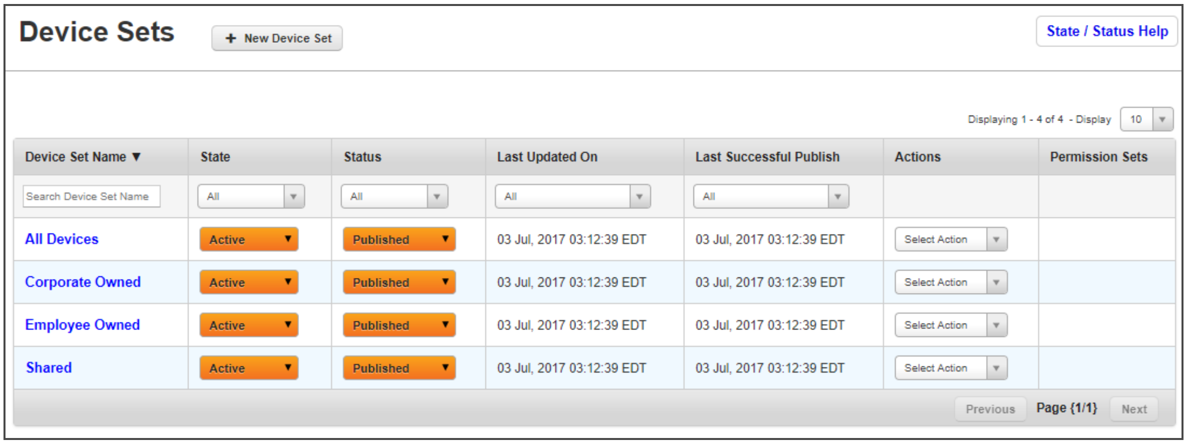
- Sending a message to all devices
- Sending a message to all iOS devices
- Sending a message to all Android devices

For more information on sending push notifications and email messages, refer Kony Management User Guide.

17.1 Sending a Message to All Devices

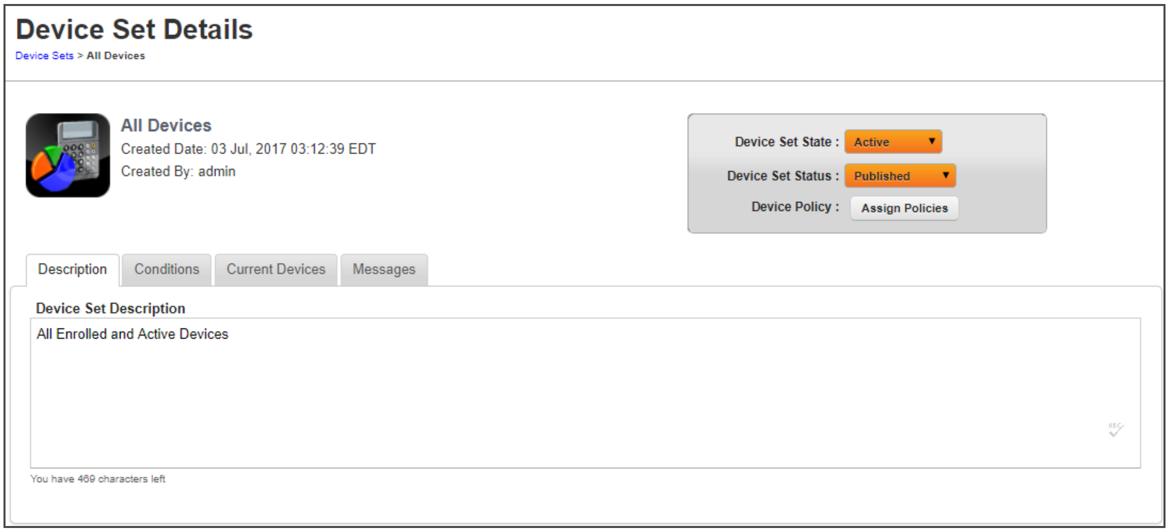
To send a message to all devices, do the following:

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 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	

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

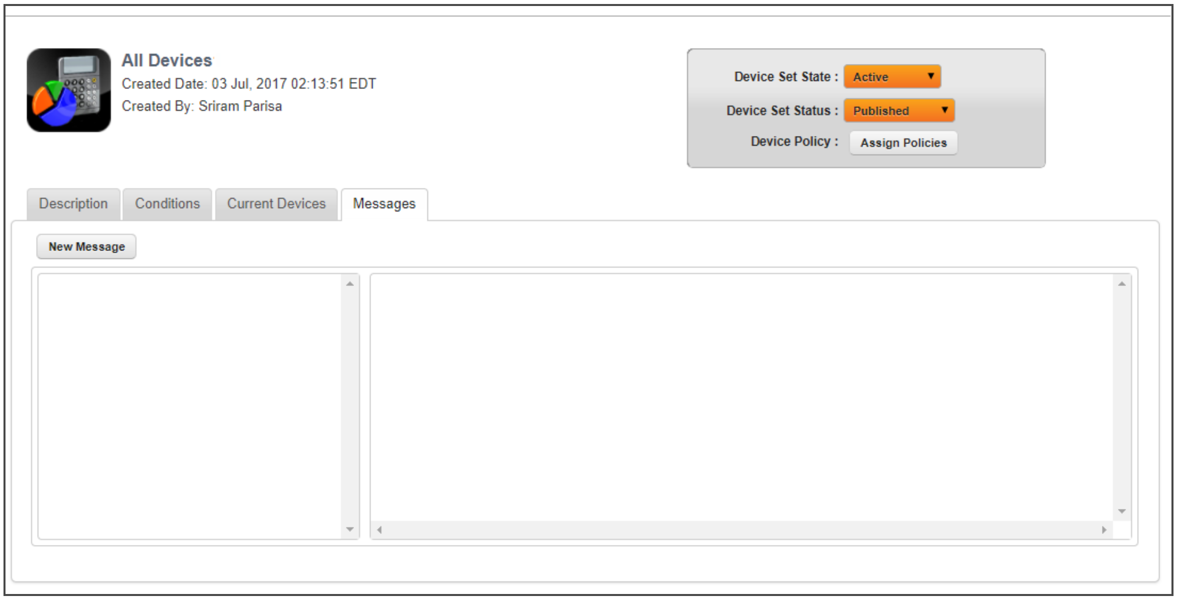
Description | Conditions | Current Devices | Messages

Device Set Description

All Enrolled and Active Devices

You have 469 characters left

3. Click **Messages**. The Messages tab opens.



All Devices

Created Date: 03 Jul, 2017 02:13:51 EDT

Created By: Sriram Parisa

Device Set State : Active

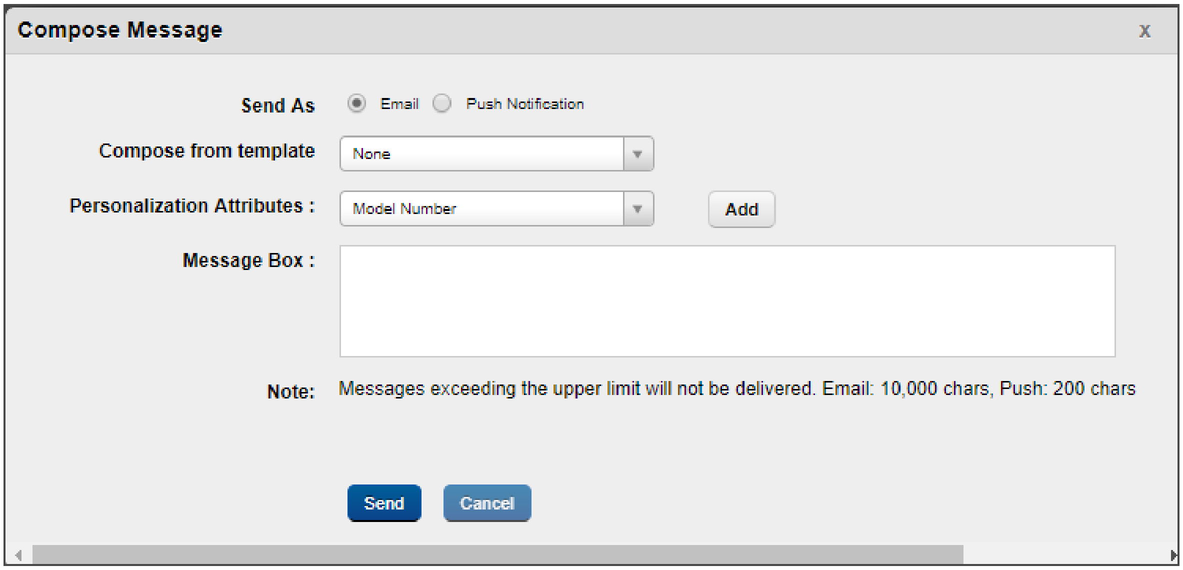
Device Set Status : Published

Device Policy : Assign Policies

Description | Conditions | Current Devices | Messages

New Message

4. Click **New Message**. The Compose Message page appears.



Compose Message

Send As ● Email ○ Push Notification

Compose from template: None

Personalization Attributes : Model Number

Message Box :

Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

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.

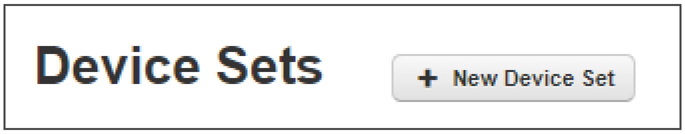
8. Click **OK**. Your message is sent to all devices in the device set.

17.2 Sending a Message to all iOS devices

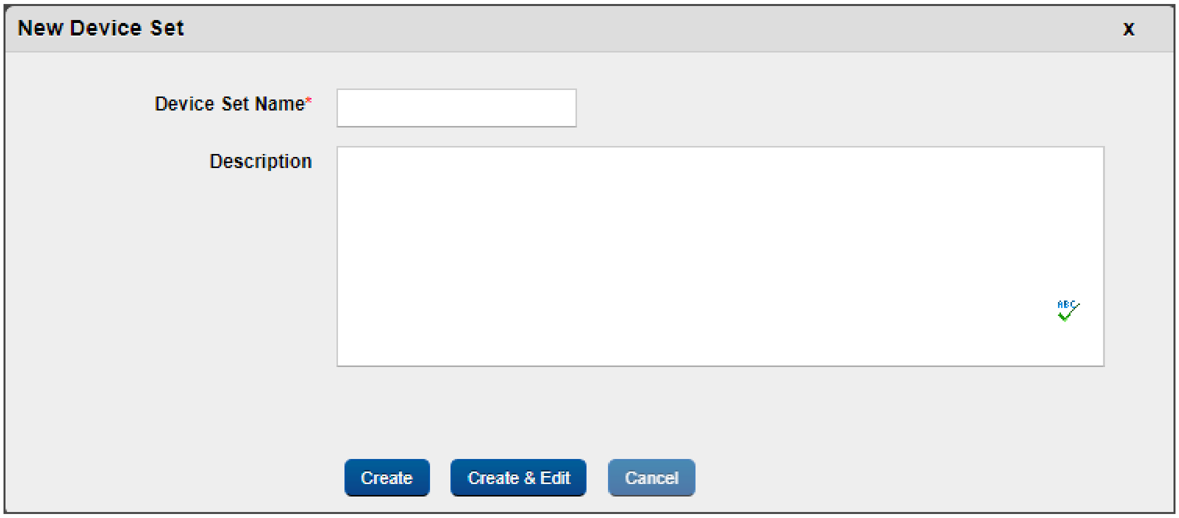
To create a new device set for iOS and send a message to all iOS devices, do the following:

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.



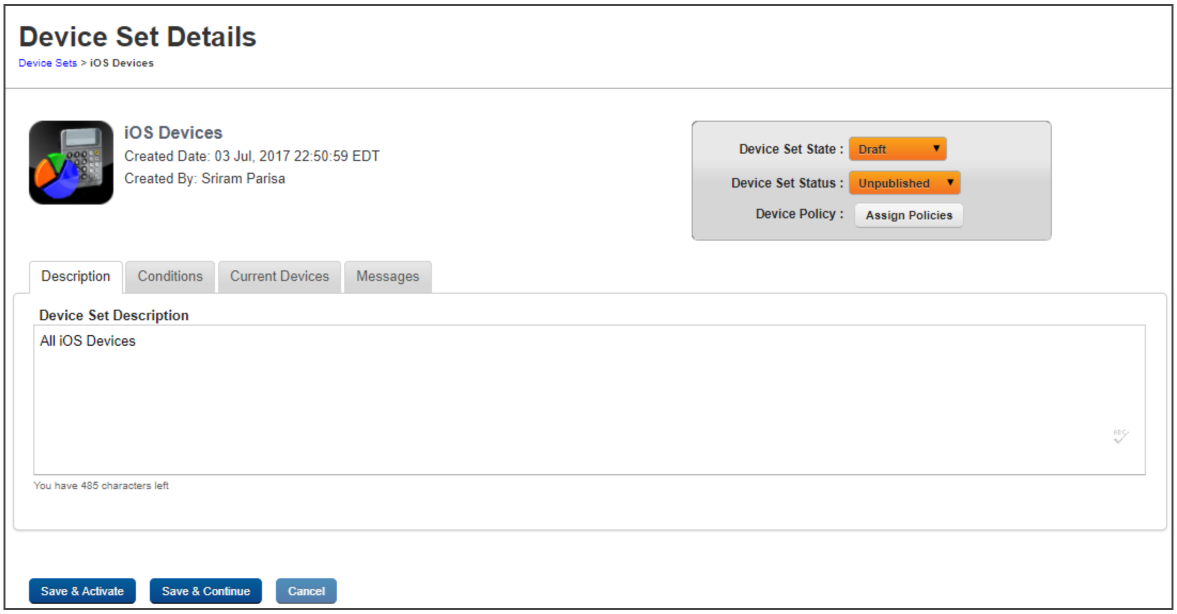
The **New Device Set** window appears.



3. In the **Device Set Name** field, enter **iOS 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 > iOS Devices

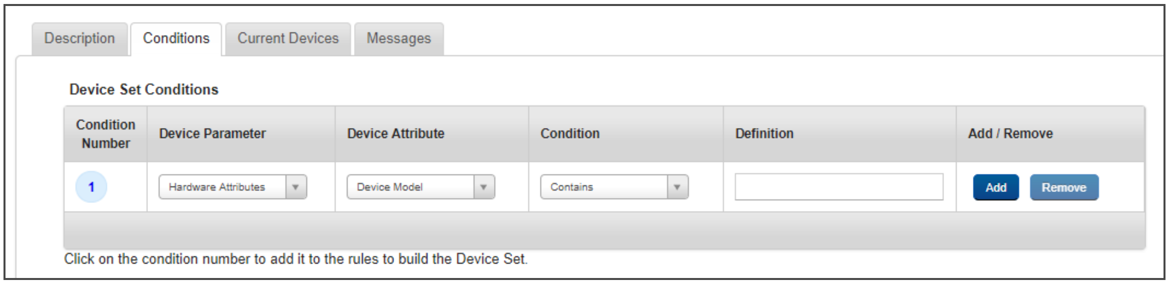
iOS Devices
Created Date: 03 Jul, 2017 22:50:59 EDT
Created By: Sriram Parisa

Device Set State : Draft
Device Set Status : Unpublished
Device Policy : Assign Policies

Device Set Description
All iOS Devices

You have 485 characters left

6. Click **Conditions** tab. The Conditions tab opens.

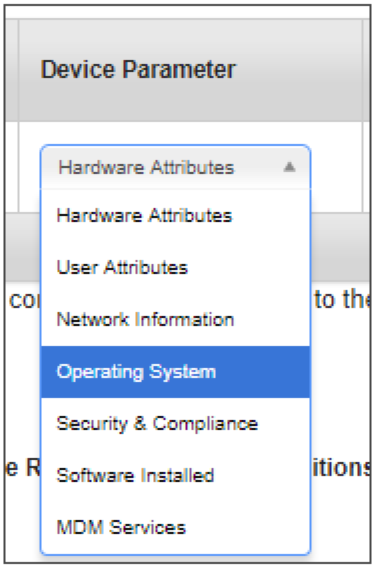


Device Set Conditions

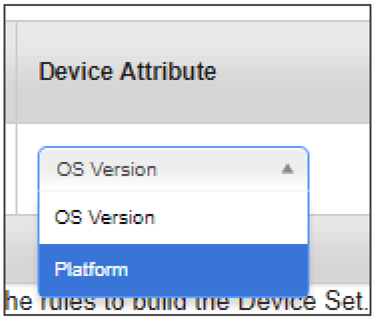
Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Hardware Attributes	Device Model	Contains		Add Remove

Click on the condition number to add it to the rules to build the Device Set.

7. From the **Device Parameter** list, select **Operating System**.

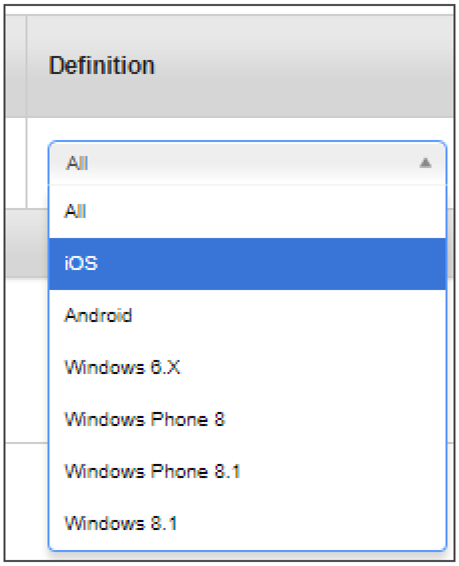


8. From the **Device Attribute** list, select **Platform**.

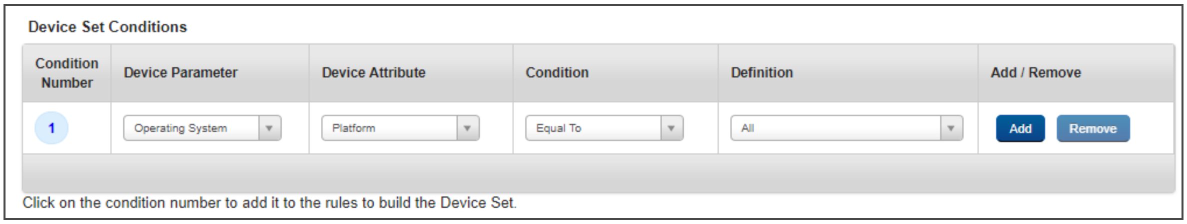


9. Leave the **Condition** list as is to **Equal To**.

10. 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	Add Remove

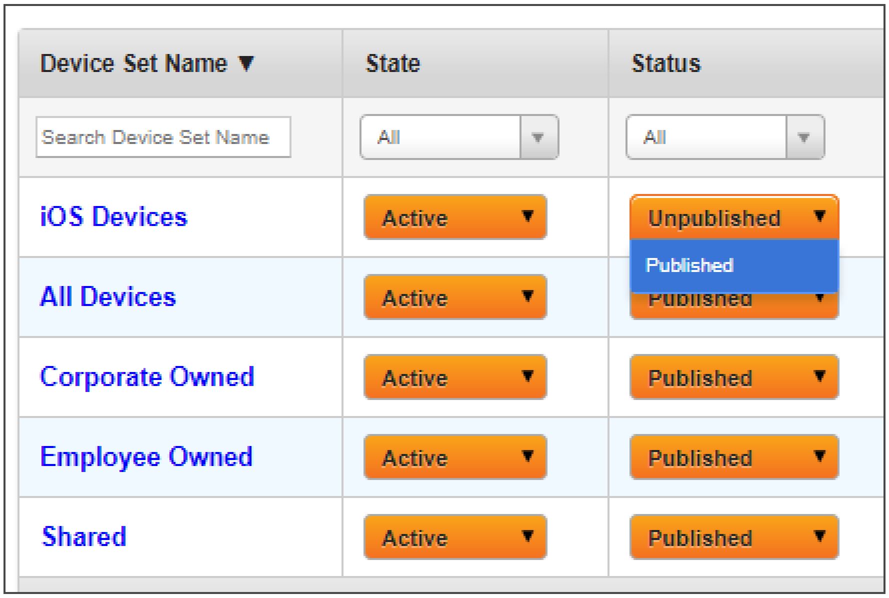
Click on the condition number to add it to the rules to build the Device Set.

11. Click the Condition number to add it to the Definition set.

12. Click **Validate & Search**. All devices that meet the definition criteria set will appear below.

13. 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**.

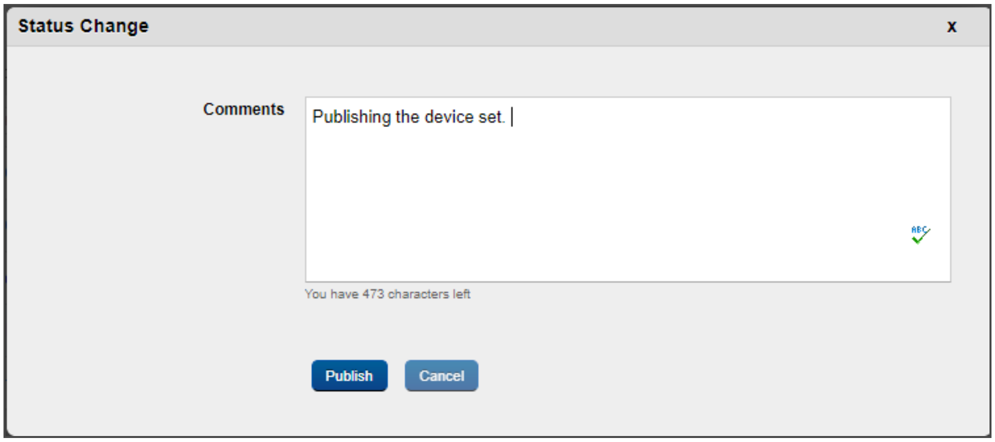
14. From the **Status** column of the device set, click **Published** to publish the device set.



Device Set Name ▼	State	Status
Search Device Set Name	All	All
iOS Devices	Active ▼	Unpublished ▼ Published
All Devices	Active ▼	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

Comments: Publishing the device set.

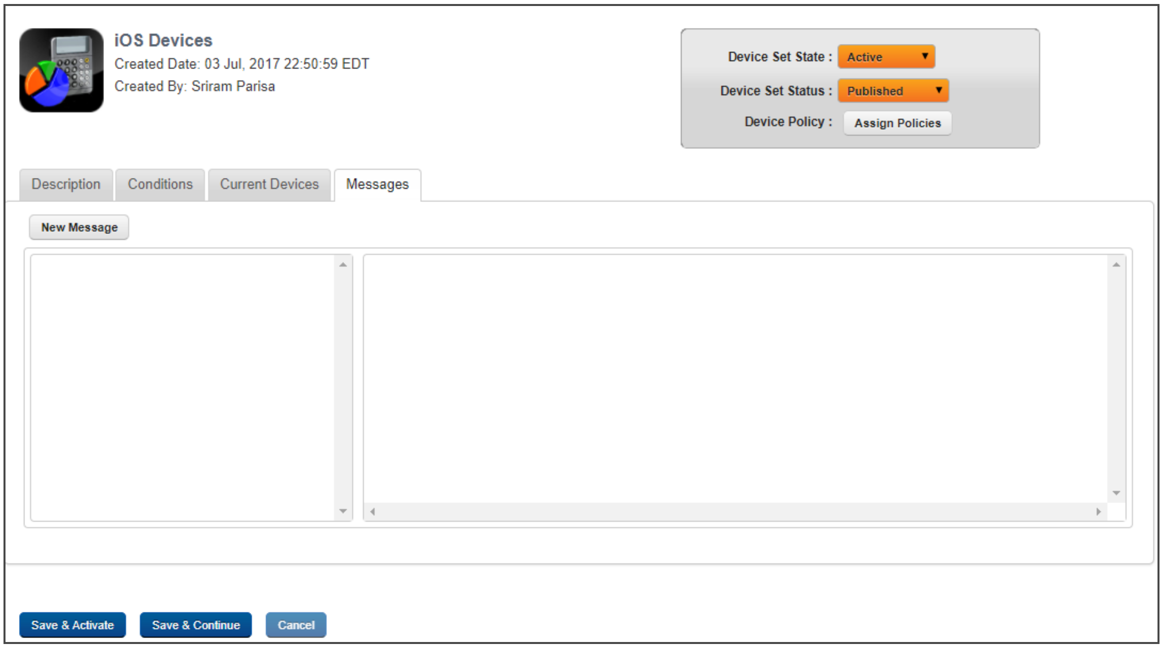
You have 473 characters left

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.

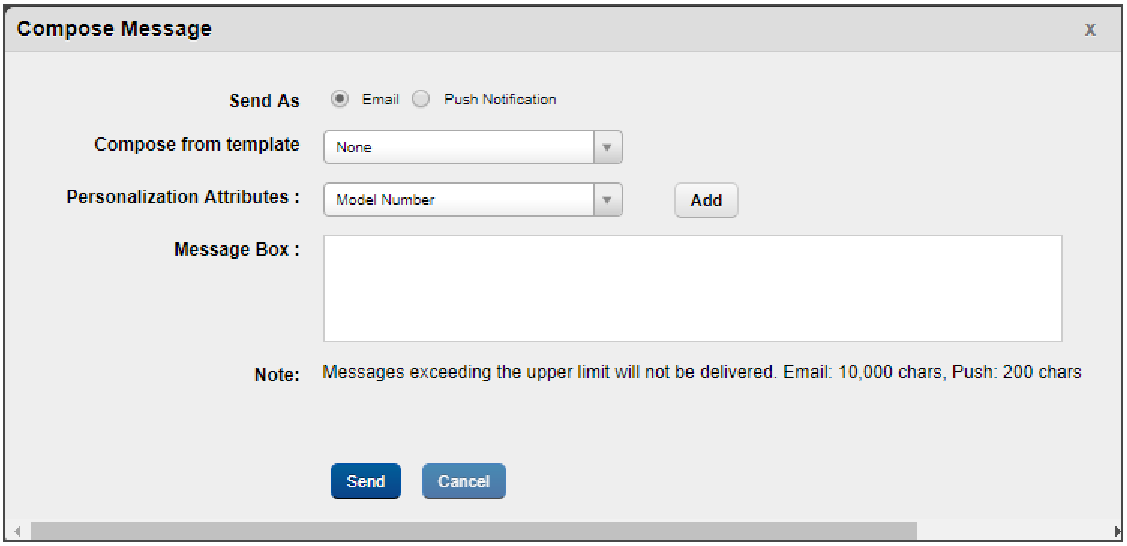
19. Click **Messages**. The Messages tab opens.



iOS Devices
Created Date: 03 Jul, 2017 22:50:59 EDT
Created By: Sriram Parisa

Device Set State : Active
Device Set Status : Published
Device Policy : Assign Policies

20. Click **New Message**. The Compose Message page appears.



Compose Message

Send As: ● Email ○ Push Notification
Compose from template: None
Personalization Attributes : Model Number
Message Box :
Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

21. In the **Send As** field, select **Push Notification**.

22. In the **Message Box**, enter your message.

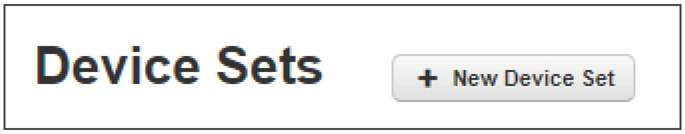
23. Click **Send**. The Send Message - Success message appears.

24. Click **OK**. Your message is sent to all devices in the device set.

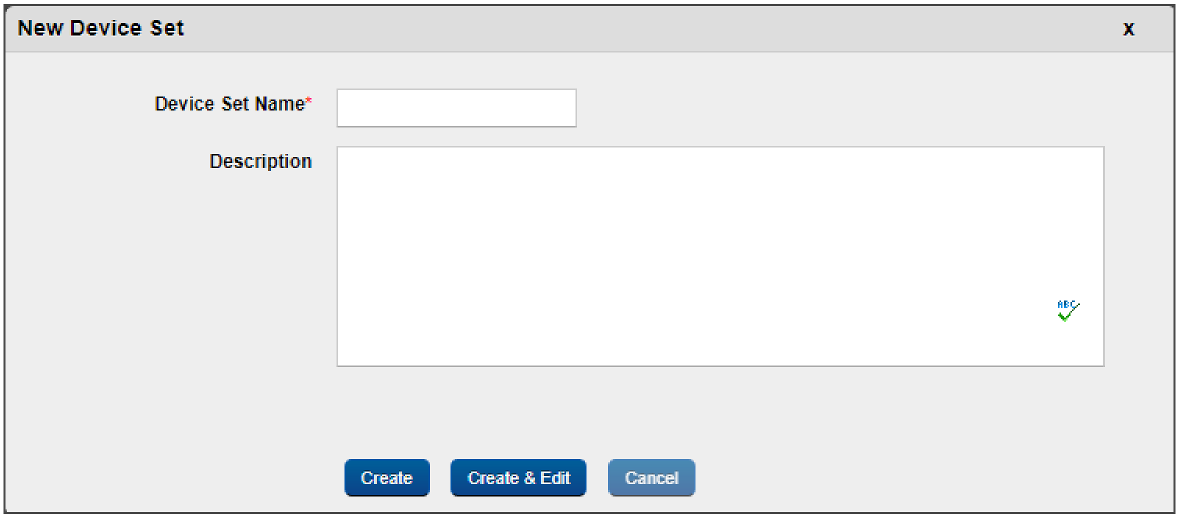
17.3 Sending a Message to all Android devices

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.

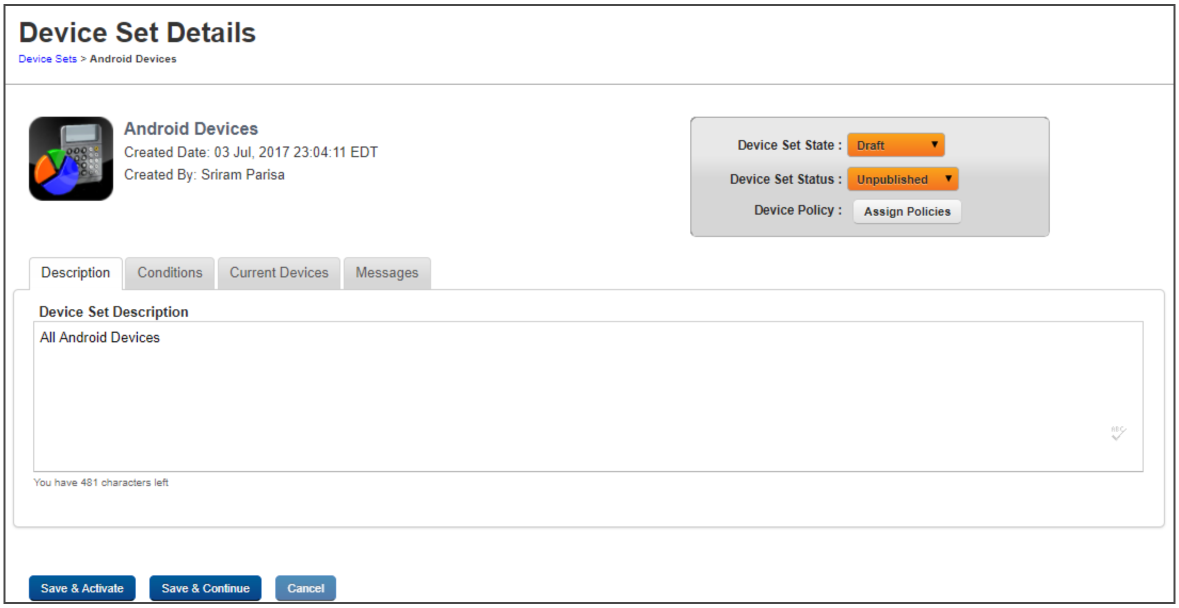


The **New Device Set** window appears.



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

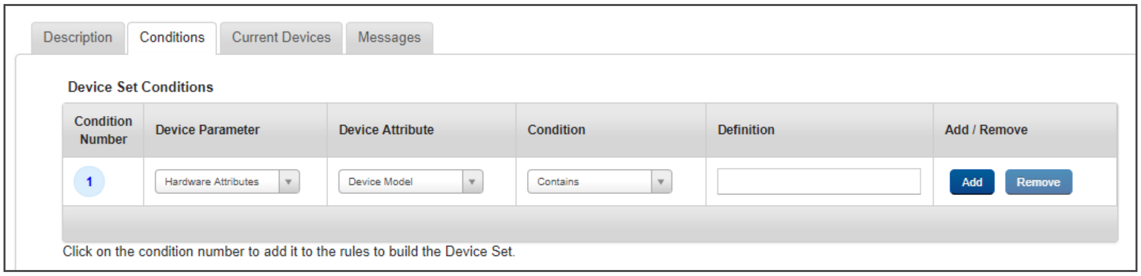
Android Devices
Created Date: 03 Jul, 2017 23:04:11 EDT
Created By: Sriram Parisa

Device Set State : Draft
Device Set Status : Unpublished
Device Policy : Assign Policies

Device Set Description
All Android Devices

You have 481 characters left

6. Click **Conditions** tab. The Conditions tab opens.

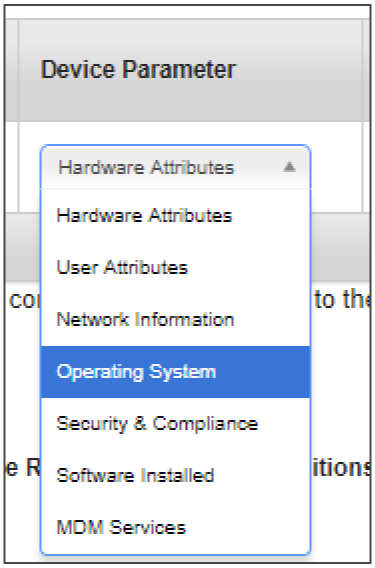


Device Set Conditions

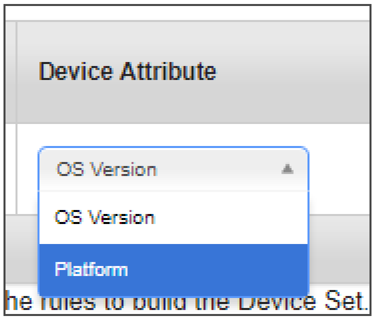
Condition Number	Device Parameter	Device Attribute	Condition	Definition	Add / Remove
1	Hardware Attributes	Device Model	Contains		Add Remove

Click on the condition number to add it to the rules to build the Device Set.

7. From the **Device Parameter** list, select **Operating System**.

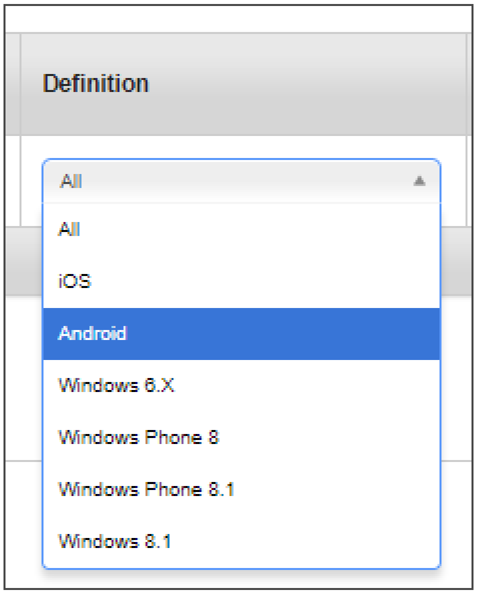


8. From the **Device Attribute** list, select **Platform**.



9. Leave the **Condition** list as is to **Equal To**.

10. From the **Definition** list, select **Android**.



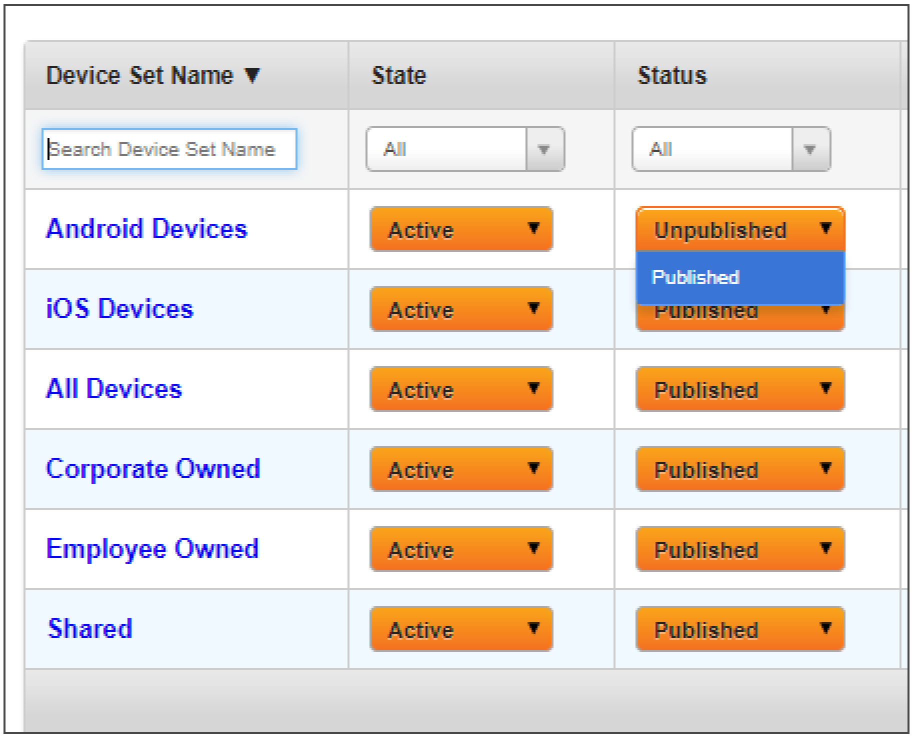
The condition is added.

11. Click the Condition number to add it to the Definition set.

12. Click **Validate & Search**. All devices that meet the definition criteria set will appear below.

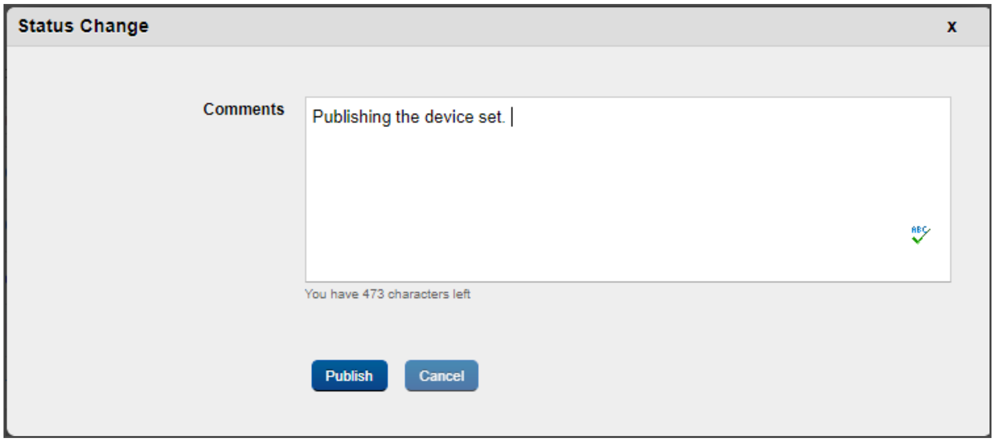
13. Click **Save & Activate**. The device set page appears with the newly created device set in the list. Note that the state of the device set is set to **Active**.

14. From the **Status** column of the device set, click **Published** to publish the device set.



Device Set Name ▼	State	Status
Search Device Set Name	All	All
Android Devices	Active	Unpublished Published
iOS Devices	Active	Published
All Devices	Active	Published
Corporate Owned	Active	Published
Employee Owned	Active	Published
Shared	Active	Published

The Status Change dialog appears.



Status Change

Comments: Publishing the device set.

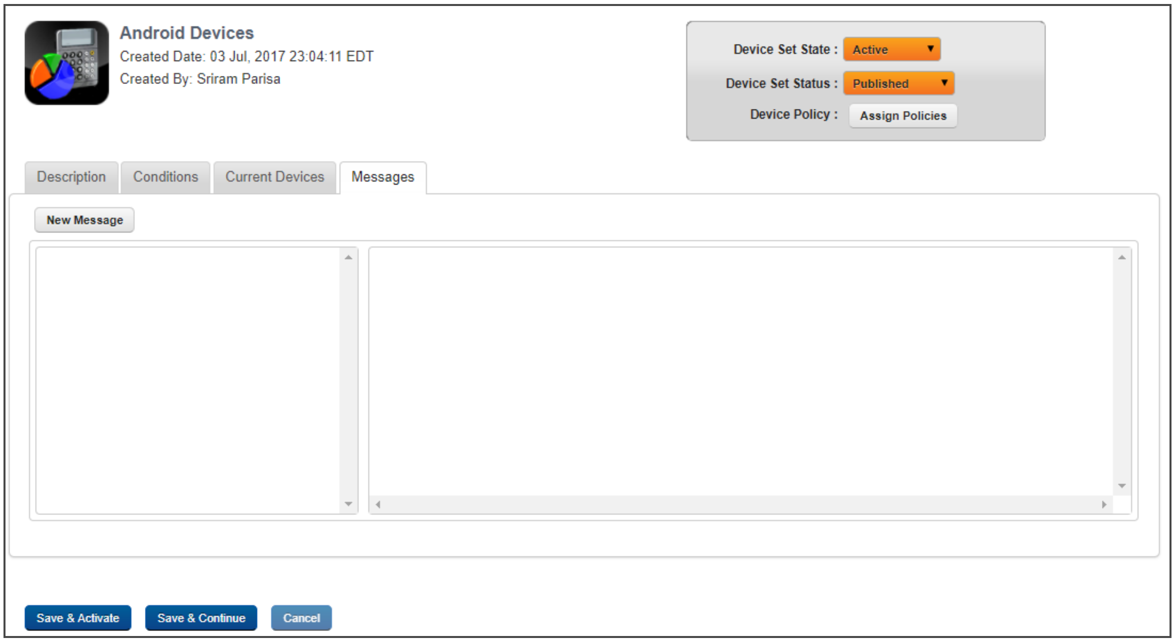
You have 473 characters left

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.

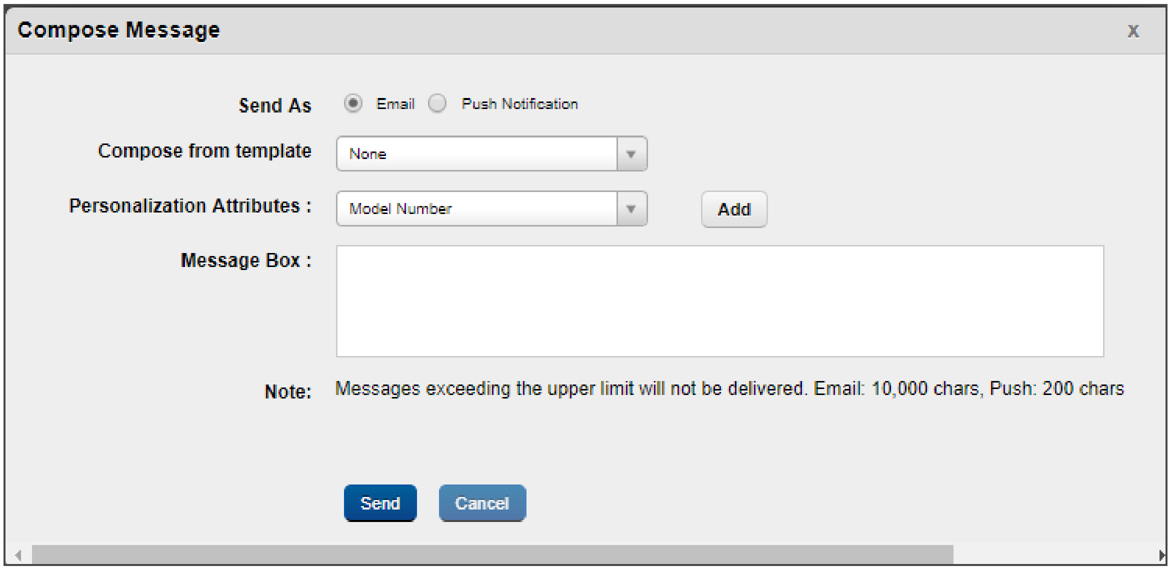
18. Click **Messages**. The Messages tab opens.



Android Devices
Created Date: 03 Jul, 2017 23:04:11 EDT
Created By: Sriram Parisa

Device Set State : Active
Device Set Status : Published
Device Policy : Assign Policies

19. Click **New Message**. The Compose Message page appears.



Compose Message

Send As ● Email ○ Push Notification
Compose from template: None
Personalization Attributes : Model Number
Message Box :
Note: Messages exceeding the upper limit will not be delivered. Email: 10,000 chars, Push: 200 chars

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.

18. Annexure

18.1 Internet Explorer 9 Compatibility Issues

Issue

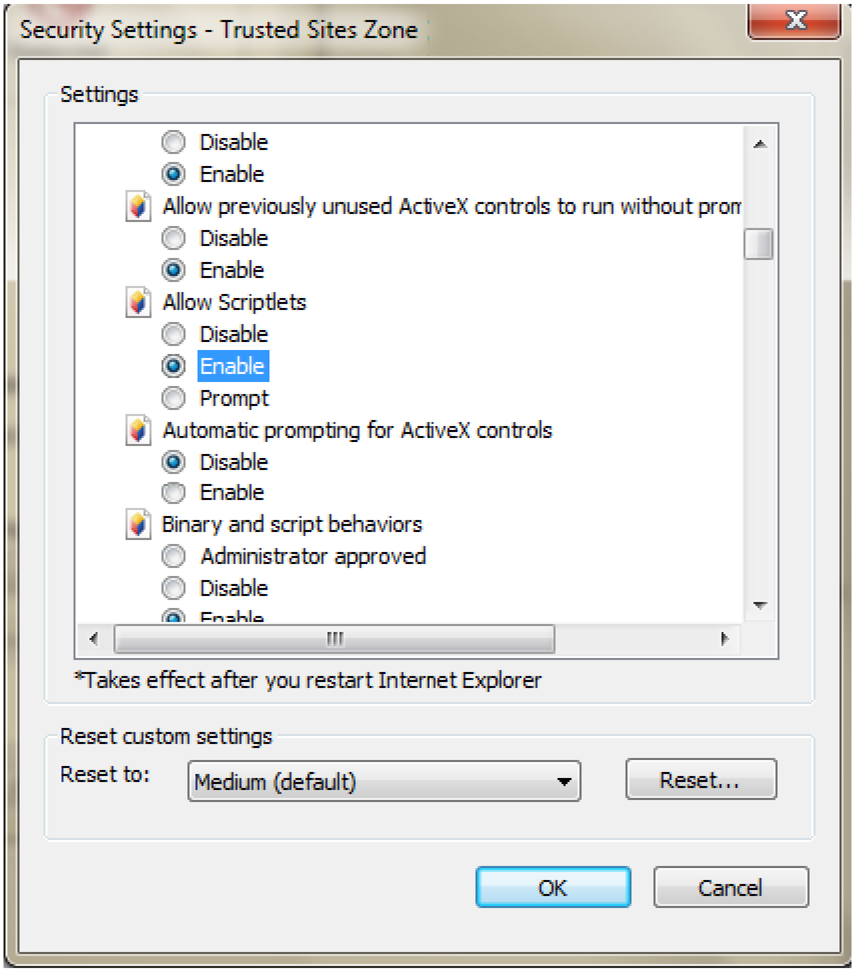
If you login to EMM application using Internet Explorer 9, and when you unpublish a policy from the Policy Details page, IE9 is unable to resolve the resultant page. To resolve this issue, follow the below workaround.

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.



Security Settings - Trusted Sites Zone

Settings

○ Disable
● Enable

Allow previously unused ActiveX controls to run without prom

○ Disable
● Enable

Allow Scriptlets

○ Disable
● Enable
○ Prompt

Automatic prompting for ActiveX controls

● Disable
○ Enable

Binary and script behaviors

○ Administrator approved
○ Disable
● Enable

*Takes effect after you restart Internet Explorer

Reset custom settings

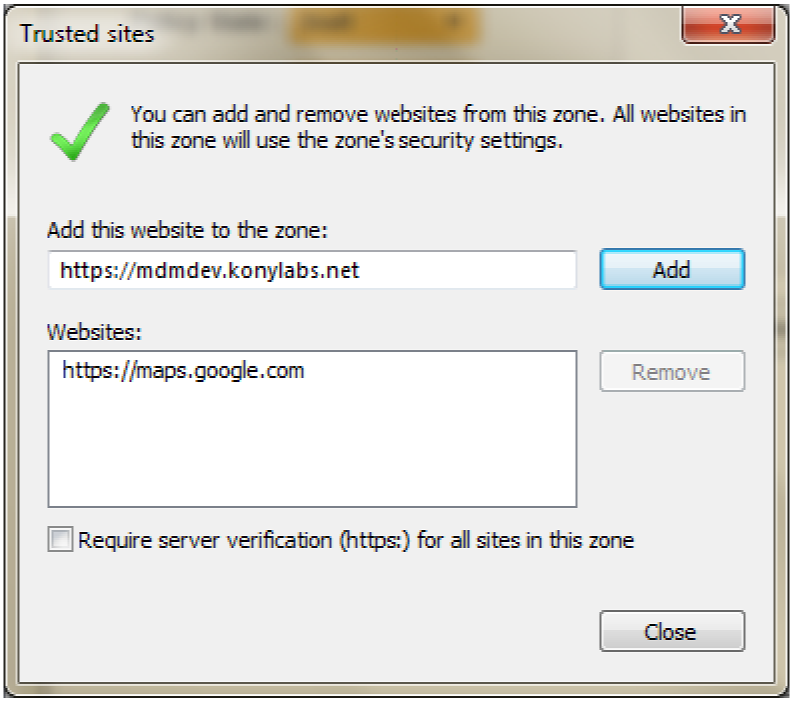
Reset to: Medium (default)

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.



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

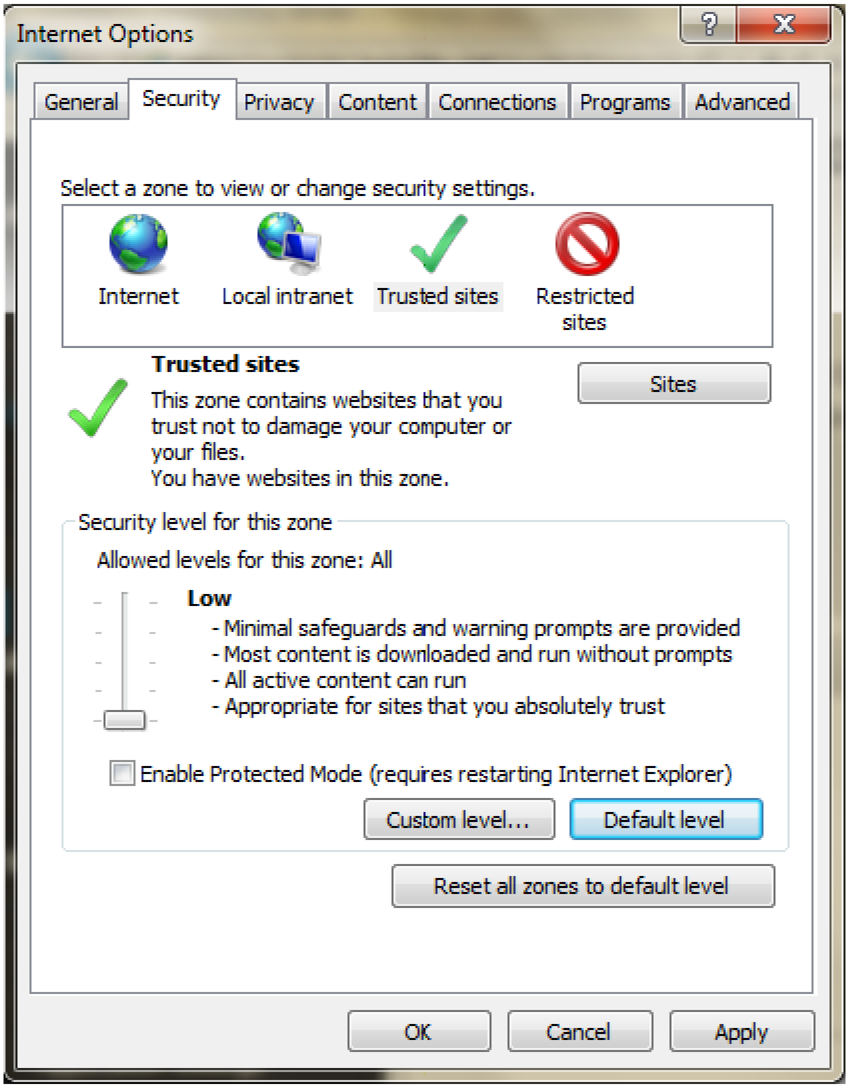
https://mdmdev.konylabs.net

Websites:

https://maps.google.com

□ Require server verification (https:) for all sites in this zone

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.



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

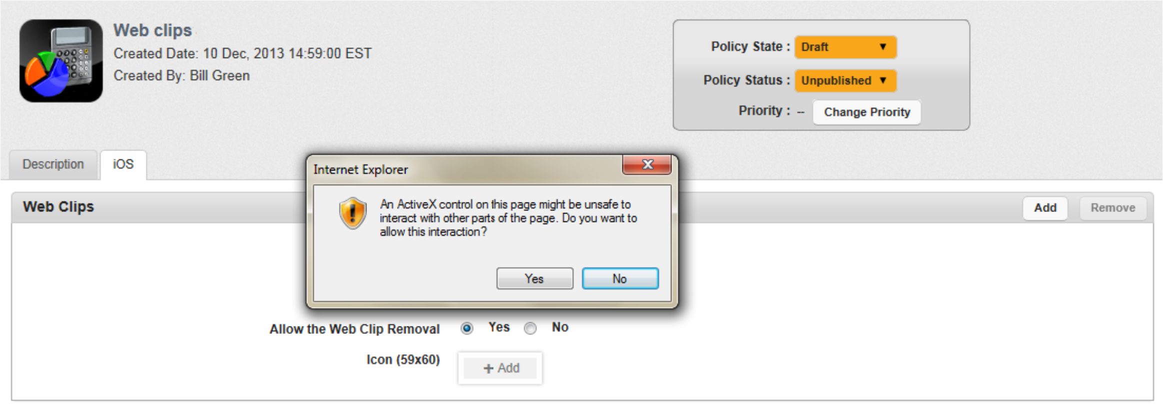
Allowed levels for this zone: All

Low

- Minimal safeguards and warning prompts are provided
- Most content is downloaded and run without prompts
- All active content can run
- Appropriate for sites that you absolutely trust

□ Enable Protected Mode (requires restarting Internet Explorer)

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.



Web clips
Created Date: 10 Dec, 2013 14:59:00 EST
Created By: Bill Green

Policy State : Draft
Policy Status : Unpublished
Priority : --

Internet Explorer

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

Allow the Web Clip Removal ● Yes ○ No

Icon (59x60)

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.