User Guide

Fusion EMM

Manage & Maintain IT Environment

vxl software

User Guide

Published on 8th Dec 2016

Last Updated on 8th Dec 2016

Document Version 1.0

Documentation Disclaimer

Screenshots and graphics in this manual may differ slightly from your product due to differences in your product release version or your computer operating system. Reasonable efforts were made to ensure that the information in this document was complete and accurate. VXL Software Solutions Pvt. Ltd. assumes no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Copyright

Trademarks

VXL Support

To access our support systems please navigate to http://vxlsupport.me and log a ticket.

VXL Software Solutions Pvt. Ltd.
241/242, Solitaire Corporate Park,
Chakala, Andheri(E),
Mumbai-400093
www.vxlsoftware.com

Table of Contents

Introduction & Getting Started

This document consists of administrator user instructions for Fusion EMM Software. The document assumes that Fusion EMM Software is already installed as per the instructions provided in the Installation manual.

Fusion EMM is a web based remote management application for managing client devices.

Fusion EMM enables administrators to manage or monitor the following networked devices:

- Portable Tablet Computing Devices
- Mobile Phones
- Handheld Data Acquisition Devices

Fusion EMM can manage and monitor devices consist of following types of operating systems:

- iOS
- Android

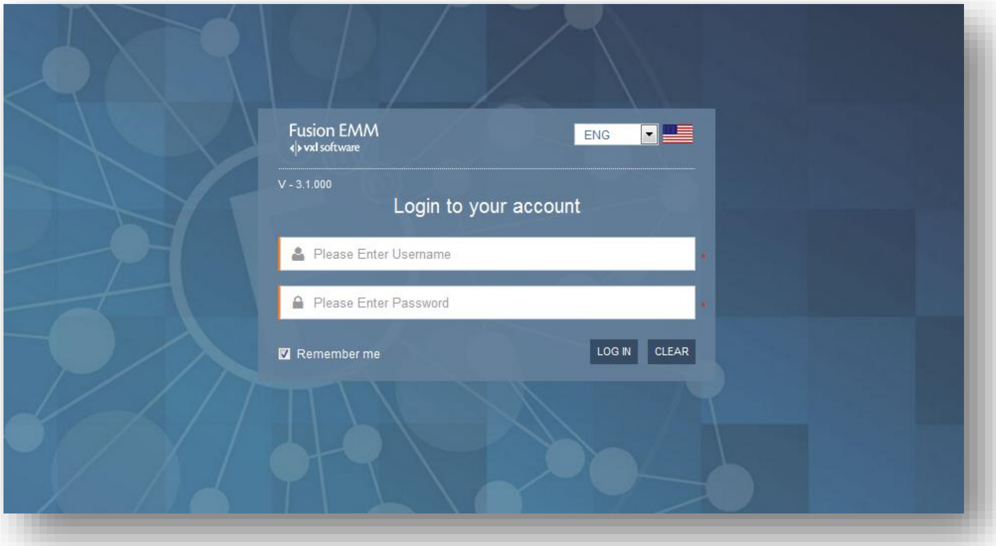
Login to Fusion EMM

1. Open the web browser.

   Enter the URL in the format: http ://< server IP address/ Host name>

If using SSL, enter the URL in the format: https://<server HOST NAME only>

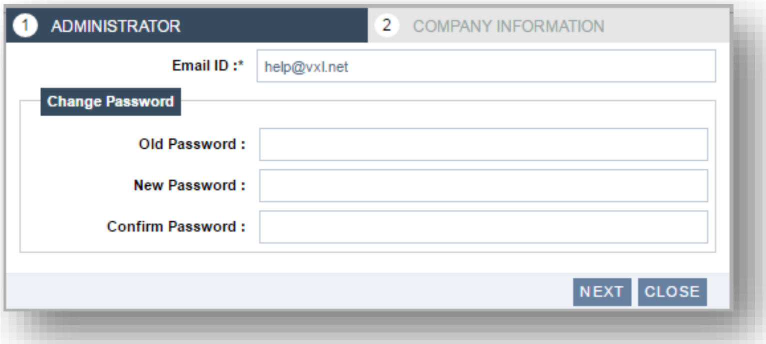
2. Select language from dropdown. After selection, respective language will be effective on Fusion EMM server.
3. In **User Name,** enter the default user name **admin**.
4. For both user names, in **Password** enter the default password **admin**.
5. Click **Log in**.



- On Login Screen, flag indicates the browser language
- To log in to Fusion EMM subsequently, you need to create a new user through the **Configuration Setup** feature of Fusion EMM.
- When User keeps server idle for 30 minutes, user get session out/ sign out message on server.
- If browser gets closed accidently after user login then user gets release within 1 Min.

For information about creating a new user, see “Creating a User"” in “Configuring Fusion EMM”.

When you login in to Fusion EMM for the first time, dialog boxes to change password and configure company information with default group name, as shown below, are displayed.



Email ID :* help@vxl.net

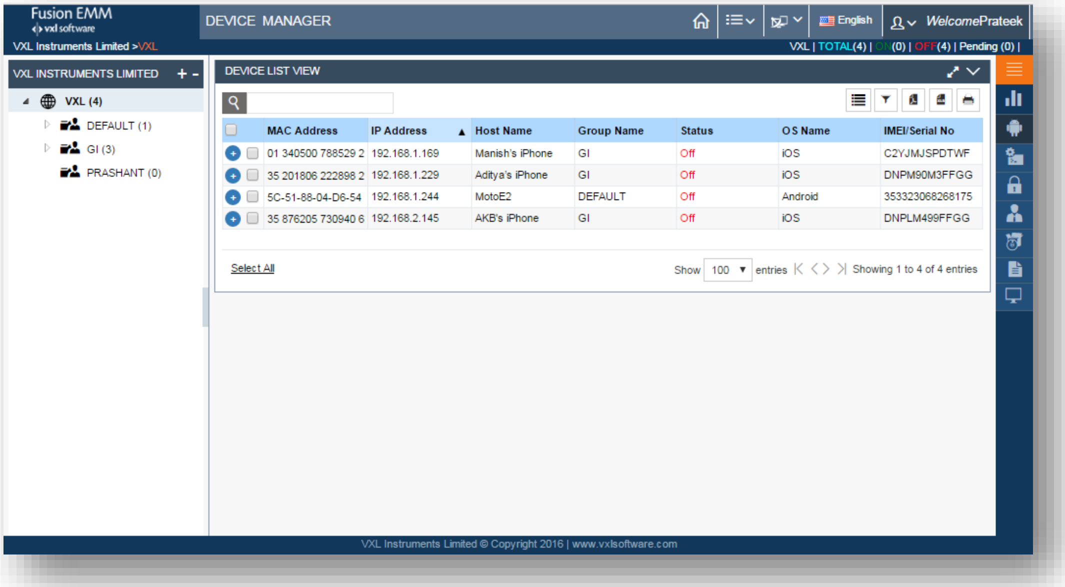
Change Password

Old Password :

New Password :

Confirm Password :

After successful authentication, the Home (**Device Manager**) page is display.



VXL Instruments Limited >VXL

VXL | TOTAL(4) | ON(0) | OFF(4) | Pending (0) |

MAC Address	IP Address	Host Name	Group Name	Status	OS Name	IMEI/Serial No
01 340500 788529 2	192.168.1.169	Manish's iPhone	GI	Off	iOS	C2YJMJSPDTWF
35 201806 222898 2	192.168.1.229	Aditya's iPhone	GI	Off	iOS	DNPM90M3FFGG
5C-51-88-04-D6-54	192.168.1.244	MotoE2	DEFAULT	Off	Android	353323068268175
35 876205 730940 6	192.168.2.145	AKB's iPhone	GI	Off	iOS	DNPLM499FFGG

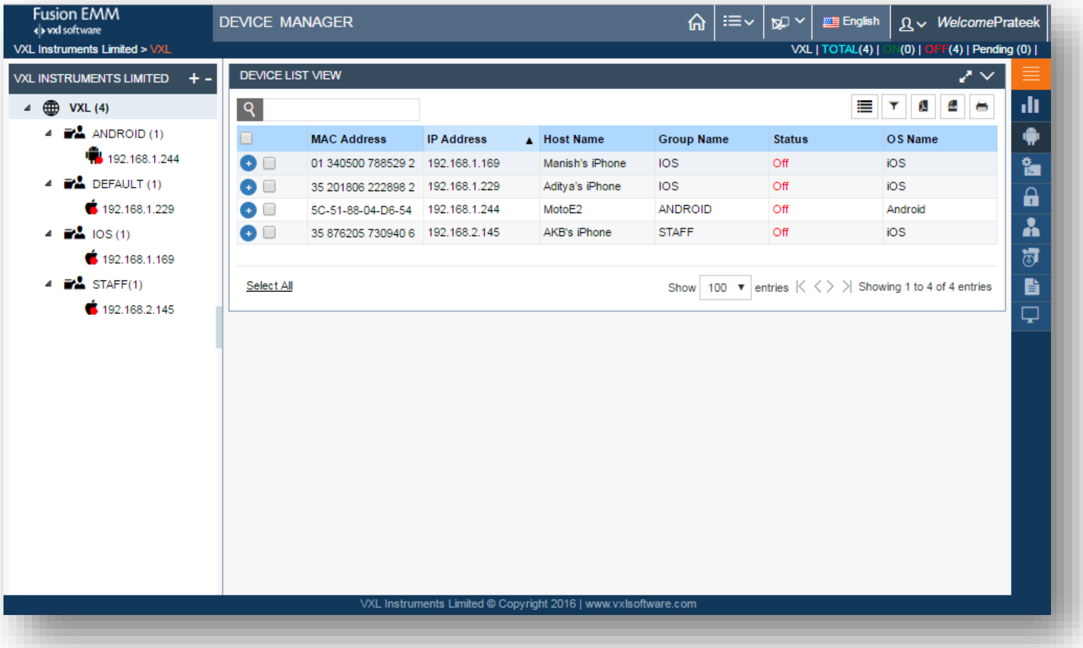
Show 100 entries Showing 1 to 4 of 4 entries

VXL Instruments Limited © Copyright 2016 | www.vxlsoftware.com

- On Toolbar flag indicates the browser language.
- Next to flag, selected language name will be viewed.

Understanding the Interface

The home page displays the devices, device groups, and status of newly created tasks. You can also create new tasks using Fusion EMM's commands and functions, and use the icons and menus to navigate Fusion EMM.



	MAC Address	IP Address	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	IOS	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All
Show 100 entries
Showing 1 to 4 of 4 entries
VXL Instruments Limited © Copyright 2016 | www.vxlsoftware.com

Devices Tree

The devices tree displays devices registered in Fusion EMM. It enables you to create groups to place the managed devices in a logical order.

Devices are displayed at the group level and at the device or terminal node level. You can add, edit or delete groups and subgroups; and configure their settings in the devices tree.

At the highest level of the devices tree, the company name is display by default. Below the company name is the name of the specific site of the company.

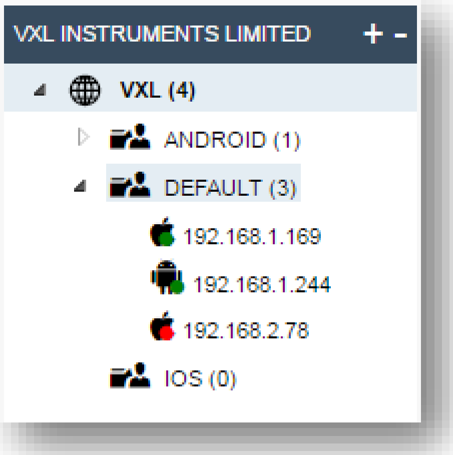
The default group is display below the site name. When devices are discovered and enrolled for management in Fusion EMM , they are automatically registered into the default group. You can create other groups, in addition to the default group, under a site.

You can also add subgroups to a group. The subgroups added are listed under the group in the devices tree.

You can add client devices to a group or to a subgroup. The devices are listed under the respective group or subgroup.

In the example, the device tree hierarchy is display as:

1. Company: VXL Instruments Limited
2. Site: VXL
3. Group: Default and VXL Group
4. Subgroup: New subgroup
5. Devices: 192.168.1.169, 192.168.1.244 and 192.168.2.78.

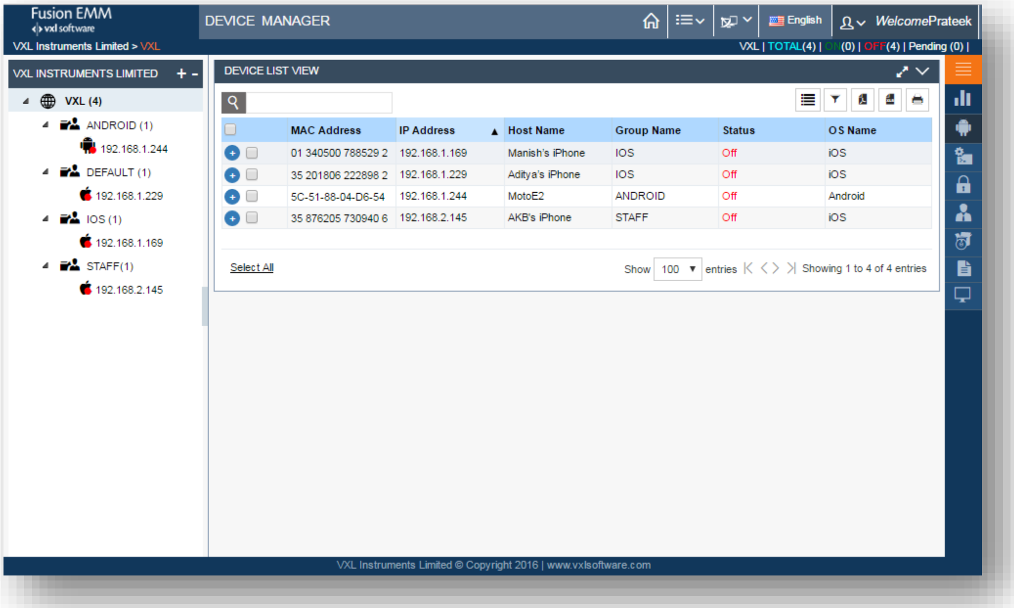


The company, site and default group name is as per the company information entered when you first log in to Fusion EMM . The number of subgroups you can add to a group is also limited by the group level you have entered at the time of initial Fusion EMM log in.

The default group name (Default) and group level (10) displayed in **Company Information** at the time of the initial log in can be changed if required.

For more information about the devices tree, see "Working with the Devices Tree."

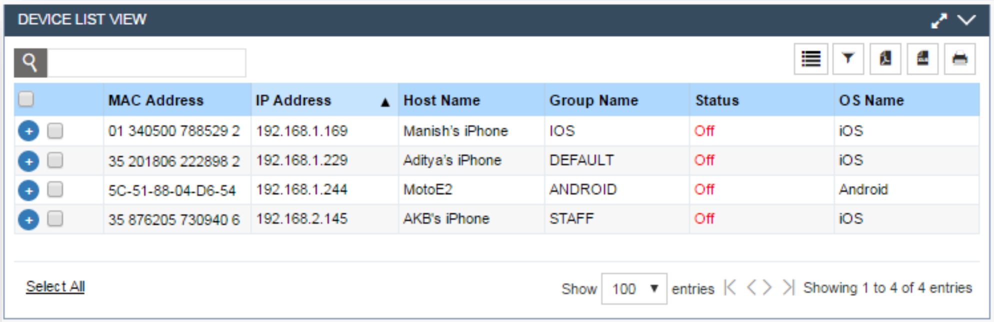
Group View



□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	IOS	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

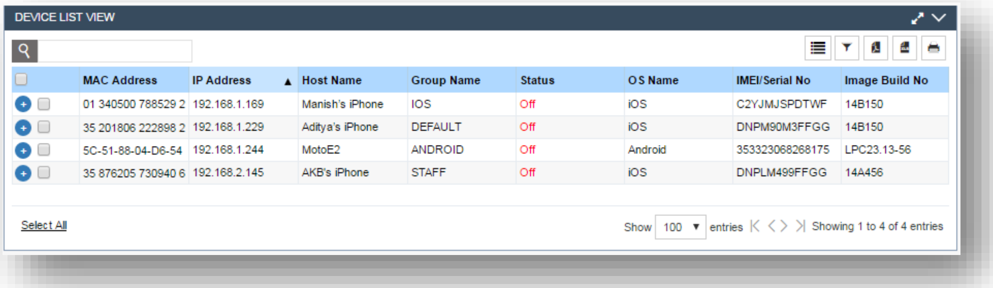
The group view displays the devices in a group along with the MAC address, IP address, Host name and similar details for each device.

Device List View



□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

If you resize the screen,some columns may not be displayed.



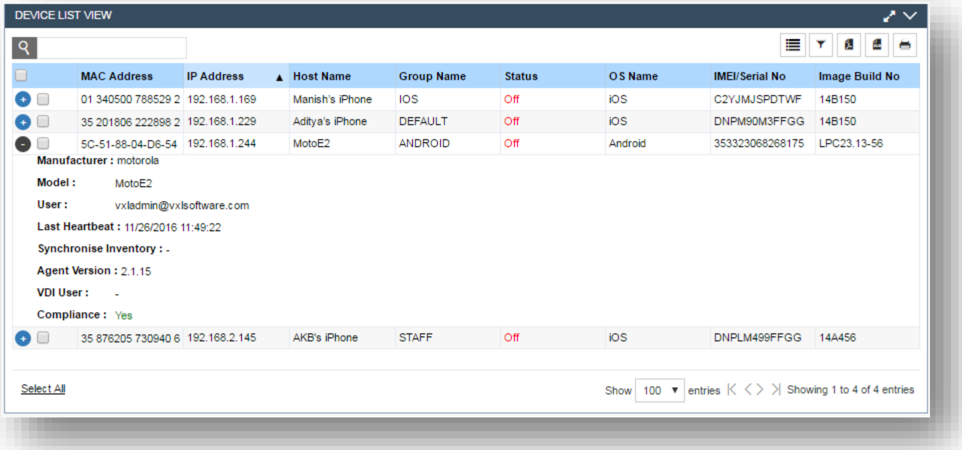
DEVICE LIST VIEW

□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No	Image Build No
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS	C2YJMJSPDTWF	14B150
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS	DNPM90M3FFGG	14B150
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android	353323068268175	LPC23.13-56
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS	DNPLM499FFGG	14A456

Select All

Show 100 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

To view device details in columns not shown in the table, click +.



DEVICE LIST VIEW

□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No	Image Build No
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS	C2YJMJSPDTWF	14B150
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS	DNPM90M3FFGG	14B150
- □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android	353323068268175	LPC23.13-56

Manufacturer : motorola

Model : MotoE2

User : vxladmin@vxlsoftware.com

Last Heartbeat : 11/26/2016 11:49:22

Synchronise Inventory : -

Agent Version : 2.1.15

VDI User : -

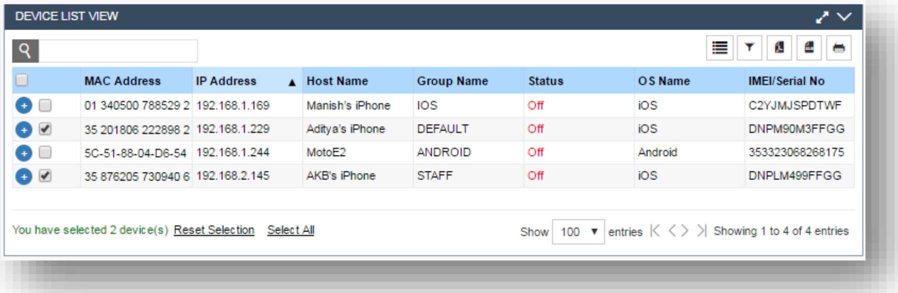
Compliance : Yes

□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No	Image Build No
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS	DNPLM499FFGG	14A456

Select All

Show 100 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

From the group view, you can select multiple devices and apply a setting to all the selected devices.



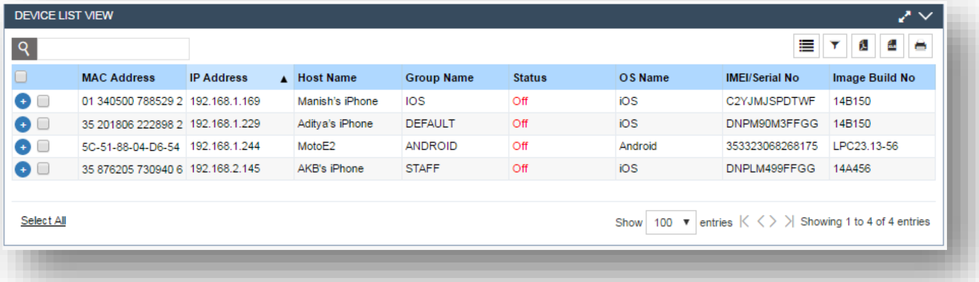
DEVICE LIST VIEW

□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS	C2YJMJSPDTWF
+ ☑	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS	DNPM90M3FFGG
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android	353323068268175
+ ☑	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS	DNPLM499FFGG

You have selected 2 device(s) Reset Selection Select All

Show 100 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

To choose the columns to view in the group view



DEVICE LIST VIEW

□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No	Image Build No
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS	C2YJMJSPDTWF	14B150
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS	DNPM90M3FFGG	14B150
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android	353323068268175	LPC23.13-56
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS	DNPLM499FFGG	14A456

Select All

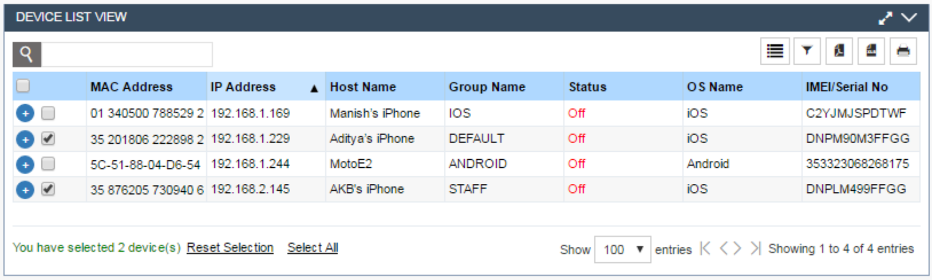
Show 100 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

1. In the area above the table, click ☰.
2. Select the check boxes for the columns to view.
3. To view details of columns that are not displayed in the table, click + in the first column next to the **MAC Address** column.
4. To view details of a specific device, in the **MAC Address** column, click MAC address of the required device.

The device details are displayed below the table.

Applying Settings to Multiple Devices

From the group view, you can select multiple devices and apply a setting to all the selected devices.



DEVICE LIST VIEW

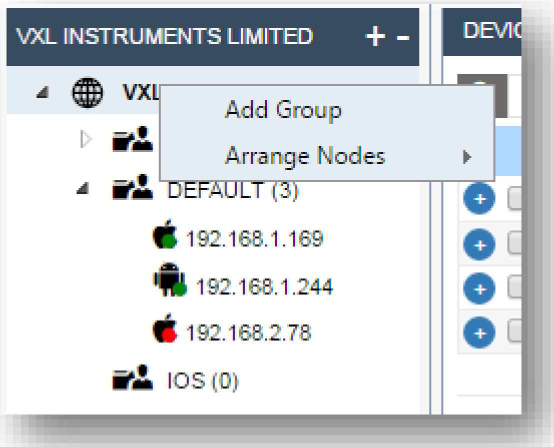
□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name	IMEI/Serial No
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	IOS	Off	iOS	C2YJMJSPDTWF
+ ☑	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS	DNPM90M3FFGG
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	Off	Android	353323068268175
+ ☑	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS	DNPLM499FFGG

You have selected 2 device(s) Reset Selection Select All

Show 100 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

Context Menu

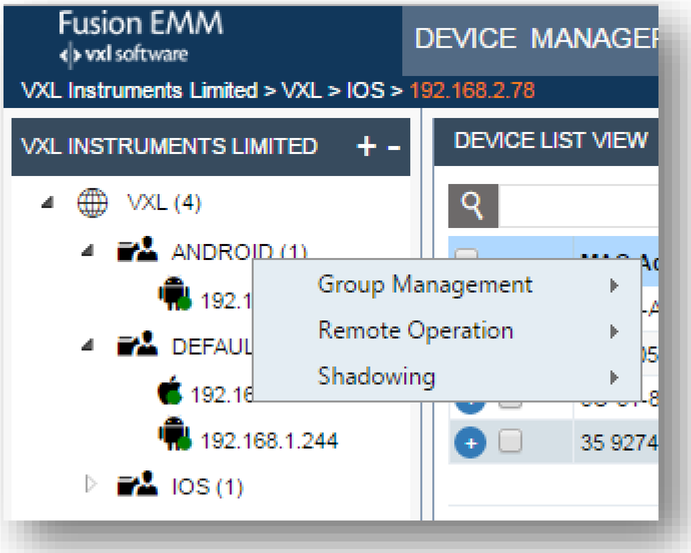
Right click on any device/ group /Site context menu option shows, which include,



SITE:

- Add Group
- Arrange Nodes:
    - IP address
    - Mac Address
    - Host Name

Group / Node:



- Group Management (only for node)
    - Add Subgroup
    - Edit Group

    - Delete Group
- Remote control tools
    - Sync Inventory
    - Send Message/ ALL
    - Lock Device / ALL
- Shadowing
    - VNC

* Some settings are Restricted to node and vice versa.

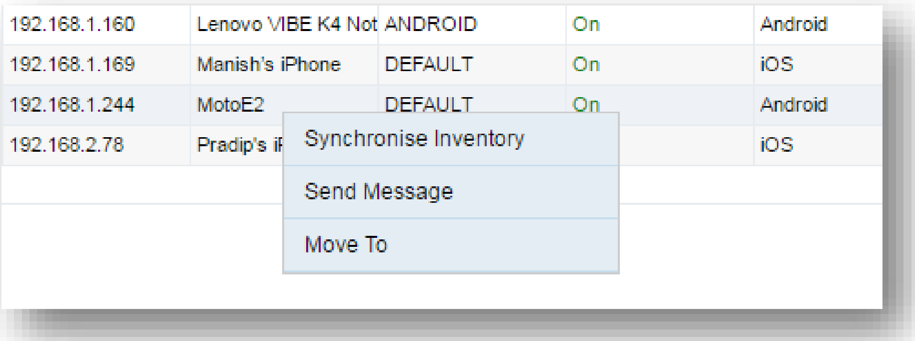
Working with Remote Control

Remote control enables the administrator to remotely control functions such as, locking, shutting down, and restarting devices in a group.

From the group view/ Device List view, you can manage the remote control functions described below.

Function	Description
Synchronizing inventory	Sync data for the all devices in a group
Sending messages	Send a messages to client devices in a group
Move to	We can move selected client to group in which we want to move.

To administer the functions remotely, right-click in the table in the group view.



192.168.1.160	Lenovo VIBE K4 Not	ANDROID	On	Android
192.168.1.169	Manish's iPhone	DEFAULT	On	iOS
192.168.1.244	MotoE2	DEFAULT	On	Android
192.168.2.78	Pradip's iP			iOS

Select and apply the required remote control function.

For information on applying remote control functions , see the following sections in "Working with Remote Control" in “Working with the Devices Tree”.

- Synchronizing Inventory
- Sending Messages to Devices

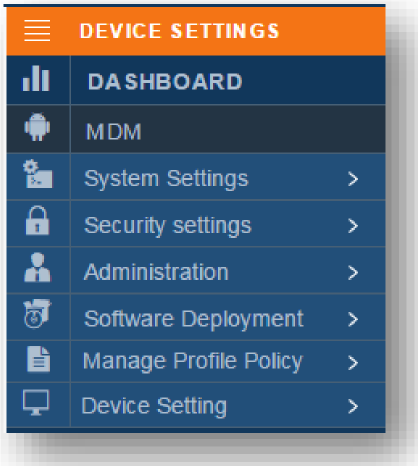
Viewing Operating System Profile

You can view the operating system profile for the devices in a group.

The information displayed is specific to the operating system. For example, the information displayed for an Android system is different from the information displayed for a iOS system.

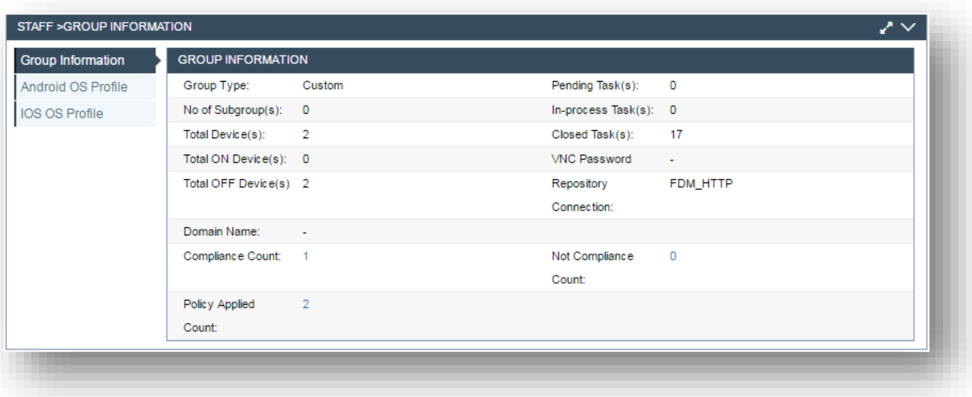
To view the profile details

1. In the devices tree, select the required group.



2. The **Group Information** panel for the group consists of default data set for group.
3. The **Group Information** tab is selected by default.

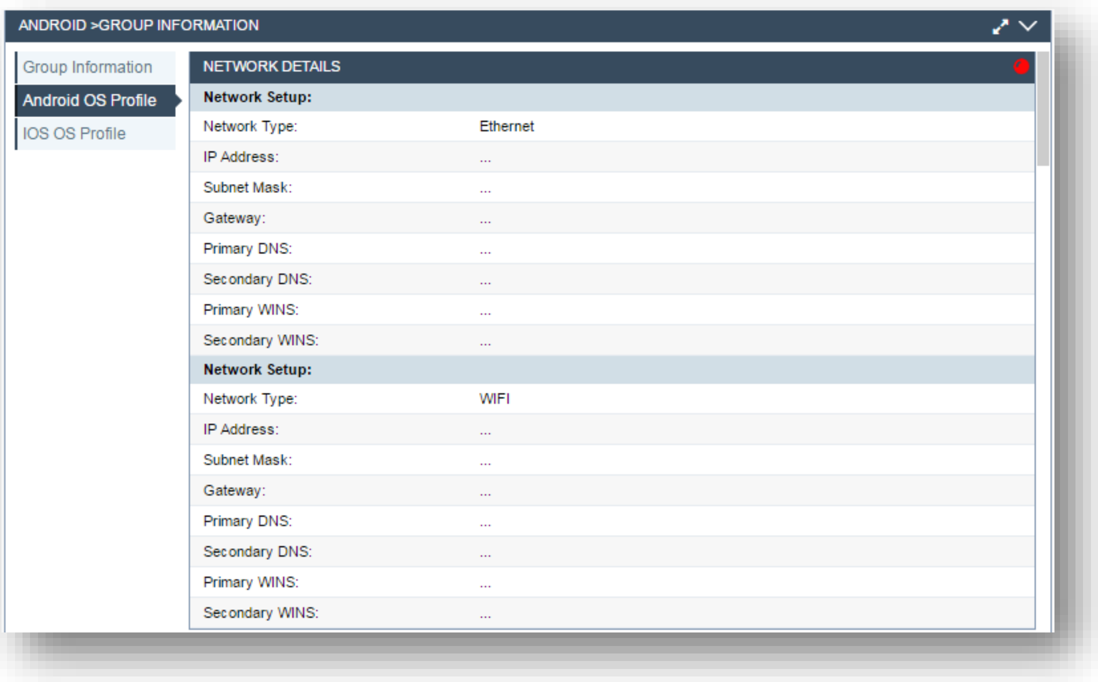
- To view the iOS or Android operating system profile, click on respective Profile tab open
- Default group Information displayed on group information tab
- Group Type, Total devices, policy count, pending task, Total off device etc.



GROUP INFORMATION

Group Type:	Custom	Pending Task(s):	0
No of Subgroup(s):	0	In-process Task(s):	0
Total Device(s):	2	Closed Task(s):	17
Total ON Device(s):	0	VNC Password	-
Total OFF Device(s)	2	Repository Connection:	FDM_HTTP
Domain Name:	-		
Compliance Count:	1	Not Compliance Count:	0
Policy Applied Count:	2		

- In OS type (Android/iOS) tab default module settings displayed.
- Default and applied settings displayed in green and red indicator for all OS.

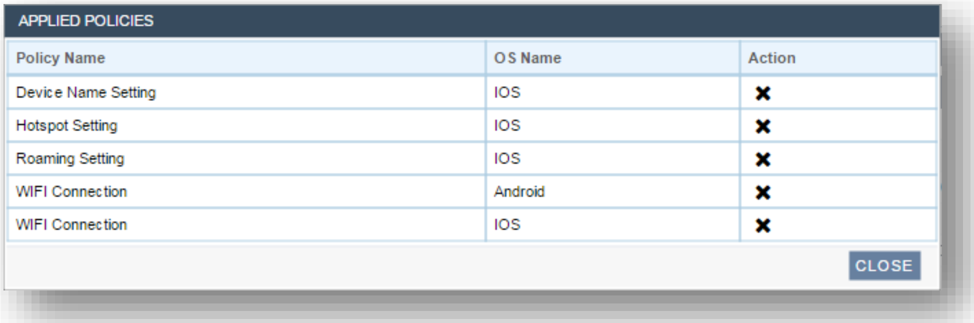


NETWORK DETAILS

Network Setup:	
Network Type:	Ethernet
IP Address:	...
Subnet Mask:	...
Gateway:	...
Primary DNS:	...
Secondary DNS:	...
Primary WINS:	...
Secondary WINS:	...
Network Setup:	
Network Type:	WIFI
IP Address:	...
Subnet Mask:	...
Gateway:	...
Primary DNS:	...
Secondary DNS:	...
Primary WINS:	...
Secondary WINS:	...

Group Information: Policy Count

1. Settings applied on group, number of settings get displayed on policy count.
2. Click on Policy count, applied policy popup displayed.



APPLIED POLICIES

Policy Name	OS Name	Action
Device Name Setting	IOS	✖
Hotspot Setting	IOS	✖
Roaming Setting	IOS	✖
WIFI Connection	Android	✖
WIFI Connection	IOS	✖

3. Click on Delete button to cancel Action performed on group.
4. Click on Close to close popup.

Pending Task Activity Details

Tasks awaiting completion are listed in **Pending Task Activity Details**.

> For information on pending tasks , see the "Monitoring Tasks" in “Working with the Task Manager in Android”.

Toolbar

Icons on the toolbar enable you to navigate to other pages within Fusion EMM , check for notifications and to log out of Fusion EMM .

Icon	Description
⌂	Device Manager
☰	Menu Hide/Open
🔍	Discovery
🖥	Task Management

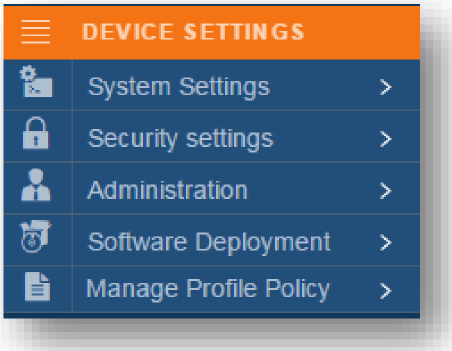
▦	Asset Management
📋	Reports and Audit Logs
⚙	Configuration Setup
⏻	Log out
🖵	VNC Notifications
⤢	Maximize screen
⌄	Expand Screen
⤡	Minimize screen
⌃	Collapse Screen
▼	Advanced Filter

Right Menu

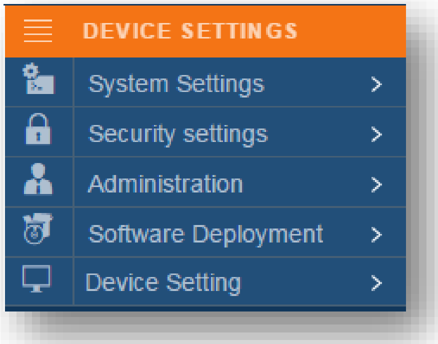
The menu on the right side of the home page enables you to access all functions of the device configuration modules.

Depending on the hierarchy level selected in the devices tree, the right menu displays various functions.

- Right menu of devices tree for Android:

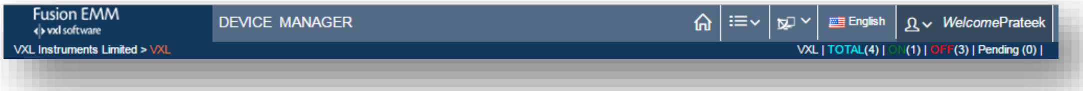


- Right menu of devices tree for iOS:



InfoBar

The Info Bar displays a summary of the devices.


Fusion EMM
vxl software
DEVICE MANAGER
English
WelcomePrateek
VXL Instruments Limited > VXL
VXL | TOTAL(4) | ON(1) | OFF(3) | Pending (0) |

Details displayed in the Info Bar include:

- Company Name
- Site Name
- Group name
- Total number of devices in the group

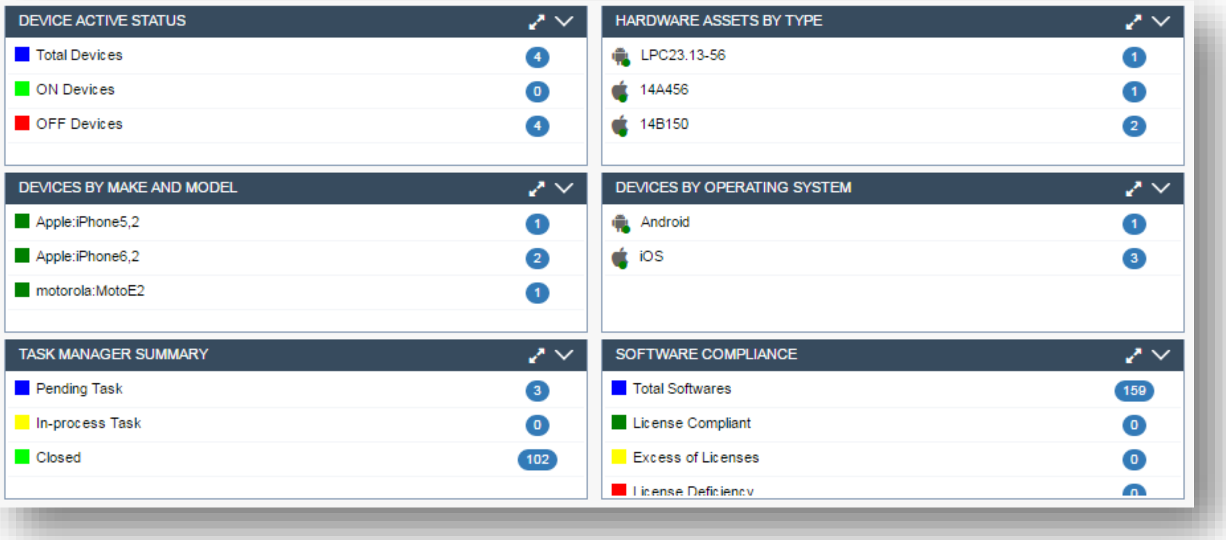
- Devices with an ON status
- Devices with an OFF status
- Schedules pending execution
- Group settings: Custom, IP, Domain group or Subnet.

Understanding the Dashboard

The dashboard provides a graphical overview of Fusion EMM such as status of tasks, devices by operating system and software installed on the devices and status of the monitored devices.

To view the dashboard

- On the right menu, click **Dashboard**.



DEVICE ACTIVE STATUS

🟦 Total Devices	4
🟩 ON Devices	0
🟥 OFF Devices	4

HARDWARE ASSETS BY TYPE

LPC23.13-56	1
14A456	1
14B150	2

DEVICES BY MAKE AND MODEL

🟩 Apple:iPhone5,2	1
🟩 Apple:iPhone6,2	2
🟩 motorola:MotoE2	1

DEVICES BY OPERATING SYSTEM

Android	1
iOS	3

TASK MANAGER SUMMARY

🟦 Pending Task	3
🟨 In-process Task	0
🟩 Closed	102

SOFTWARE COMPLIANCE

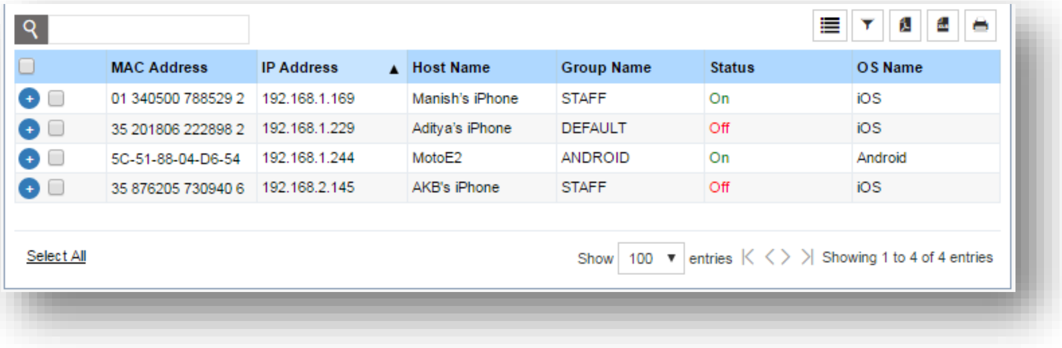
🟦 Total Softwares	159
🟩 License Compliant	0
🟨 Excess of Licenses	0
🟥 License Deficiency	0

To view details of any displayed parameter displayed on the dashboard, click the number against the required parameter.

Understanding Common Operations

Some operations are common across Fusion EMM . This section describes these commonly used operations.

Showing or Hiding Table Columns

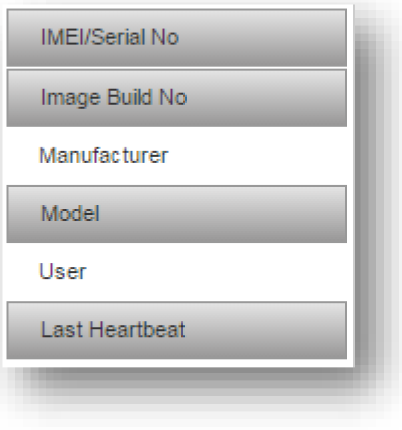


□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All

Show 100 ▼ entries |< < > >| Showing 1 to 4 of 4 entries

1. In the area above the table, click ☰.
2. The list of columns as shown in the example below is display.



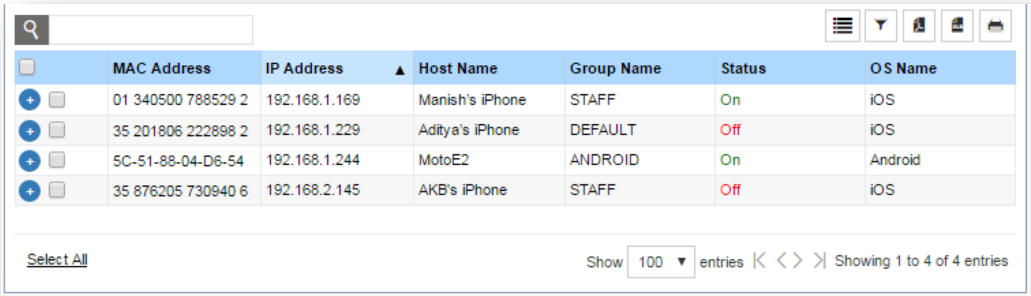
3. Select or clear the check boxes to show or hide columns as required.

Configuring Filters

You can add filters to select the details to view from a table. You can also edit or delete the filters added.

Device Manager search filter are now saved user wise.

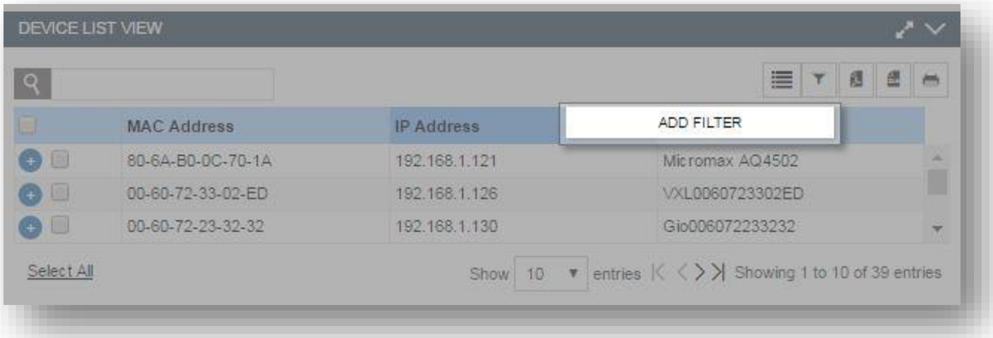
Adding a Filter



MAC Address	IP Address	Host Name	Group Name	Status	OS Name
01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All   Show 100 entries   Showing 1 to 4 of 4 entries

1. In the area above the table, click ▼.
2. The **Add Filter** button is display.



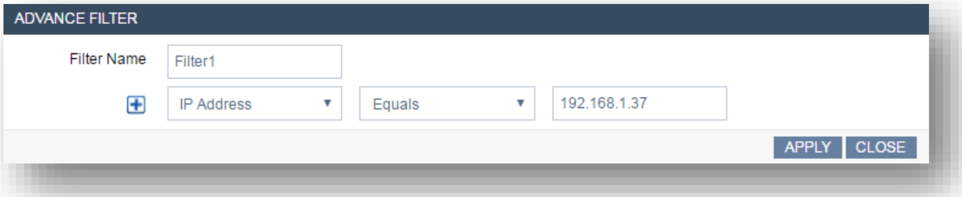
DEVICE LIST VIEW

ADD FILTER

MAC Address	IP Address	
80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
00-60-72-33-02-ED	192.168.1.126	VXL0060723302ED
00-60-72-23-32-32	192.168.1.130	Gio006072233232

Select All   Show 10 entries   Showing 1 to 10 of 39 entries

3. Click **Add Filter**.
4. The **Advance Filter** dialog box is display.



ADVANCE FILTER

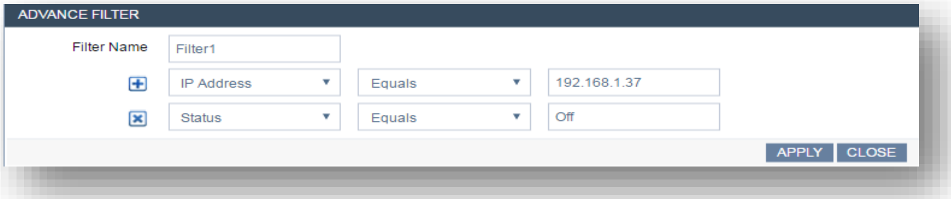
Filter Name: Filter1

IP Address ▾   Equals ▾   192.168.1.37

APPLY   CLOSE

5. In **Filter Name**, enter a name for the filter.
6. In the **Column Name** list, select the required column.

7. In the **Condition** list, select the required filtering condition.
8. The text box to enter the filter parameter is display.
9. Enter the required parameter.
10. You can add additional filter criteria.
11. To add a filter criterion, click ⊞

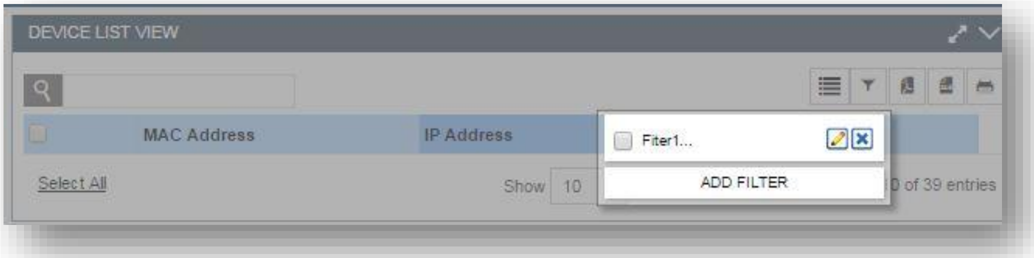


ADVANCE FILTER

Filter Name	Filter1		
⊞	IP Address ▾	Equals ▾	192.168.1.37
☒	Status ▾	Equals ▾	Off

APPLY CLOSE

12. Enter details for the criterion added.
13. Click **Apply**.
14. To view the newly added filter, click ▼.
15. The added filter is display.



DEVICE LIST VIEW

☐	MAC Address	IP Address

☐ Fiter1...

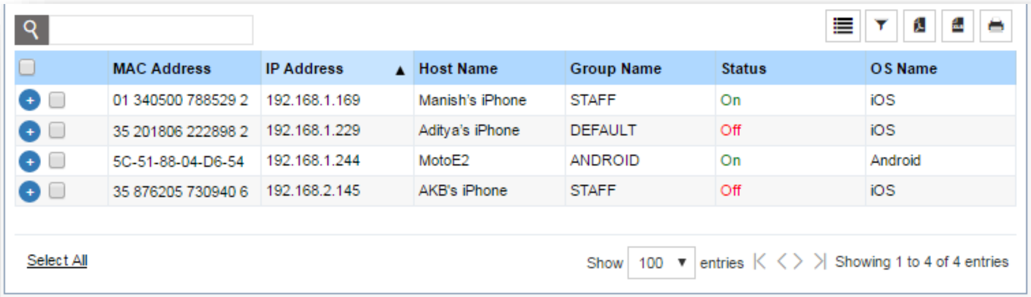
ADD FILTER

Select All

Show 10

0 of 39 entries

Editing a Filter



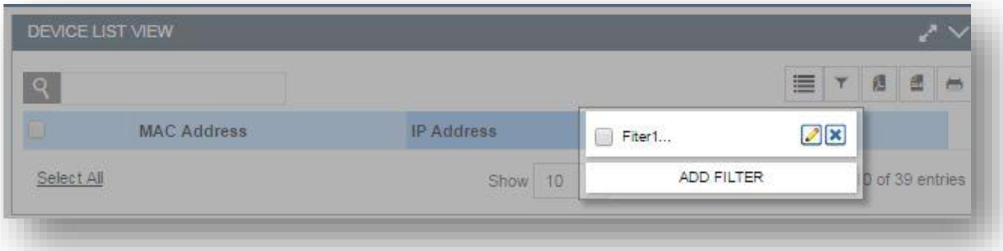
	☐	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+	☐	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+	☐	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+	☐	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+	☐	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All

Show 100 ▾ entries

Showing 1 to 4 of 4 entries

1. In the area above the table, click ▼.
2. The filter(s) are displayed.



DEVICE LIST VIEW

□	MAC Address	IP Address

□ Fiter1... ✎ ☒

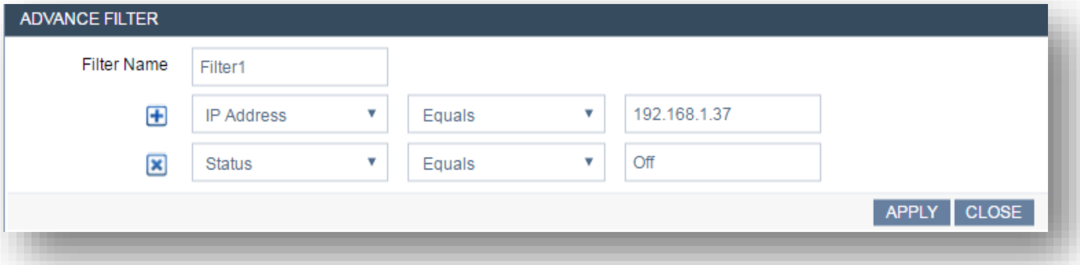
ADD FILTER

Select All

Show 10

0 of 39 entries

3. Click the edit button ✎ for the filter to edit.



ADVANCE FILTER

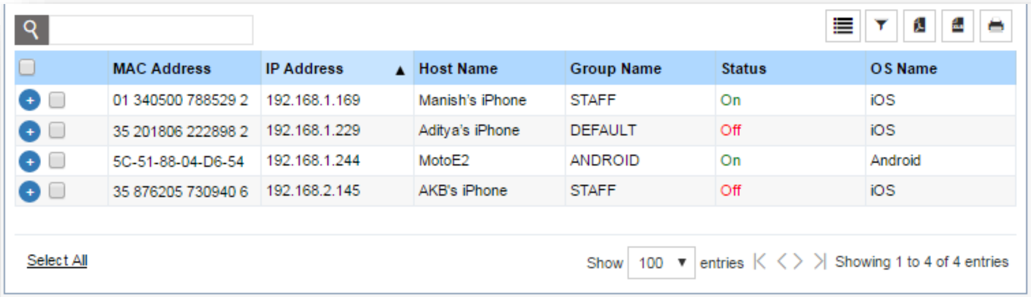
Filter Name: Filter1

⊞	IP Address	Equals	192.168.1.37
☒	Status	Equals	Off

APPLY CLOSE

4. In **Advance Filter**, change the filter details as required.
5. Click **Apply**.

Deleting a Filter

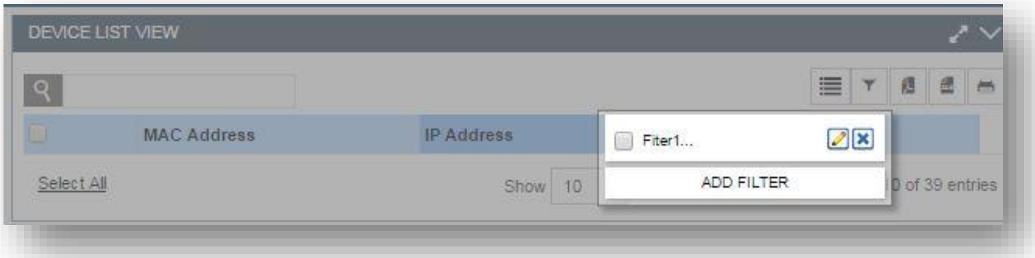


□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All

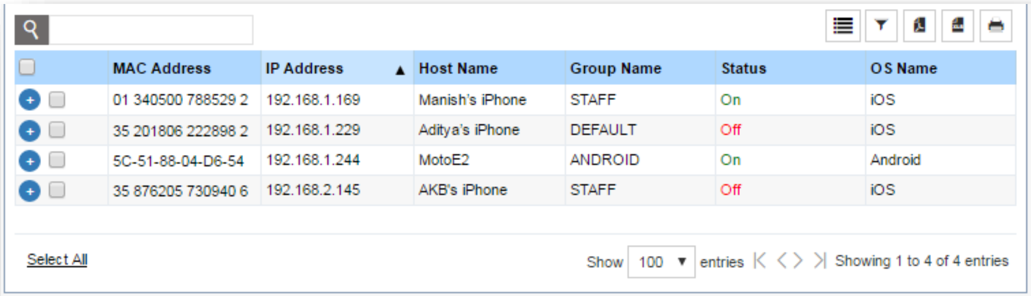
Show 100 ▼ entries |< < > >| Showing 1 to 4 of 4 entries

1. In the area above the table, click ▼.
2. The filter(s) are displayed.



3. To delete a filter, click the delete button ☒.

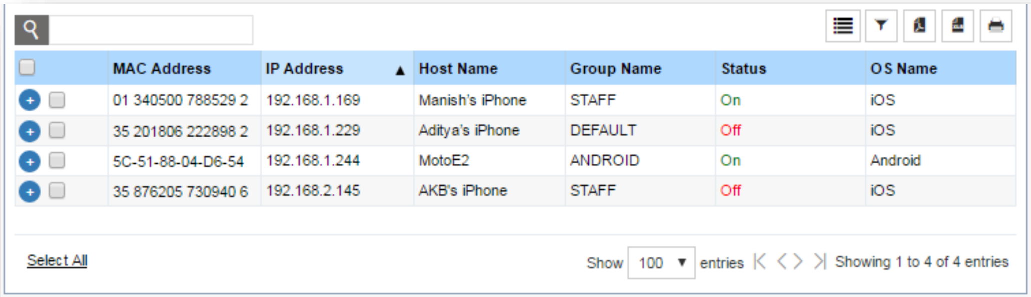
Exporting Data to PDF



□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

1. To export data in pdf format, click button.
2. Open or save the file.

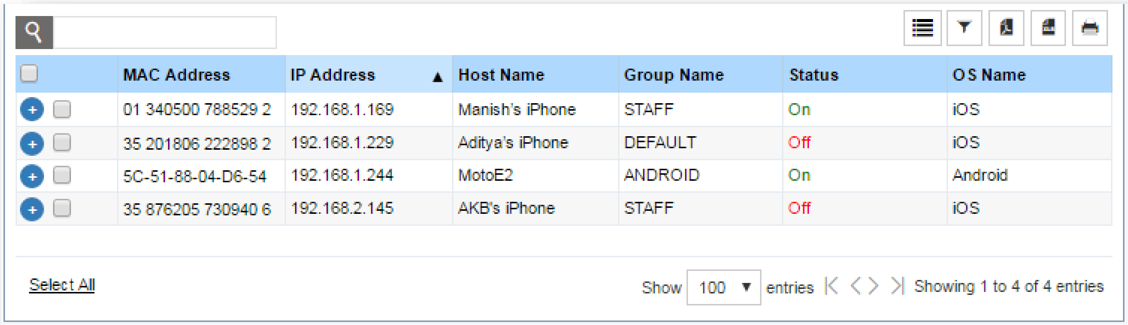
Exporting Data to Excel



□	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

1. To export data in excel format, click button.
2. Open or save the file.

Printing Displayed Details



	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	01 340500 788529 2	192.168.1.169	Manish's iPhone	STAFF	On	iOS
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	DEFAULT	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	ANDROID	On	Android
+ □	35 876205 730940 6	192.168.2.145	AKB's iPhone	STAFF	Off	iOS

Select All

Show 100 entries

Showing 1 to 4 of 4 entries

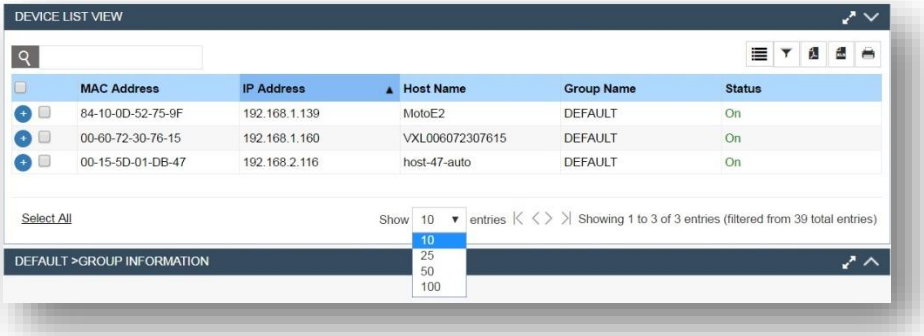
1. In the area above the table, click 🖨 to print displayed data.

Customizing the Table View

You can select the number of entries to display in a table.

To select the number of entries to display

- In the drop-down list below the table, select the required number of entries.
- To navigate through the displayed list of entries, click the arrows.



DEVICE LIST VIEW

	MAC Address	IP Address ▲	Host Name	Group Name	Status
+ □	84-10-0D-52-75-9F	192.168.1.139	MotoE2	DEFAULT	On
+ □	00-60-72-30-76-15	192.168.1.160	VXL006072307615	DEFAULT	On
+ □	00-15-5D-01-DB-47	192.168.2.116	host-47-auto	DEFAULT	On

Select All

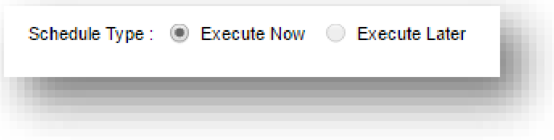
Show 10 entries

Showing 1 to 3 of 3 entries (filtered from 39 total entries)

Scheduling Tasks

You can execute tasks immediately or schedule them for execution later.

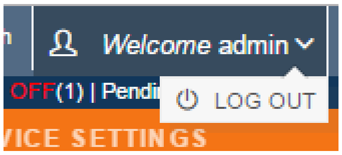
- To execute tasks immediately, select the **Execute Now** schedule type.
- To execute tasks later, select the **Execute Later** schedule type.
- Execute later functionality not applicable for iOS device.



Schedule Type : ● Execute Now ○ Execute Later

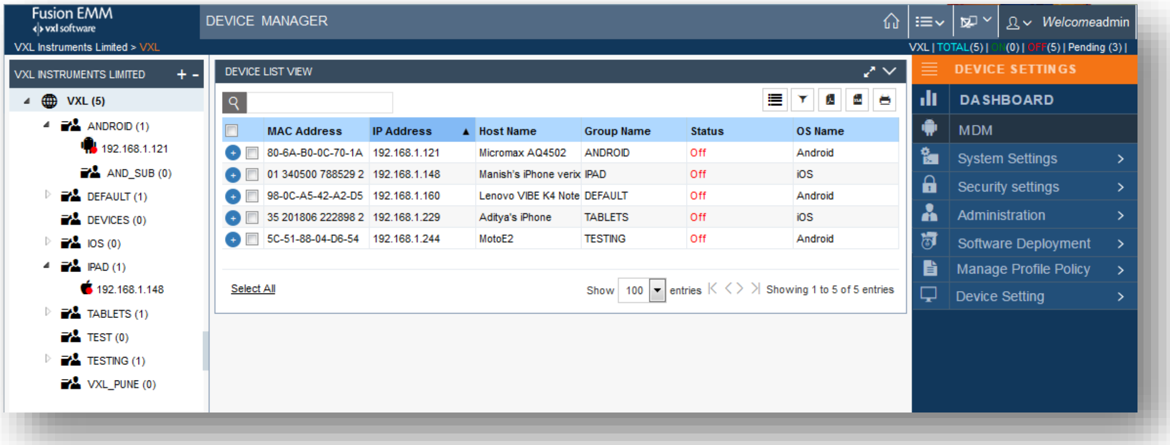
Logout from Fusion EMM

- On the tool bar, click the LogOut button under the username.



Working with the Devices Tree

The left pane of the **Device Manager** or home page is the devices tree. It displays devices registered in Fusion EMM at the group level and at the device or terminal node level.



	MAC Address	IP Address ▲	Host Name	Group Name	Status	OS Name
+ □	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502	ANDROID	Off	Android
+ □	01 340500 788529 2	192.168.1.148	Manish's iPhone verix	IPAD	Off	iOS
+ □	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	Off	Android
+ □	35 201806 222898 2	192.168.1.229	Aditya's iPhone	TABLETS	Off	iOS
+ □	5C-51-88-04-D6-54	192.168.1.244	MotoE2	TESTING	Off	Android

Select All

Show 100 entries

Showing 1 to 5 of 5 entries

The devices tree enables you to manage groups and configure their settings. Settings applied to a group are applied by default to all devices within the group.

Although the devices tree is not limited in size and can contain any number of hierarchical levels, adding too many levels can make the system unmanageable.

The devices tree displays the following hierarchy:

1. Company
2. Site
3. Group
4. Devices or Terminal Nodes

In the example, the hierarchy is display as:

1. VXL Instruments Limited (company)
2. VXL (site)
3. Default (group)
4. 100.97.62.163, 192.168.0.102, etc. (devices or terminal nodes)

The company name is display at the highest level of the devices tree. The company site name displays below the company name.

The default group is placed below the site name. When devices are discovered and enrolled for management in Fusion EMM, they are automatically registered into the default group. You can create other groups, in addition to the default group, under a site.

You can also add subgroups to a group. The subgroups added are listed under the group in the devices tree.

You can add client devices to a group or to a subgroup. The devices are listed under the respective group or subgroup.

> To move a device from one group to another, drag the device to the destination group.

The symbols and colors displayed against the devices in the tree view indicate various operating systems and status of the devices.

Symbol	Description
🟢	Device is ON.
🔴	Device is OFF.
🤖	The device uses a Android operating system.
🍎	The device uses an iOS operating system.

In the devices tree, you can add, edit or delete groups and subgroups; and configure their settings.

Adding a Group

You can add groups at the site node of the devices tree.

1. To add a group
2. In the devices tree, right-click the site node.
3. Click **Add Group**.
4. Enter a name for the new group.

The new group cannot have the same name as an existing group. For example, if you try to create a group with the existing group name then it will give error as “Group already exists.”

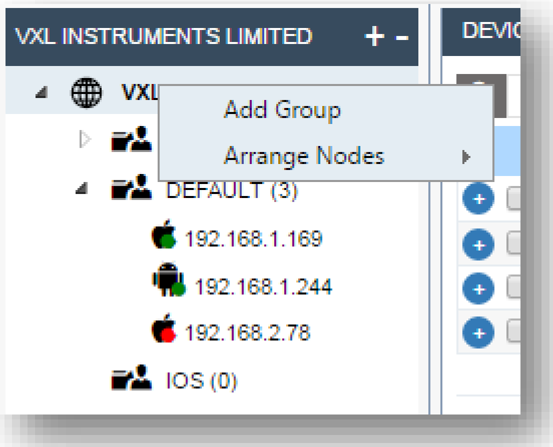
Working with the Node View

You can view devices in the devices tree by IP address, MAC address or host name.

To select the devices, display view

1. In the devices tree, right-click the site node.
2. Select **Arrange Nodes**.
3. Select **IP Address**, **MAC Address** or **Host Name** as required.

The group nodes in the devices tree are arranged based on this selection. For example, if you select the **IP Address** option the nodes are displayed according to their IP addresses.



Similarly, if you select **MAC Address** or **Host Name**, the nodes are displayed accordingly.

Context Menu

While some group settings can be configured before devices are registered in Fusion EMM , some settings must be done after the registration of devices.

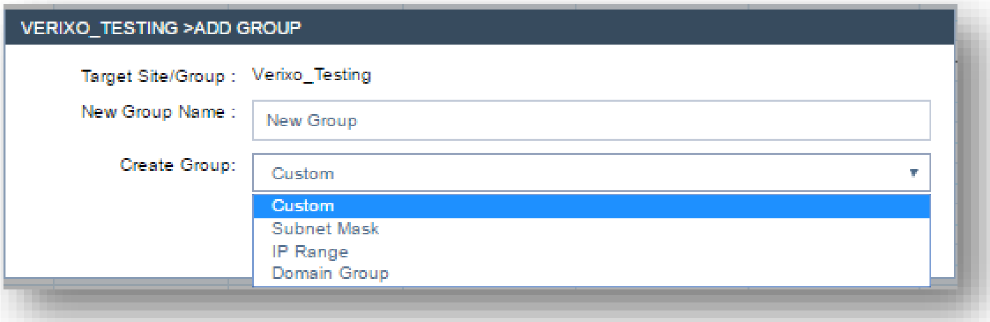
Working with Groups Before Device Registration

Configuring Group Settings

The administrator can set the subnet or range of IP addresses to list in a group. When registered, the devices will be automatically assigned to the group.

To manage group settings

1. In the devices tree, right-click the **Site Node**.
2. Click **Add Group**.
3. In **Add Group**, in **Create Group by**, select **Custom**, **Subnet, Domain or IP Range.**



VERIXO_TESTING >ADD GROUP

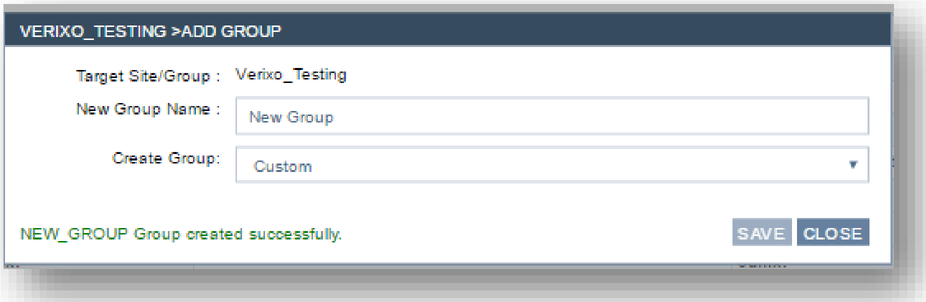
Target Site/Group : Verixo_Testing

New Group Name : New Group

Create Group: Custom

Creating Group with Custom Settings

Any device, irrespective of its IP range or Subnet, can be registered under this group.



VERIXO_TESTING >ADD GROUP

Target Site/Group : Verixo_Testing

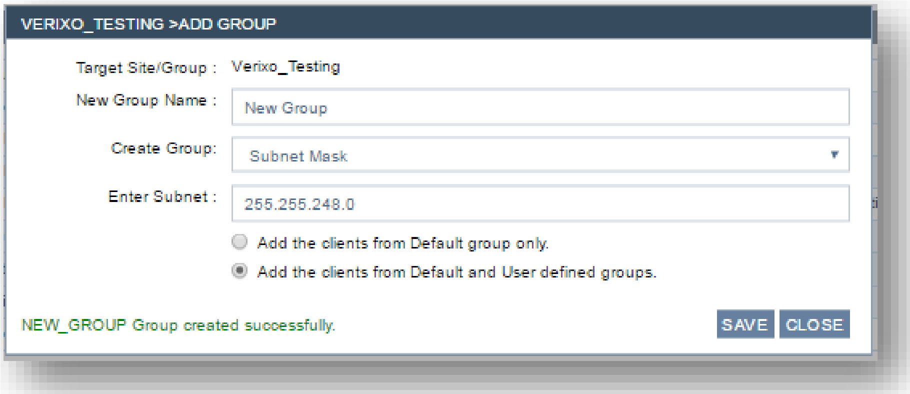
New Group Name : New Group

Create Group: Custom

NEW_GROUP Group created successfully.

Creating Group by Subnet

Devices that belong to a subnet can be registered under one group.



VERIXO_TESTING >ADD GROUP

Target Site/Group : Verixo_Testing

New Group Name : New Group

Create Group: Subnet Mask

Enter Subnet : 255.255.248.0

○ Add the clients from Default group only.

● Add the clients from Default and User defined groups.

NEW_GROUP Group created successfully.

To create a group by subnet

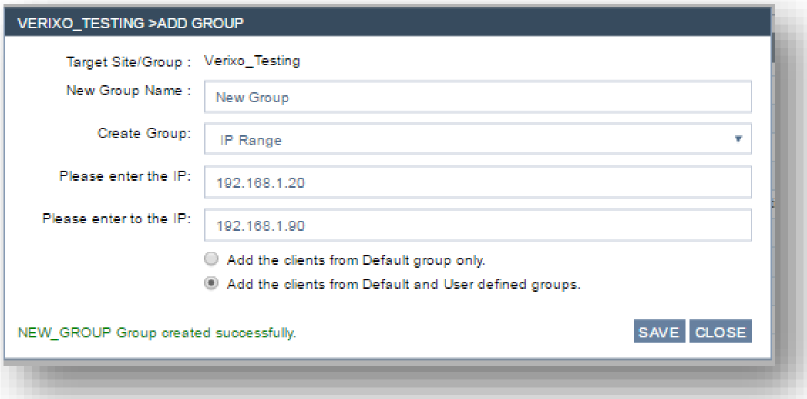
1. In **Enter Subnet** textbox, enter the subnet.
2. Select **Add the clients from Default group only** or **Add the clients from Default and User defined groups**.
    a. If you select the **Add the clients from Default group only** option, then only devices which is present in the default group and matches the subnet criteria will be added into this group.
    b. If you select the **Add the clients from Default and User defined groups** option, all the devices which is present on the server and matches the subnet criteria will be moved into this group.
3. Click **Save.**

The **Saved successfully** message is display.

Creating Group by IP Range

When you create a group by IP range, devices with IP addresses that fall within the specified range are listed under this group.

To create a group by IP range



VERIXO_TESTING >ADD GROUP

Target Site/Group : Verixo_Testing

New Group Name : New Group

Create Group: IP Range

Please enter the IP: 192.168.1.20

Please enter to the IP: 192.168.1.90

○ Add the clients from Default group only.

● Add the clients from Default and User defined groups.

NEW_GROUP Group created successfully.

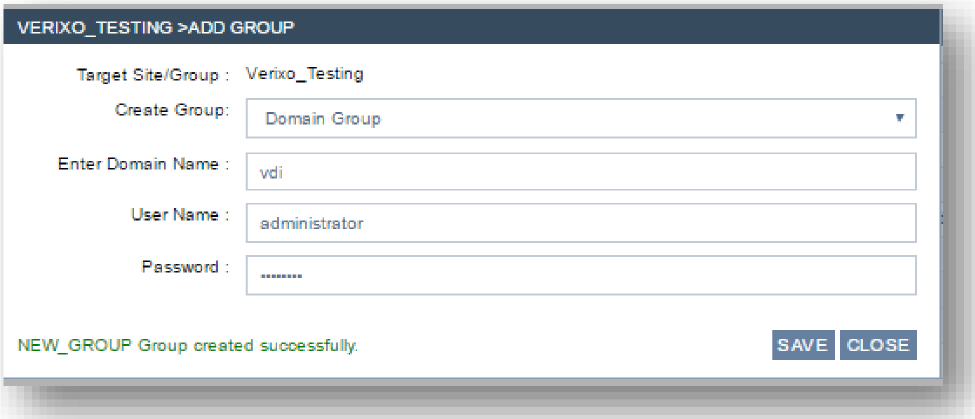
1. In **Enter from IP** and **Enter to IP** textbox, enter the required IP range.
2. Select **Add the clients from Default group only** or **Add the clients from Default and User defined groups.**
3. Click **Save**.

   The **Saved successfully** message is display.

Creating Group by Domain group

1. In **Enter Domain name.**
2. Enter credentials of domain server.
3. Click **Save**.

   The **Saved successfully** message is display.



VERIXO_TESTING >ADD GROUP

Target Site/Group : Verixo_Testing

Create Group: Domain Group

Enter Domain Name : vdi

User Name : administrator

Password : ••••••••

NEW_GROUP Group created successfully.

- In the subnet group, only the sub group with type as IP-Range can be added.
- In the IP range group, only the sub group with type as IP range can be added.
- In the Domain group, only the sub group with type as Custom can be added.

Adding a Subgroup

- You can organize the devices listed in a group into various subgroups.
- On adding any subgroup then all the settings of the parent group get inherited to the added subgroup.

To add a subgroup

1. In the devices tree, right-click the group node.
2. In **Group Management**, click **Add Subgroup**.
3. Enter a name for the new subgroup.

Editing a Group

You can edit a group name as well as the group type.

To edit a group

1. In the devices tree, right-click the group node.
2. In **Group Management**, click **Edit Group**.
3. Edit the group name.

Group Edit Policy

1. Group with type IP Range can be edited and converted to type Custom, Subnet or Domain Group.
2. Group with type as Subnet can be edited and converted to type as Custom, IP Range or Domain Group.
3. Group with type as Domain Group can be edited and converted to type as only custom.

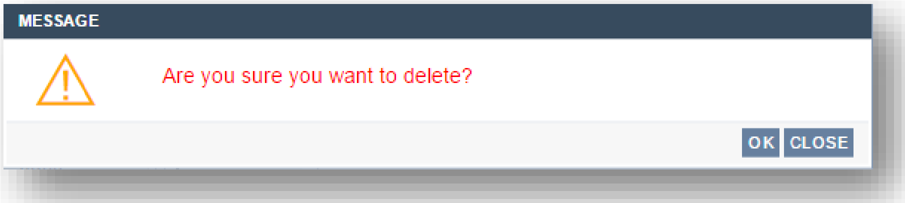
Based on the conversion, the devices will gets moved to their respective group if they fall within the defined condition of any group present in the tree if not they will get moved to default group.

Deleting a Group

1. In the devices tree, right-click the group node.
2. In **Group Management**, click **Delete Group**.

   Are you sure you want to delete?

   Prompts display.



MESSAGE

Are you sure you want to delete?

3. Click **OK**.

A group cannot be deleted if it is in use.

Working with Groups After Device Registration

Some group settings can be configured when devices are registered in Fusion EMM and listed under the group node.

With device user can able to access some common features as without device listed below: -

- Edit Group
- Delete Group
- Add Sub Group

Drag-and-Drop Overview

Node Drag Drop:

- Node drag and drop feature control enables users to drag and drop tree nodes.
- Dragging and dropping of nodes can be performed within the same group or between two different groups.
- You can also specify the inheritance operations to be performed based upon the option selected for the client inheritance settings in the general configuration.
- By default, the inheritance setting is “Never”.

Group Drag Drop:

- Group drag and drop feature control enables user to drag and drop group within the tree.
- Dragging and dropping of group can be performed only between groups of type custom.
- When we try to move the group, which is in, use then it show message the group cannot be moved, group in use.
- You can also specify the inheritance operations to be performed based upon the option selected for the group inheritance settings in the general configuration.
- By default, the inheritance setting is “Never”.
- If the group inheritance settings selection is always when we drag drop the group or group along with nodes the settings gets inherited to group as well as nodes present in the group which is being dragged.
- If the group inheritance settings set to Selection, when we drag drop the group with or without devices then it will ask for the confirmation whether the parent group settings need to be inherited to group or to both group as well as devices.
- If the group inheritance settings set to Never, when we drag drop the group it will move the group without inheriting the parent group settings to the groups, which is being moved.

Working with Remote Control

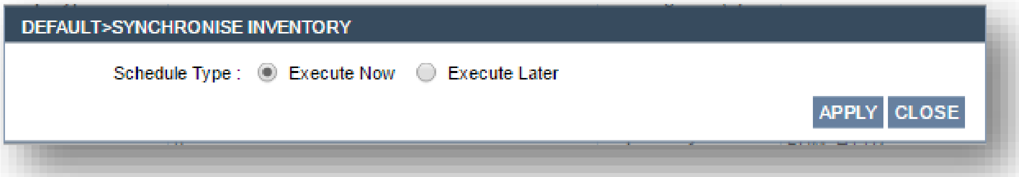
Remote control enables the administrator to remotely control functions such as capturing device data, sending a message in a group.

Synchronizing Inventory

Inventory synchronization enables the administrator to acquire details of all devices in a group.

To synchronize inventory

1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Synchronise Inventory**.



DEFAULT>SYNCHRONISE INVENTORY

Schedule Type : ● Execute Now ○ Execute Later

3. Select the required **Schedule Type**.

4. Click **Apply**.

The **Request for settings update processed** message is display.

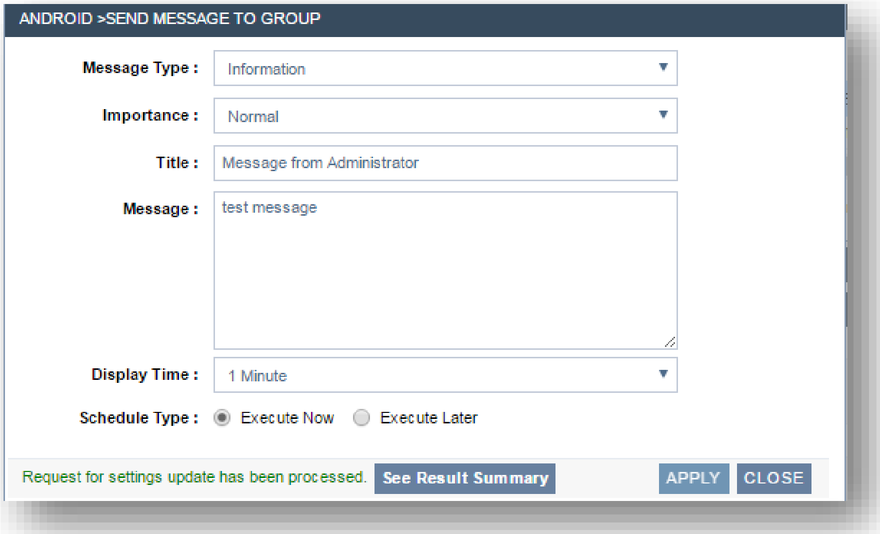
Sending Messages to Devices

You can send messages to all devices in a group at the same time.

To send messages to all devices

1. In the devices tree, right-click the group node.

2. In **Remote Control**, select **Send Message All**.



ANDROID >SEND MESSAGE TO GROUP

Message Type : Information

Importance : Normal

Title : Message from Administrator

Message : test message

Display Time : 1 Minute

Schedule Type : ● Execute Now ○ Execute Later

Request for settings update has been processed.

3. Enter the required details.

4. Click **Apply**.

The **Request for settings update processed** message is display.

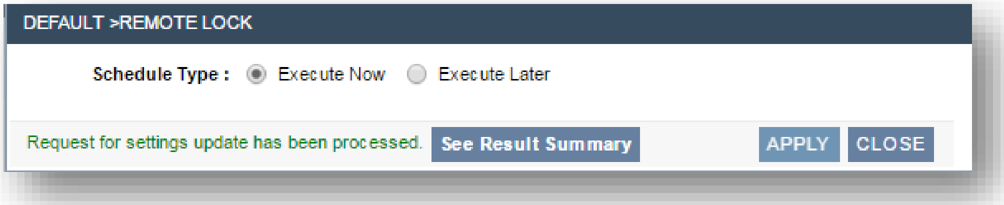
Locking Devices

You can lock all the devices in a group.

To lock the devices

1. In the devices tree, right-click the group node.

2. In **Remote Control**, select **Lock Computer All**.



Request for settings update has been processed.

3. Select the required **Schedule Type**.
4. Click **Apply**.

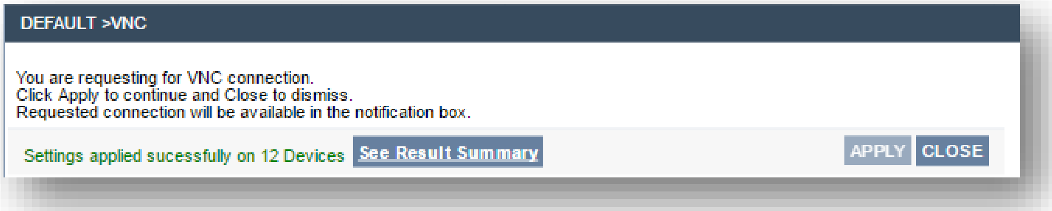
   The **Request for settings update processed** message is display.

Applying Shadowing VNC

In shadowing VNC, Fusion EMM sends an instruction to the device that it needs to VNC. Two secure channels are then created by the device and administrator's browsers to the Fusion EMM server. The channels are then combined to provide the VNC access. An administrator can open multiple secure channels.

To apply shadow VNC

1. In the devices tree, right-click the group node.
2. In **Shadowing**, select **VNC**.
3. In the **VNC** dialog box, click **Apply**.



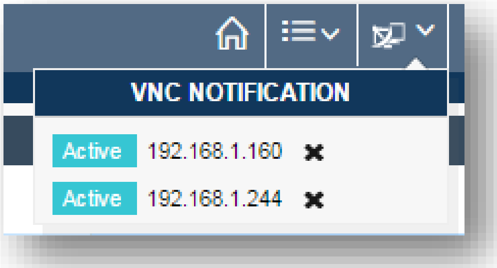
You are requesting for VNC connection.
Click Apply to continue and Close to dismiss.
Requested connection will be available in the notification box.

Settings applied sucessfully on 12 Devices

If the settings are successfully applied to a device, it implies that that the device is connected to the network.

💡	User should have resolved the browser error by installing the certificate. VNC password should be set on group. Shadowing VNC only applicable for Android.

4. After applying setting, IP address of that client will get list out in VNC Notification .
5. After task applied successfully status on VNC notification changes from Pending to Active state.
6. If click on cancel button, then setting goes failed with reason “User permission denied” and client IP address gets removed automatically from VNC notification list.



VNC NOTIFICATION

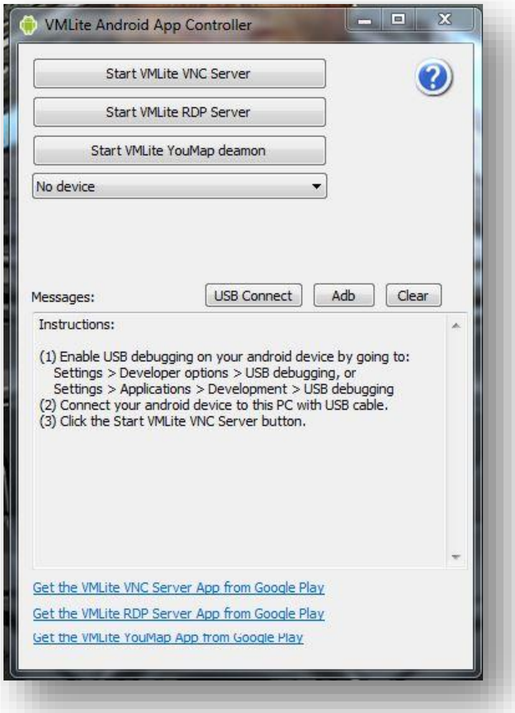
Active 192.168.1.160 ✖

Active 192.168.1.244 ✖

To access the VNC of a device, in **VNC Notifications**, click its IP address and proceed to provide remote assistance.

Before applying shadowing VNC, user have to install VMLite & keep proper setup as per given below:

1. Install ‘VMLite VNC Server’ on device from Play Store by using Google account (Find app in to MyApp list -> Purchased App).
2. After installation is complete, open VMLite VNC Server app -> Go to Settings icon (Gear icon on top) -> Change VNC port value 5901 to 5900.
3. Install "VMLite Android App Controller" software on any Windows system. (This will help to start VMLite VNC Server for selected device.)
4. Connect the Android device via USB to Windows system where "VMLite Android App Controller" is installed.



Instructions:

(1) Enable USB debugging on your android device by going to:
Settings > Developer options > USB debugging, or
Settings > Applications > Development > USB debugging
(2) Connect your android device to this PC with USB cable.
(3) Click the Start VMLite VNC Server button.

Get the VMLite VNC Server App from Google Play
Get the VMLite RDP Server App from Google Play
Get the VMLite YouMap App from Google Play

5. Follow on-screen instructions shown on VMLite Android App Controller software:

(a) Enable USB debugging on your Android device by going to:

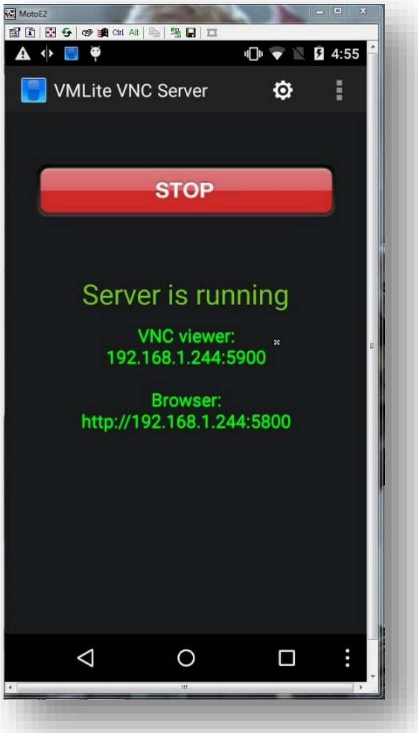
Settings > Developer options > USB debugging or

Settings > Applications > Development > USB debugging

(b) Connect your Android device to this PC with USB cable.

(c) Click the ‘Start VMLite VNC Server’ button.

6. On successful configuration, on device “Server is running" message is shown.



Server is running

VNC viewer:
192.168.1.244:5900

Browser:
http://192.168.1.244:5800

7. After the above message, user can remove the connected Android device from Windows system and can be able to take VNC via VNC viewer or by browser by using the URL provided.

Working with Devices

You can also configure settings for a single device from the devices tree. To access device settings, in the devices tree, right-click the device or terminal node. The configuration settings for a single device are similar to the configuration settings for a group.

At the device level, you can configure settings for the functions mentioned below.

Function	Description
Synchronizing inventory	Sync all data for a device
Sending messages	Send a message to a single client device

Function	Description
Locking the device	Lock a device from the server
Applying shadow VNC	Apply VNC to a device

Please refer to the group configuration settings and similarly configure the device settings.

Configuring Fusion EMM

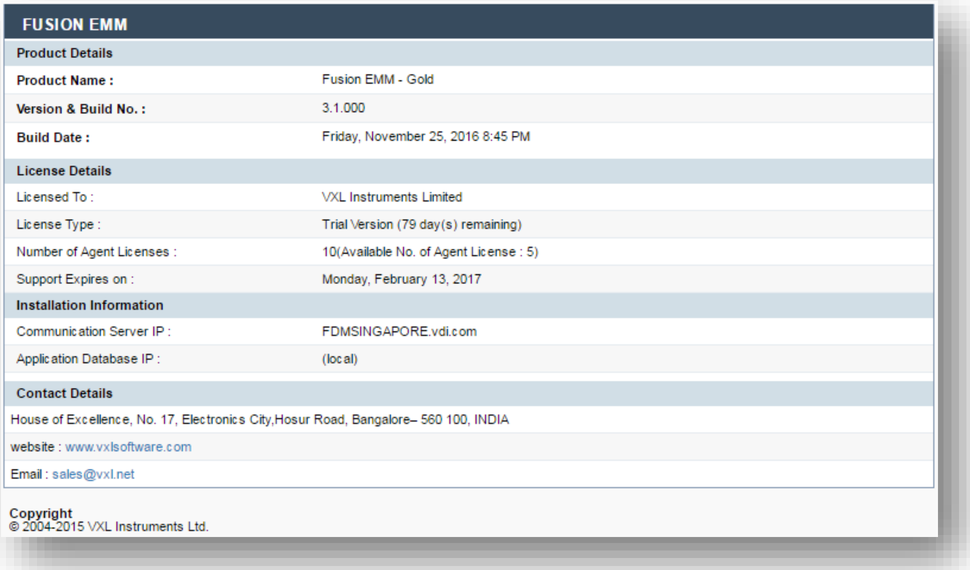
The configuration setup functionality enables you to:

1. Apply the setting and operations performed on an individual client to a group of clients, or to another client.
2. Create a template of the settings, and deploy it across the group or node.

To open the **Configuration Setup** page

1. Click Views ☰ on the toolbar. Select Configuration Setup ⚙

The **Fusion EMM** details are displayed.



FUSION EMM

Product Details	
Product Name :	Fusion EMM - Gold
Version & Build No. :	3.1.000
Build Date :	Friday, November 25, 2016 8:45 PM
License Details	
Licensed To :	VXL Instruments Limited
License Type :	Trial Version (79 day(s) remaining)
Number of Agent Licenses :	10(Available No. of Agent License : 5)
Support Expires on :	Monday, February 13, 2017
Installation Information	
Communication Server IP :	FDMSINGAPORE.vdi.com
Application Database IP :	(local)
Contact Details	
House of Excellence, No. 17, Electronics City,Hosur Road, Bangalore– 560 100, INDIA	
website : www.vxlsoftware.com	
Email : sales@vxl.net	

Copyright
© 2004-2015 VXL Instruments Ltd.

Managing Users

User Management enables you to create and manage organization or customer details, user roles, user group and users in Fusion EMM .

In **User Management**, you can search, create, edit, and delete user related parameters.

Working with a Company Profile

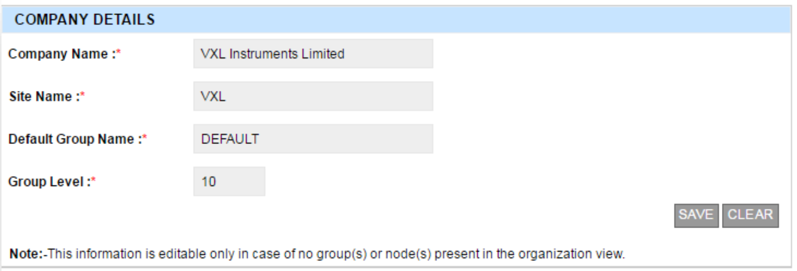
You can configure customer details such as company, site and default group name, and group level. These details display in the devices tree on the **Device Manager** page.

Editing Company Details

User can edit the company details only if no group(s) or node(s) exists in the devices tree. If a new group is created, or a new client is discovered in the server and listed in the devices tree, the option to edit **Company Details** becomes disabled.

To edit the company profile

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **Customer**.
   a. The **Company Details** section is display. It displays the company information entered when logging in to Fusion EMM Server for the first time.



COMPANY DETAILS

Company Name :*	VXL Instruments Limited
Site Name :*	VXL
Default Group Name :*	DEFAULT
Group Level :*	10

Note:-This information is editable only in case of no group(s) or node(s) present in the organization view.

For information about entering company details when you login in to *Fusion EMM* for the first time, see the “Login to Fusion EMM” section in “Getting Started”.

3. Change company details as required.
4. Click **Save.**

Working with User Roles

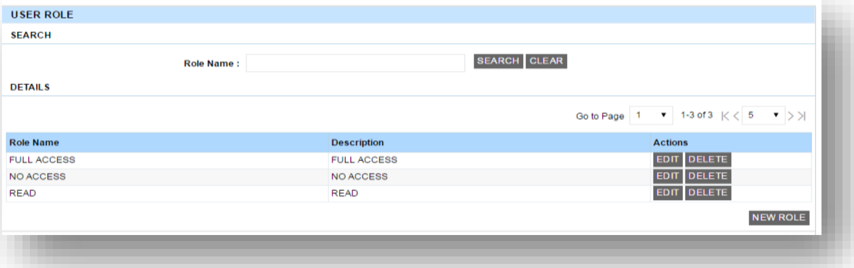
The **User Role** enables you to search, create, modify and delete user roles; and assign access rights to a user.

You can assign a user the following access rights for a particular module:

1. Full Access: user has full access rights to apply settings, and manage or cancel tasks in the application.
2. Read Access: user has the right to only read or view the settings applied.
3. No Access: user has the right to only view the client device or Fusion EMM information. The user has no management rights.

Creating a User Role

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **User Role**.



USER ROLE

SEARCH

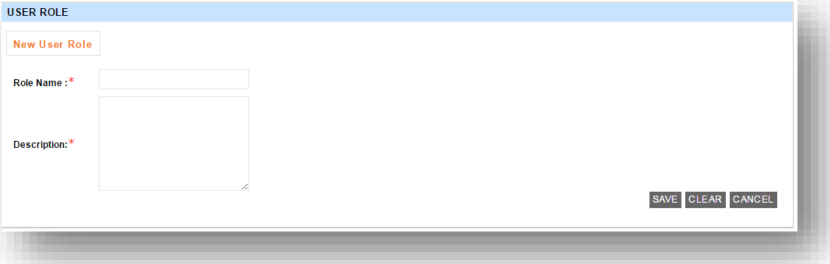
Role Name :

DETAILS

Go to Page 1 ▾ 1-3 of 3 |< < 5 ▾ > >|

Role Name	Description	Actions
FULL ACCESS	FULL ACCESS	EDIT DELETE
NO ACCESS	NO ACCESS	EDIT DELETE
READ	READ	EDIT DELETE

3. Under **Details**, click **New Role**.



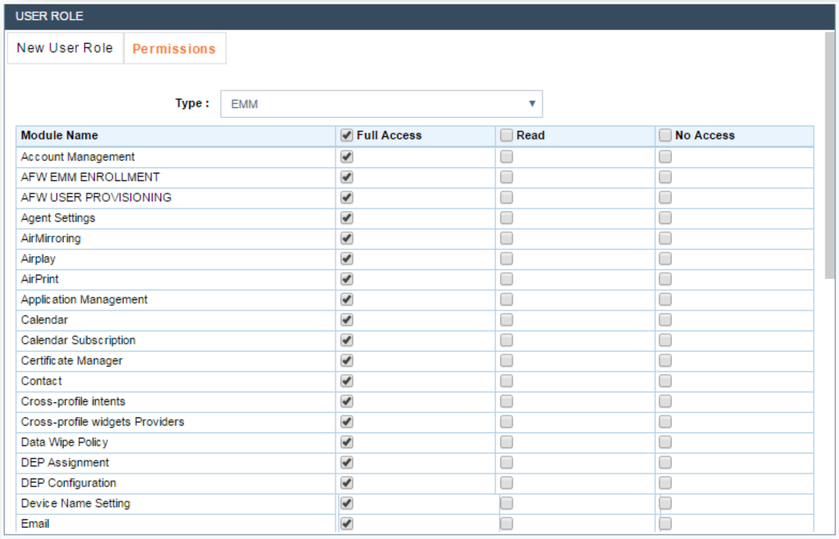
USER ROLE

New User Role

Role Name :*

Description:*

4. On the **New User Role** tab, enter the **Role Name** and **Description**.
5. Click **Save**.



USER ROLE

New User Role | Permissions

Type : EMM ▾

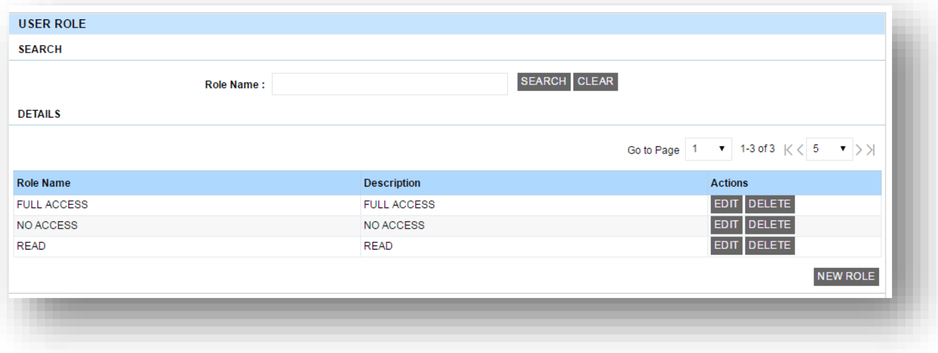
Module Name	☑ Full Access	□ Read	□ No Access
Account Management	☑	□	□
AFW EMM ENROLLMENT	☑	□	□
AFW USER PROVISIONING	☑	□	□
Agent Settings	☑	□	□
AirMirroring	☑	□	□
Airplay	☑	□	□
AirPrint	☑	□	□
Application Management	☑	□	□
Calendar	☑	□	□
Calendar Subscription	☑	□	□
Certificate Manager	☑	□	□
Contact	☑	□	□
Cross-profile intents	☑	□	□
Cross-profile widgets Providers	☑	□	□
Data Wipe Policy	☑	□	□
DEP Assignment	☑	□	□
DEP Configuration	☑	□	□
Device Name Setting	☑	□	□
Email	☑	□	□

6. On the **Permissions** tab, select the applicable check boxes to provide access rights for the module(s) to the user role.
7. Click **Save**

The **Saved successfully** message is display.

Editing a User Role

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **User Role**.



USER ROLE

SEARCH

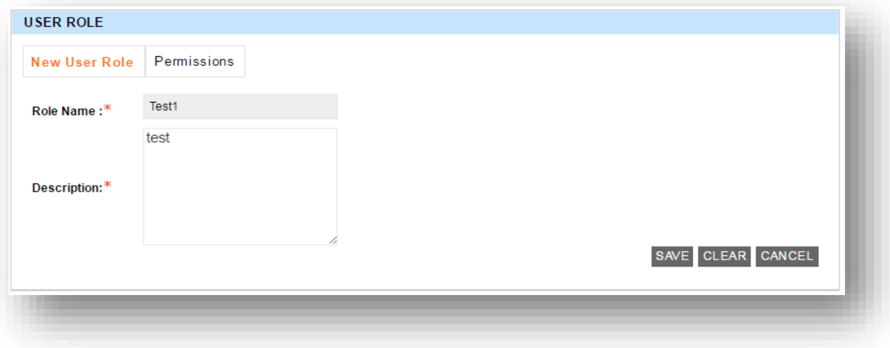
Role Name :

DETAILS

Go to Page 1 ▾ 1-3 of 3 5 ▾

Role Name	Description	Actions
FULL ACCESS	FULL ACCESS	EDIT DELETE
NO ACCESS	NO ACCESS	EDIT DELETE
READ	READ	EDIT DELETE

3. In the **Actions** column, click **Edit** for the user role to edit.

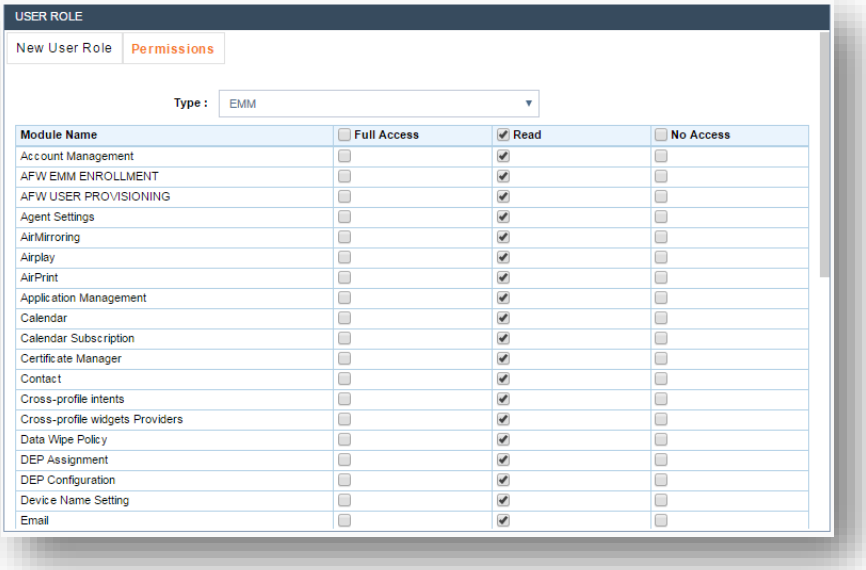


USER ROLE

Role Name :* Test1

Description:* test

4. On the **New User Role** tab, change the user role details as required.
5. Click **Save**.



USER ROLE

New User Role | Permissions

Type : EMM

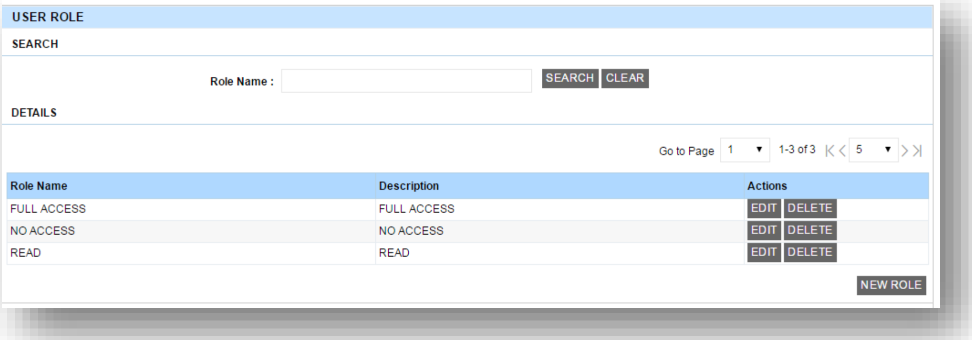
Module Name	☐ Full Access	☑ Read	☐ No Access
Account Management	☐	☑	☐
AFW EMM ENROLLMENT	☐	☑	☐
AFW USER PROVISIONING	☐	☑	☐
Agent Settings	☐	☑	☐
AirMirroring	☐	☑	☐
Airplay	☐	☑	☐
AirPrint	☐	☑	☐
Application Management	☐	☑	☐
Calendar	☐	☑	☐
Calendar Subscription	☐	☑	☐
Certificate Manager	☐	☑	☐
Contact	☐	☑	☐
Cross-profile intents	☐	☑	☐
Cross-profile widgets Providers	☐	☑	☐
Data Wipe Policy	☐	☑	☐
DEP Assignment	☐	☑	☐
DEP Configuration	☐	☑	☐
Device Name Setting	☐	☑	☐
Email	☐	☑	☐

6. On the **Permissions** tab, change the user role details as required.
7. Click **Save**.

The **Saved successfully** message is display.

Deleting a User Role

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **User Role**.



USER ROLE

SEARCH

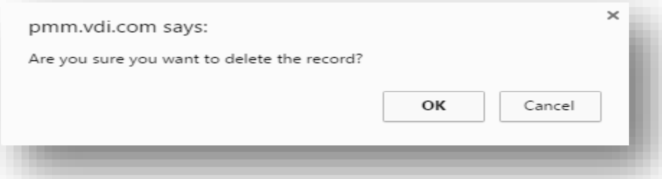
Role Name :

DETAILS

Go to Page 1 ▾ 1-3 of 3 5 ▾

Role Name	Description	Actions
FULL ACCESS	FULL ACCESS	EDIT DELETE
NO ACCESS	NO ACCESS	EDIT DELETE
READ	READ	EDIT DELETE

3. In the **Actions** column, click **Delete** for the user role to delete.
4. **Are you sure you want to delete the record?** Prompt is display.



pmm.vdi.com says:

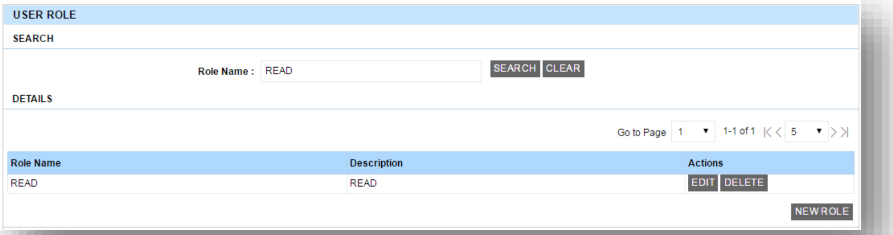
Are you sure you want to delete the record?

5. Click **OK**. The successful user role deletion message is display.

Searching a User Role

1. Expand the right menu.
2. Click**Configuration Setup**, then click **User Management**, and then click **User Role**.
3. In the **Search** section, in **Role name**, enter the role name or description, for example, No Access, Read or Full Access.
4. Click **Search**.

The required role is display.



USER ROLE

SEARCH

Role Name : READ

DETAILS

Go to Page 1 1-1 of 1 5

Role Name	Description	Actions
READ	READ	EDIT DELETE

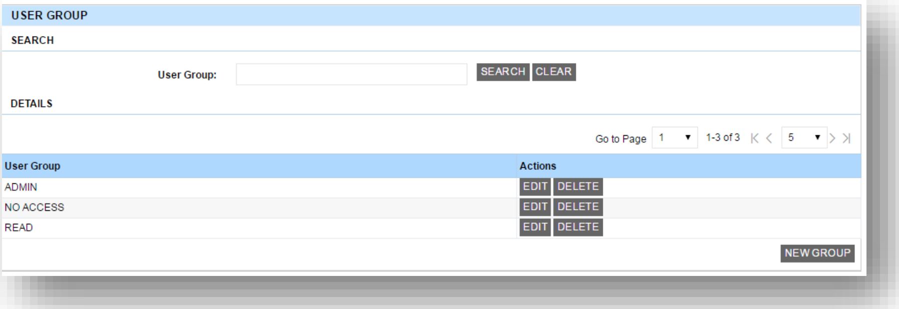
Working with User Groups

The User Group enables you to search, create, edit, and delete user groups, and to assign a user role to the user group.

Creating a User Group

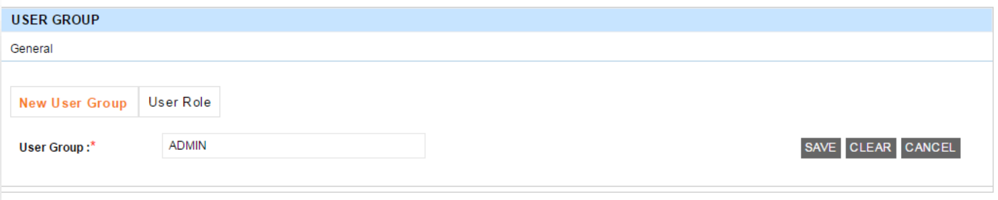
Expand the right menu.

Click Configuration Setup, then click User Management, and then click User Group.



User Group	Actions
ADMIN	EDIT DELETE
NO ACCESS	EDIT DELETE
READ	EDIT DELETE

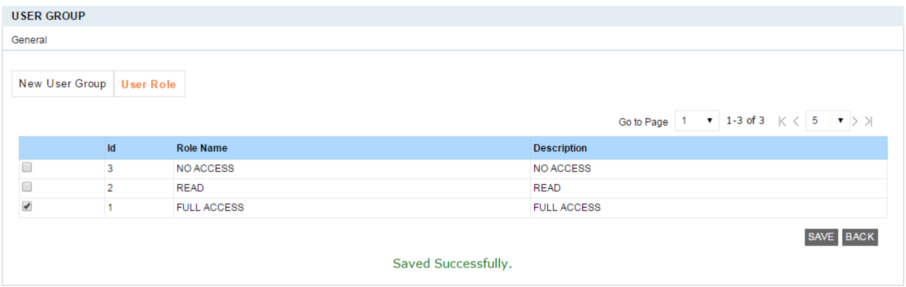
1. Under **Details**, click **New Group**.



User Group :* ADMIN

2. On the **New User Group** tab, enter the user group name.
3. Click **Save**.
4. On the **User Role** tab, in the **Select** column, select the user role(s) to assign to the user group.
5. Click **Save**.

The **Saved successfully** message is display.



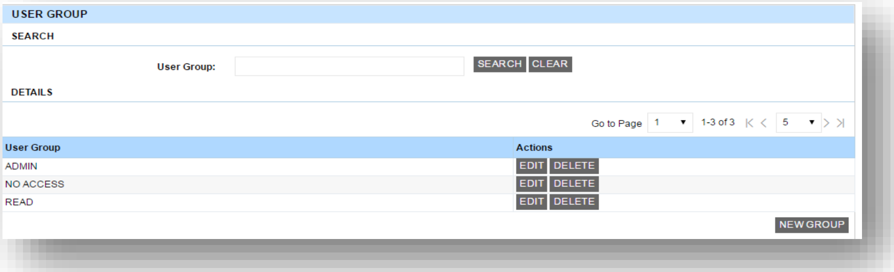
	Id	Role Name	Description
□	3	NO ACCESS	NO ACCESS
□	2	READ	READ
☑	1	FULL ACCESS	FULL ACCESS

Saved Successfully.

Editing a User Group

1. Expand the right menu.

2. Click **Configuration Setup**, then click **User Management**, and then click **User Group**.
3. In the **Actions** column, click **Edit** for the user group to edit.
4. On the **New User Group** tab, change the details as required.
5. Click **Save**.
6. On the **User Role** tab, change the details as required.



USER GROUP

SEARCH

User Group:

DETAILS

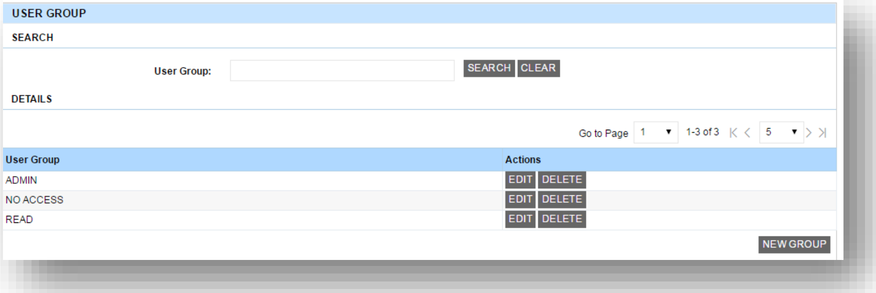
Go to Page 1 1-3 of 3 5

User Group	Actions
ADMIN	EDIT DELETE
NO ACCESS	EDIT DELETE
READ	EDIT DELETE

7. Click **Save**.

Deleting a User Group

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **User Group**.



USER GROUP

SEARCH

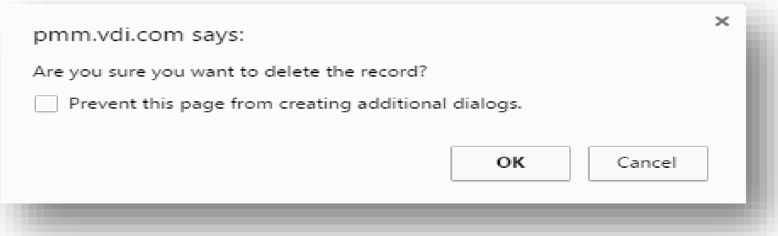
User Group:

DETAILS

Go to Page 1 1-3 of 3 5

User Group	Actions
ADMIN	EDIT DELETE
NO ACCESS	EDIT DELETE
READ	EDIT DELETE

3. In the **Actions** column, click **Delete** for the user role to delete.
4. **Are you sure you want to delete the record**? Prompt is display.



pmm.vdi.com says:

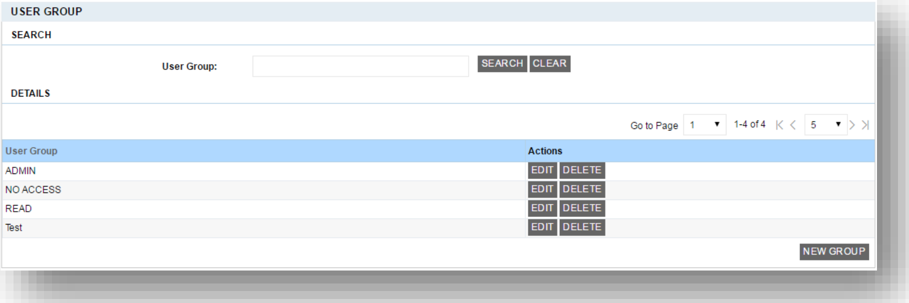
Are you sure you want to delete the record?

□ Prevent this page from creating additional dialogs.

5. Click **OK**.

Searching a User Group

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **User Group**.



USER GROUP

SEARCH

User Group:

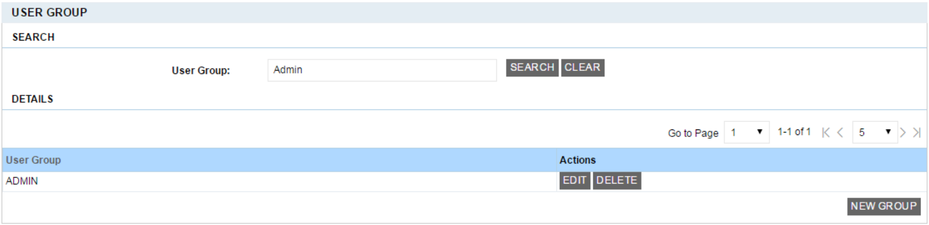
DETAILS

Go to Page 1 1-4 of 4 5

User Group	Actions
ADMIN	EDIT DELETE
NO ACCESS	EDIT DELETE
READ	EDIT DELETE
Test	EDIT DELETE

3. In the **Search** section, in **User Group**, enter the user group, for example, No Access, Read or Admin.
4. Click **Search**.

The required user group is display.



USER GROUP

SEARCH

User Group: Admin

DETAILS

Go to Page 1 1-1 of 1 5

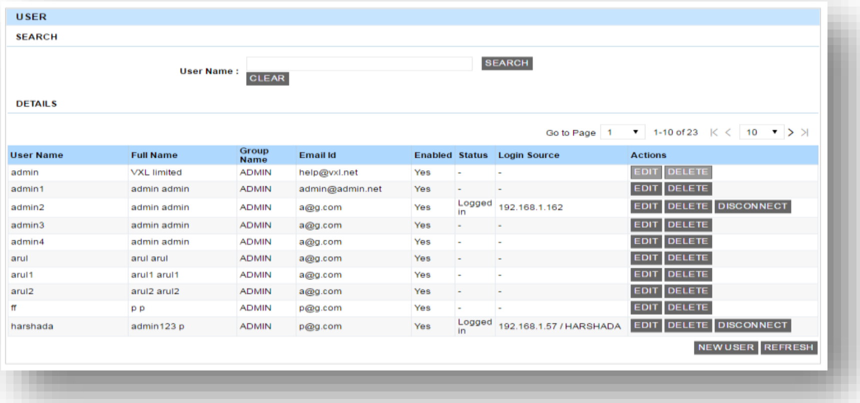
User Group	Actions
ADMIN	EDIT DELETE

Working with New Users

New User enables you to create various users for the Fusion EMM application, and to assign a group to a user.

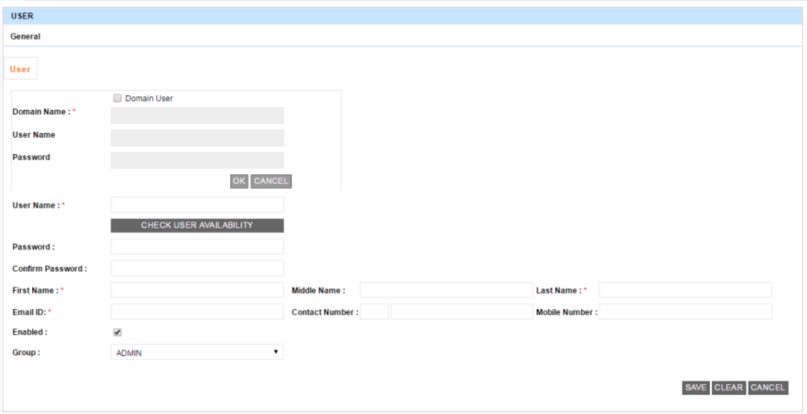
Creating a User

1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **New User**.



User Name	Full Name	Group Name	Email Id	Enabled	Status	Login Source	Actions
admin	VXL limited	ADMIN	help@vxl.net	Yes	-	-	EDIT DELETE
admin1	admin admin	ADMIN	admin@admin.net	Yes	-	-	EDIT DELETE
admin2	admin admin	ADMIN	a@g.com	Yes	Logged in	192.168.1.162	EDIT DELETE DISCONNECT
admin3	admin admin	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
admin4	admin admin	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul	arul arul	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul1	arul1 arul1	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul2	arul2 arul2	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
ff	p p	ADMIN	p@g.com	Yes	-	-	EDIT DELETE
harshada	admin123 p	ADMIN	p@g.com	Yes	Logged in	192.168.1.57 / HARSHADA	EDIT DELETE DISCONNECT

3. Under **Details**, click **New User**.



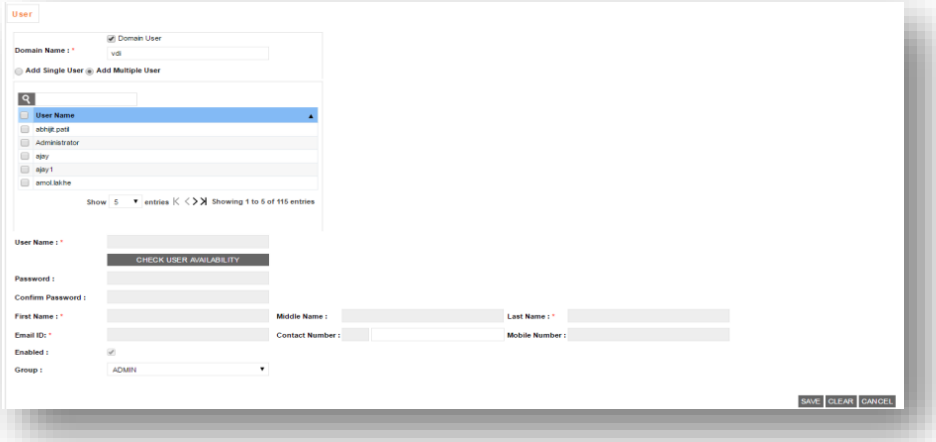
☐ Domain User

Enabled : ☑

Group : ADMIN

4. To configure the user settings for a specific user in a domain, select the **Domain User** check box.
5. In the **User Name** and **Password** text boxes pane, enter the domain administrator's user name and password.
6. Click **OK**.

a. When you enter the username and password details, a list of domain users becomes available in the **Domain User Name** list.



User

☑ Domain User

Domain Name : * vdi

○ Add Single User ● Add Multiple User

□	User Name
□	abhijit.patil
□	Administrator
□	ajay
□	ajay1
□	amol.lakhe

Show 5 entries Showing 1 to 5 of 115 entries

User Name : *

Password :

Confirm Password :

First Name : * Middle Name : Last Name : *

Email ID: * Contact Number : Mobile Number :

Enabled : ☑

Group : ADMIN

7. In the **Domain User Name** list, select the single user name or multiple user names for which the Fusion EMM application is to be configured.

If the **Domain User** check box is not selected, follow the steps listed below to create a new user.

8. Enter the mandatory details—**User Name, First Name, Last Name** and **Email Id**— and other details as required.
9. Click **Check User Availability** to confirm if the selected user name is available.
    b. If the user name exists in the application, the **User already exists** message is display.
    c. If the user name does not exist in the application, the **User name available message** is display.
10. Select the **Enabled** check box to enable the user to log into the Fusion EMM application.

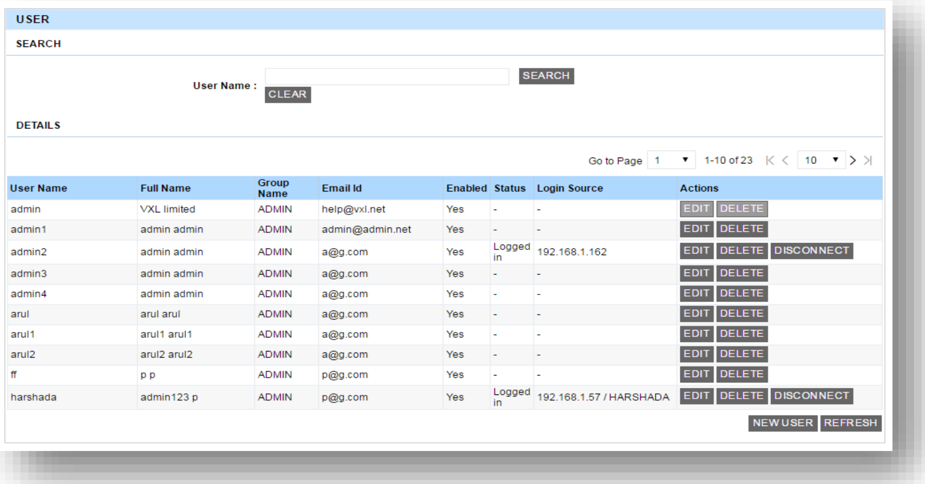
If the **Enabled** check box is not selected, the user is unable to log in to the application.

11. In the **Group** list, assign the group to enable the user to access the features of the application as applicable.

12. Click **Save**.

Searching a User

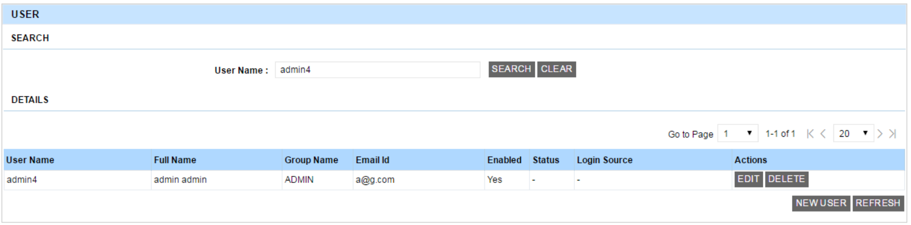
1. Expand the right menu.
2. Click **Configuration Setup**, then click **User Management**, and then click **New User**.



User Name	Full Name	Group Name	Email Id	Enabled	Status	Login Source	Actions
admin	VXL limited	ADMIN	help@vxl.net	Yes	-	-	EDIT DELETE
admin1	admin admin	ADMIN	admin@admin.net	Yes	-	-	EDIT DELETE
admin2	admin admin	ADMIN	a@g.com	Yes	Logged in	192.168.1.162	EDIT DELETE DISCONNECT
admin3	admin admin	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
admin4	admin admin	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul	arul arul	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul1	arul1 arul1	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
arul2	arul2 arul2	ADMIN	a@g.com	Yes	-	-	EDIT DELETE
ff	p p	ADMIN	p@g.com	Yes	-	-	EDIT DELETE
harshada	admin123 p	ADMIN	p@g.com	Yes	Logged in	192.168.1.57 / HARSHADA	EDIT DELETE DISCONNECT

3. In the **Search** section, in **User name**, enter the user name, full name, group name or email ID to search a record.
4. Click **Search.**

The required user is display.



User Name : admin4

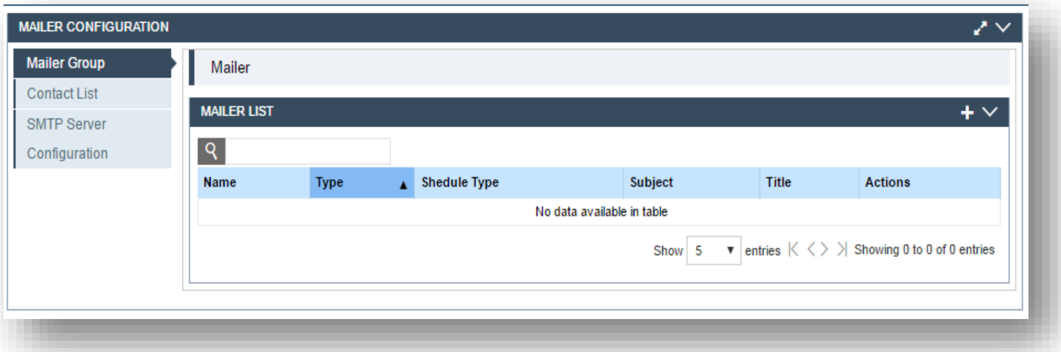
User Name	Full Name	Group Name	Email Id	Enabled	Status	Login Source	Actions
admin4	admin admin	ADMIN	a@g.com	Yes	-	-	EDIT DELETE

Working with Mailer Engine Configuration

The **Mailer Engine Configuration** enables you to set up automatic email of reports to user email ids.

Prerequisites:

1. Correct SMTP server details must be provided.
2. Antivirus software installed on the client should allow the sending email from the SMTP port.

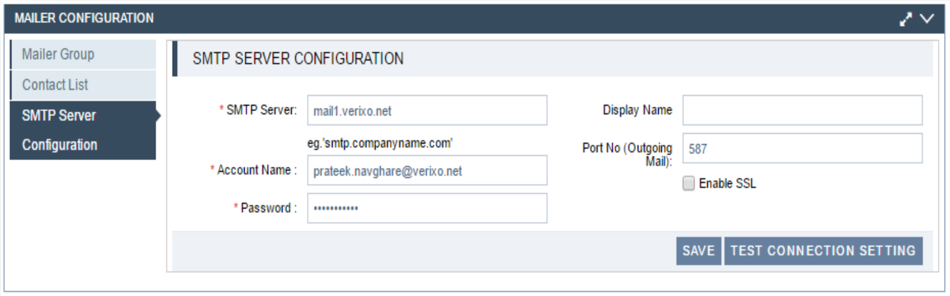


Name	Type	Shedule Type	Subject	Title	Actions
No data available in table					

Show 5 entries Showing 0 to 0 of 0 entries

Configuring the SMTP Server

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration.**



* SMTP Server: mail1.verixo.net

eg.'smtp.companyname.com'

* Account Name : prateek.navghare@verixo.net

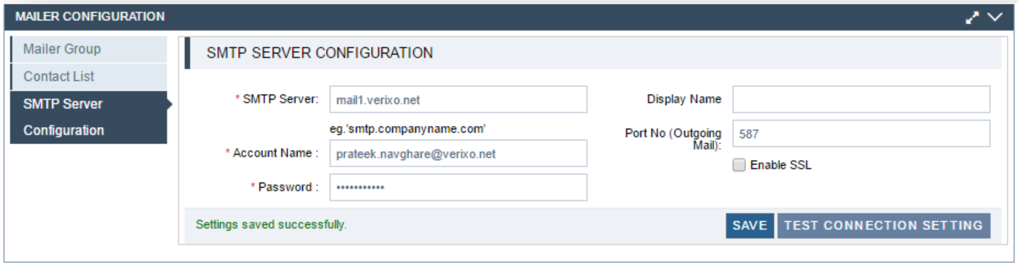
* Password : •••••••••••

Display Name

Port No (Outgoing Mail): 587

☐ Enable SSL

3. On the **SMTP Server Configuration** tab, enter the required details.
4. Test Connection Use to check whether Configure SMTP server proper or not.
5. Click **Save**.



* SMTP Server: mail1.verixo.net

eg.'smtp.companyname.com'

* Account Name : prateek.navghare@verixo.net

* Password : •••••••••••

Display Name

Port No (Outgoing Mail): 587

☐ Enable SSL

Settings saved successfully.

The SMTP server settings saved successfully message is display.

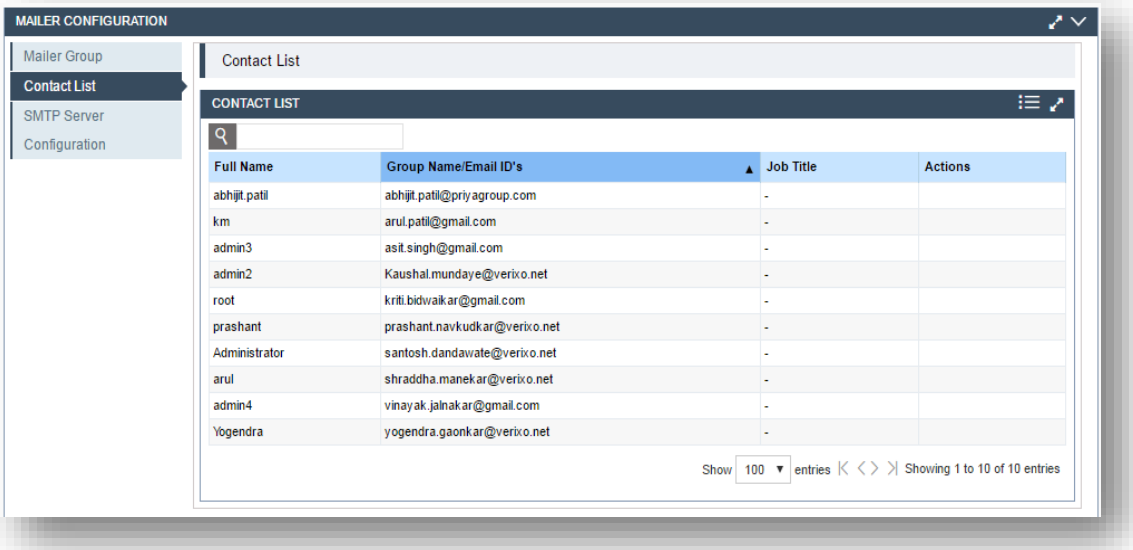
- Port number indicates the outgoing Port number
- If Enable SSL checkbox is checked then mail server going to be accessed by HTTPS.
- If it is not checked then it can be accessed by HTTP.
- If Attach .csv check box is checked then reports in the format of .csv get attached to the mail.

Configuring Contact List

Add

1. Expand the right menu.

2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration.**
3. Click on Contact List tab



MAILER CONFIGURATION

- Mailer Group
- Contact List
- SMTP Server Configuration

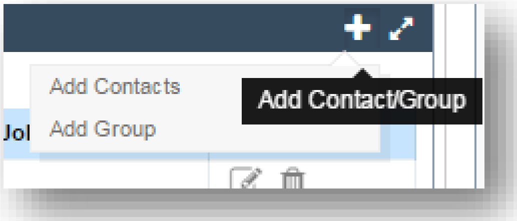
Contact List

CONTACT LIST

Full Name	Group Name/Email ID's ▲	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
admin2	Kaushal.mundaye@verixo.net	-	
root	kriti.bidwaikar@gmail.com	-	
prashant	prashant.navkudkar@verixo.net	-	
Administrator	santosh.dandawate@verixo.net	-	
arul	shraddha.manekar@verixo.net	-	
admin4	vinayak.jalnakar@gmail.com	-	
Yogendra	yogendra.gaonkar@verixo.net	-	

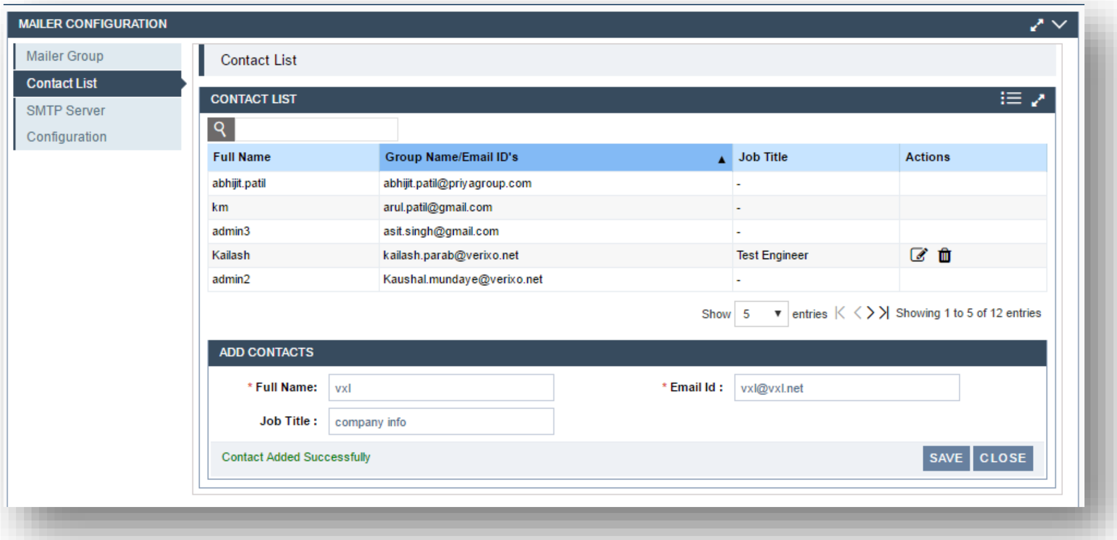
Show 100 ▾ entries Showing 1 to 10 of 10 entries

4. Click on image ✚ to add Contact/ group.
5. User able to add single/group contact records to mailer configuration.



6. Click on Add Contact to add single contact form gets open.
7. Add all mandatory fields.
8. Click On SAVE.
9. Settings saved successfully message displayed.
10. This Contact list displayed in Mailer Configure as a recipient data.

- Automatic import of email id of Fusion EMM users, domain users in the mailer contact list.



Full Name	Group Name/Email ID's	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
Kailash	kailash.parab@verixo.net	Test Engineer	
admin2	Kaushal.mundaye@verixo.net	-	

Show 5 entries Showing 1 to 5 of 12 entries

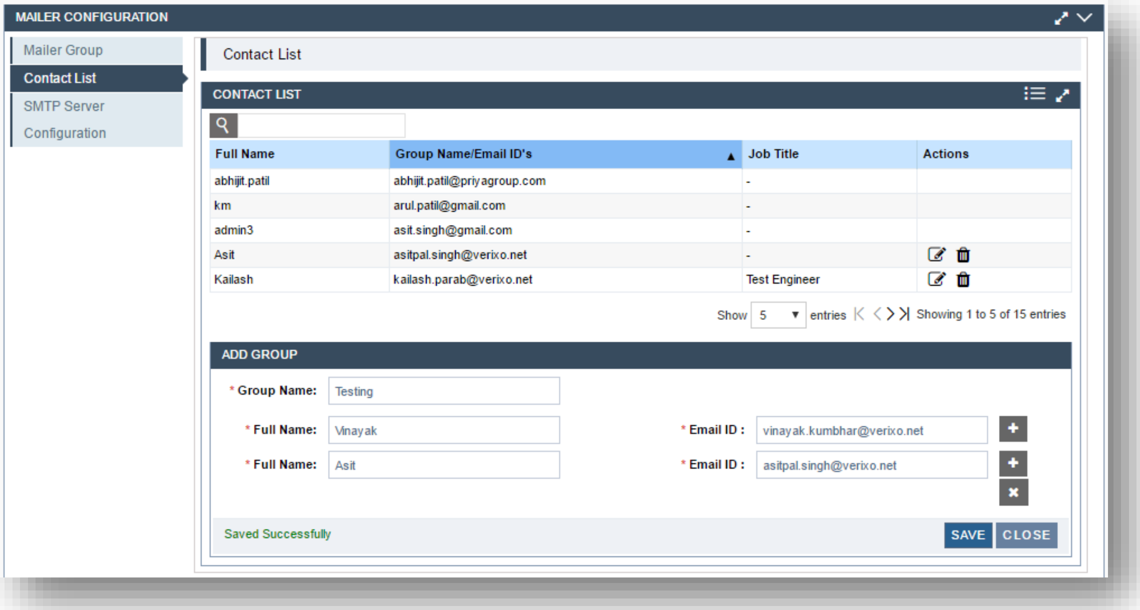
* Full Name: vxl

* Email Id : vxl@vxl.net

Job Title : company info

Contact Added Successfully

11. Add group where User able to store multiple recipient data and able to select that particular group at time of mailer configure.



Full Name	Group Name/Email ID's	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
Asit	asitpal.singh@verixo.net	-	
Kailash	kailash.parab@verixo.net	Test Engineer	

Show 5 entries Showing 1 to 5 of 15 entries

* Group Name: Testing

* Full Name: Vinayak * Email ID : vinayak.kumbhar@verixo.net

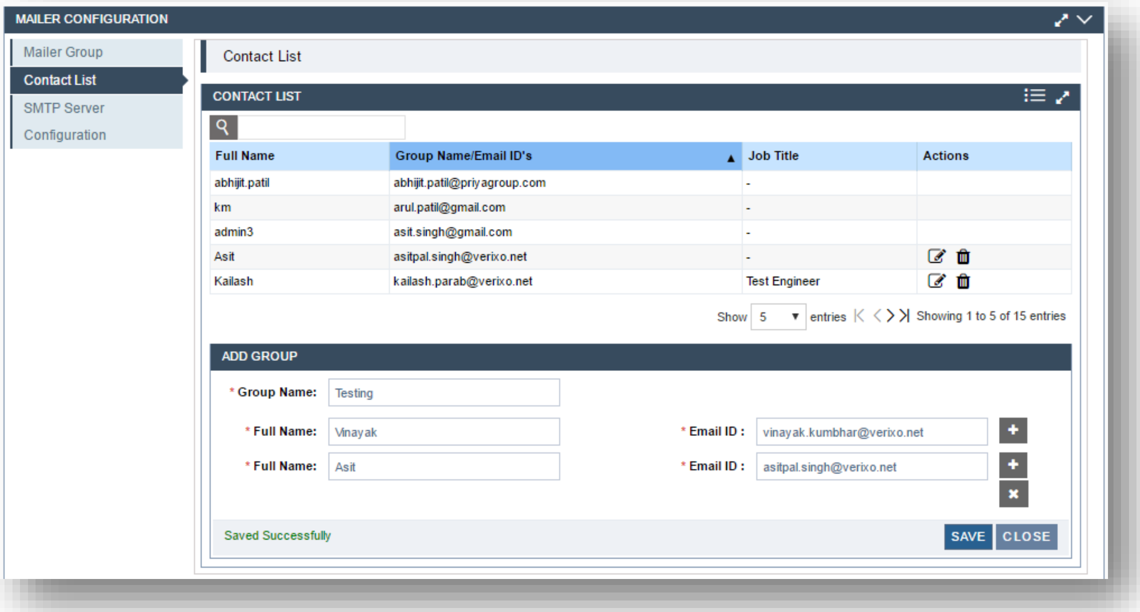
* Full Name: Asit * Email ID : asitpal.singh@verixo.net

Saved Successfully

12. Click on **SAVE**.
13. Group added successfully.

Edit

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.
3. Click **on Edit image** 📝 **.**



Full Name	Group Name/Email ID's	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
Asit	asitpal.singh@verixo.net	-	📝 🗑
Kailash	kailash.parab@verixo.net	Test Engineer	📝 🗑

Show 5 entries Showing 1 to 5 of 15 entries

ADD GROUP

* Group Name: Testing
* Full Name: Vinayak * Email ID : vinayak.kumbhar@verixo.net
* Full Name: Asit * Email ID : asitpal.singh@verixo.net

Saved Successfully

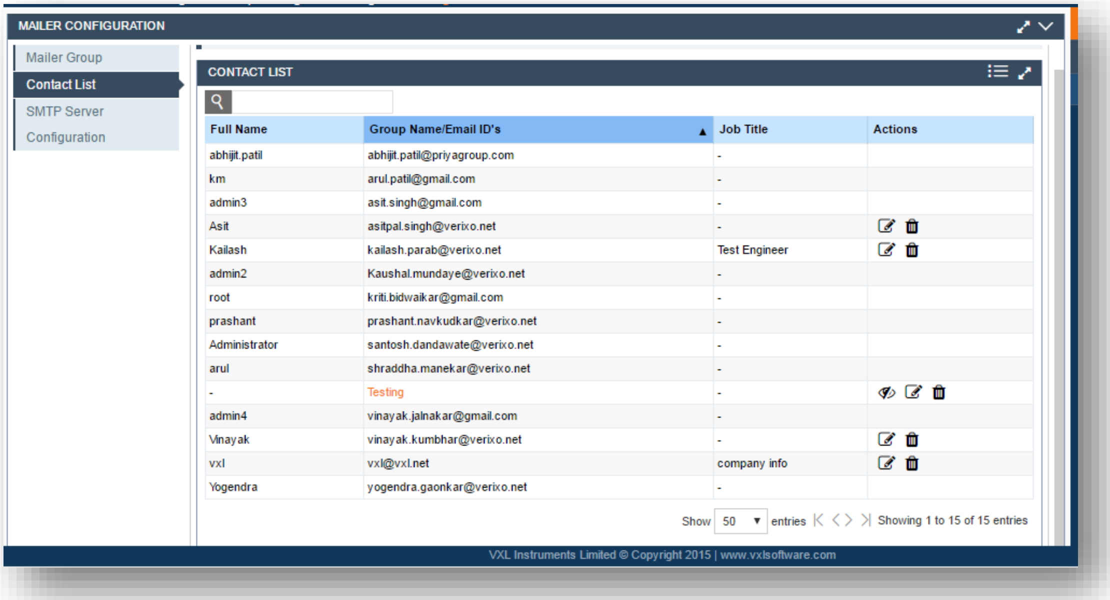
4. Click **Edit** button to edit existing contacts or group contacts.
5. Click **Save**.

The **Record Saved successfully** message is display.

Delete

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.

3. Click on delete image 🗑.

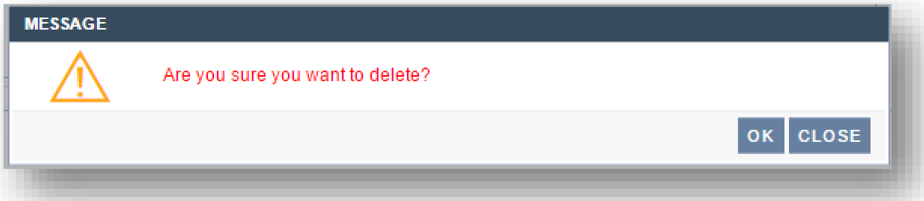


Full Name	Group Name/Email ID's ▲	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
Asit	asitpal.singh@verixo.net	-	✎ 🗑
Kailash	kailash.parab@verixo.net	Test Engineer	✎ 🗑
admin2	Kaushal.mundaye@verixo.net	-	
root	kriti.bidwaikar@gmail.com	-	
prashant	prashant.navkudkar@verixo.net	-	
Administrator	santosh.dandawate@verixo.net	-	
arul	shraddha.manekar@verixo.net	-	
-	Testing	-	👁 ✎ 🗑
admin4	vinayak.jalnakar@gmail.com	-	
Vinayak	vinayak.kumbhar@verixo.net	-	✎ 🗑
vxl	vxl@vxl.net	company info	✎ 🗑
Yogendra	yogendra.gaonkar@verixo.net	-	

Show 50 entries Showing 1 to 15 of 15 entries

VXL Instruments Limited © Copyright 2015 | www.vxlsoftware.com

4. Click **Delete** for the contact to delete. **Are you sure you want to delete the record?** Prompt is display.



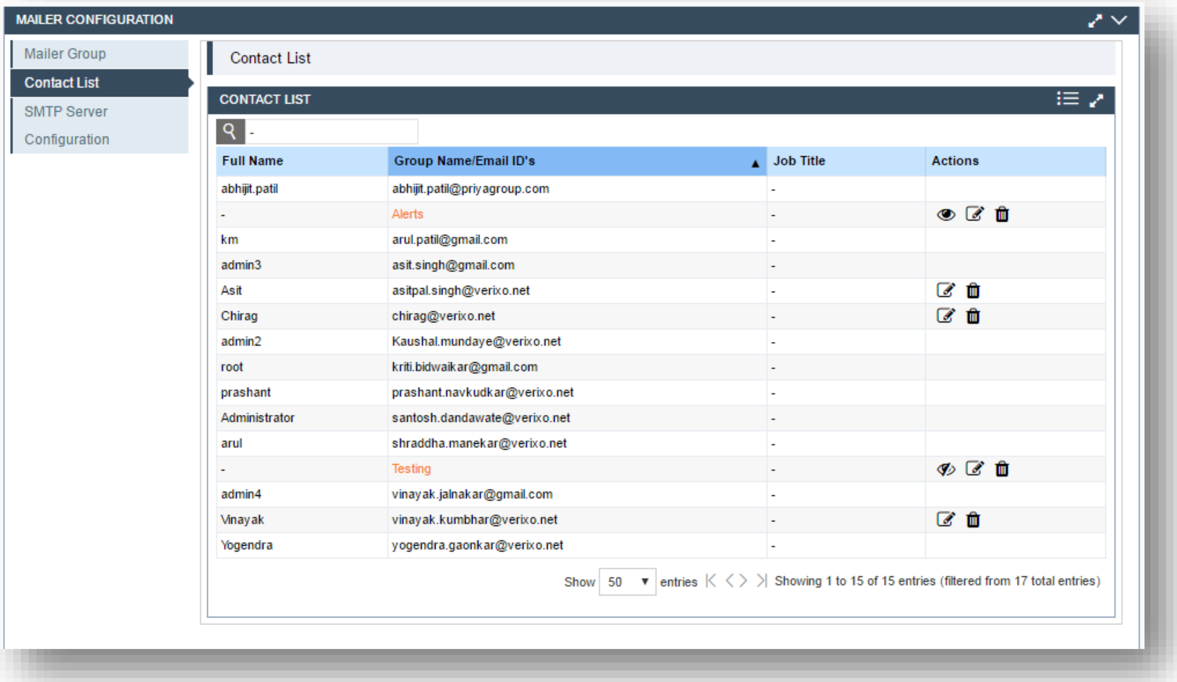
Are you sure you want to delete?

5. Click **OK**.

- Enable/ Disable functionality only available for Groups.
- Group name displayed in color.
- Group name does not contain first name as single contact.

Enable/ Disable Mailer Group

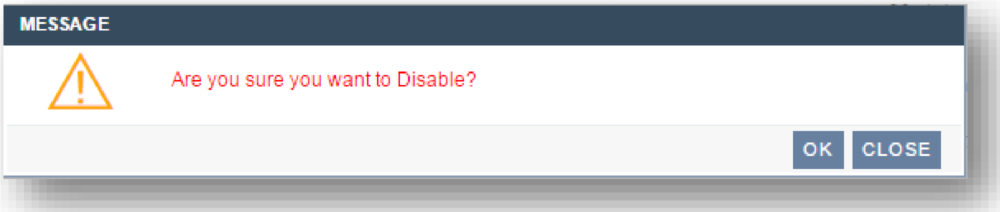
1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.
3. User able to activate and deactivate the existing mailer Logs and mailer groups by selecting ⊘ / 👁 image respectively.
4. User able to Active or Inactive only groups, For single contact Active / Inactive feature not displayed.



Full Name	Group Name/Email ID's ▲	Job Title	Actions
abhijit.patil	abhijit.patil@priyagroup.com	-	
-	Alerts	-	👁 ✎ 🗑
km	arul.patil@gmail.com	-	
admin3	asit.singh@gmail.com	-	
Asit	asitpal.singh@verixo.net	-	✎ 🗑
Chirag	chirag@verixo.net	-	✎ 🗑
admin2	Kaushal.mundaye@verixo.net	-	
root	kriti.bidwaikar@gmail.com	-	
prashant	prashant.navkudkar@verixo.net	-	
Administrator	santosh.dandawate@verixo.net	-	
arul	shraddha.manekar@verixo.net	-	
-	Testing	-	⊘ ✎ 🗑
admin4	vinayak.jalnakar@gmail.com	-	
Vinayak	vinayak.kumbhar@verixo.net	-	✎ 🗑
Yogendra	yogendra.gaonkar@verixo.net	-	

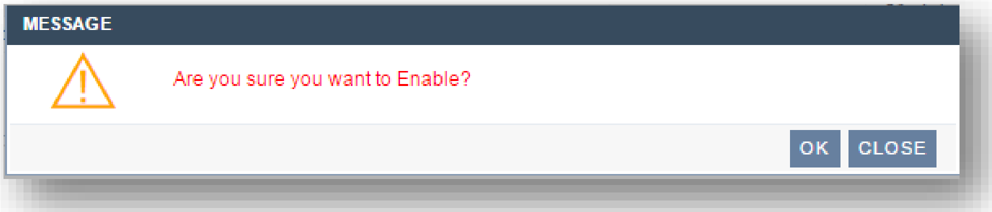
Show 50 ▼ entries |< < > >| Showing 1 to 15 of 15 entries (filtered from 17 total entries)

5. To inactive group, click on 👁 , Are **you sure you want to Disable?** Prompt is display.


MESSAGE

Are you sure you want to Disable?

6. To Active group click on , Are **you sure you want to Enable?** Prompt is display.


MESSAGE

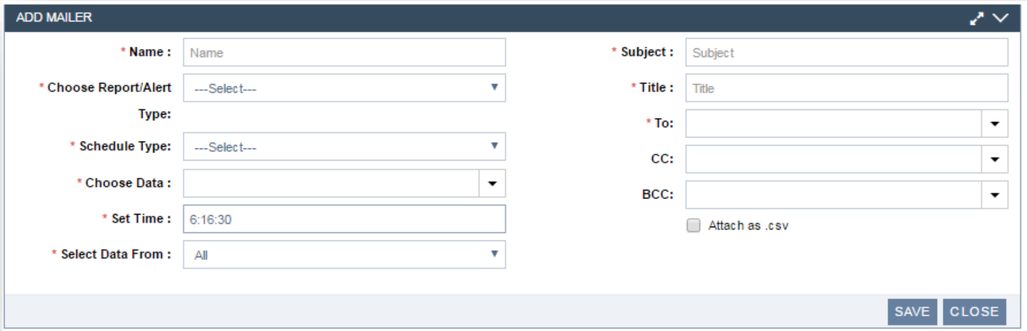
Are you sure you want to Enable?

7. Click **OK**.

Configuring Mailer group

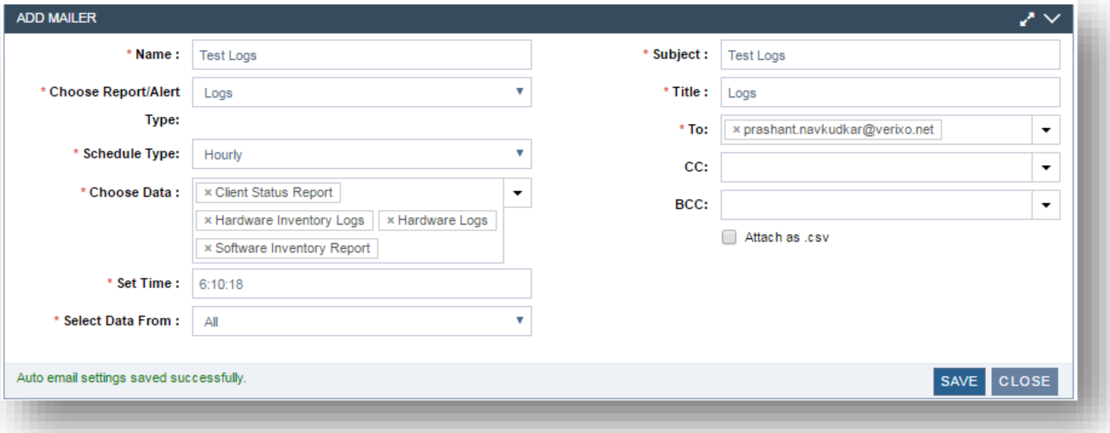
Adding a mailer group

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration** then click Mailer group
3. Click on Add image+.


ADD MAILER

* Name :	Name	* Subject :	Subject
* Choose Report/Alert Type:	---Select---	* Title :	Title
* Schedule Type:	---Select---	* To:	
* Choose Data :		CC:	
* Set Time :	6:16:30	BCC:	
* Select Data From :	All		□ Attach as .csv

4. Enter all required fields.
5. The **Email type**, **Report type**, **Subject,** and **Title** details are populated by default.
6. In **Set time**, enter the time to schedule the email.
7. In the **Email contents**, select the applicable check boxes for the logs to include in the email.
8. In **Contact details**, select the recipient(s) to add to **Recipient**, **CC Recipient** and **BCC Recipient** addresses.
9. Click **Save**.
10. Auto email setting saved successfully.



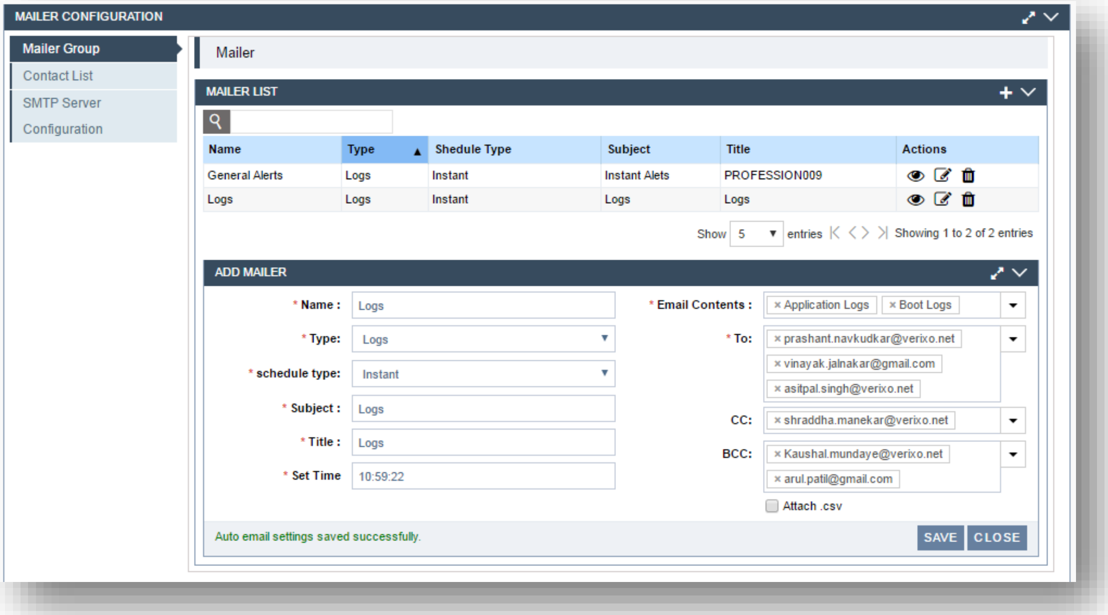
ADD MAILER

* Name :	Test Logs	* Subject :	Test Logs
* Choose Report/Alert Type:	Logs	* Title :	Logs
* Schedule Type:	Hourly	* To:	× prashant.navkudkar@verixo.net
* Choose Data :	× Client Status Report × Hardware Inventory Logs × Hardware Logs × Software Inventory Report	CC:	
* Set Time :	6:10:18	BCC:	
* Select Data From :	All		□ Attach as .csv

Auto email settings saved successfully.

Editing a mailer group

6. Expand the right menu.
7. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.
8. Click **on Edit image** ✎ **.**



Name	Type	Shedule Type	Subject	Title	Actions
General Alerts	Logs	Instant	Instant Alets	PROFESSION009	👁 ✎ 🗑
Logs	Logs	Instant	Logs	Logs	👁 ✎ 🗑

Show 5 entries Showing 1 to 2 of 2 entries

ADD MAILER

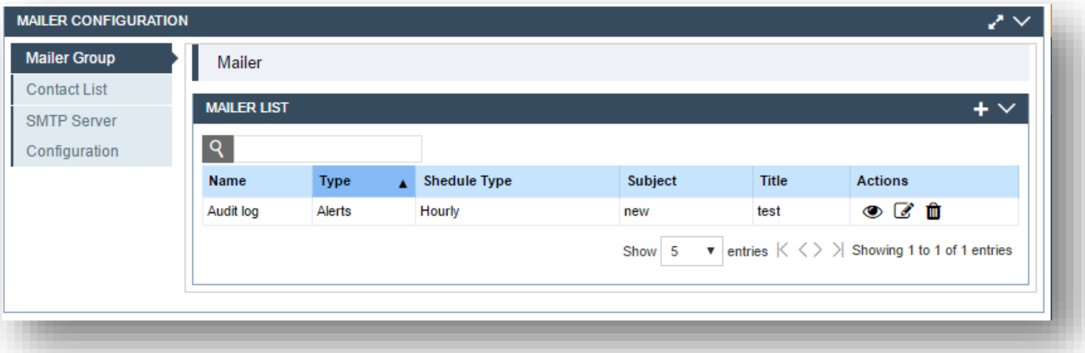
* Name :	Logs	* Email Contents :	× Application Logs × Boot Logs
* Type:	Logs	* To:	× prashant.navkudkar@verixo.net × vinayak.jalnakar@gmail.com × asitpal.singh@verixo.net
* schedule type:	Instant	CC:	× shraddha.manekar@verixo.net
* Subject :	Logs	BCC:	× Kaushal.mundaye@verixo.net × arul.patil@gmail.com
* Title :	Logs		□ Attach .csv
* Set Time	10:59:22		

Auto email settings saved successfully.

9. Click **Edit** for the contact to edit.
10. In the **Name** column, edit the contact name.
11. Click **Save**.
12. Auto email settings saved successfully message displayed.

Deleting a mailer group

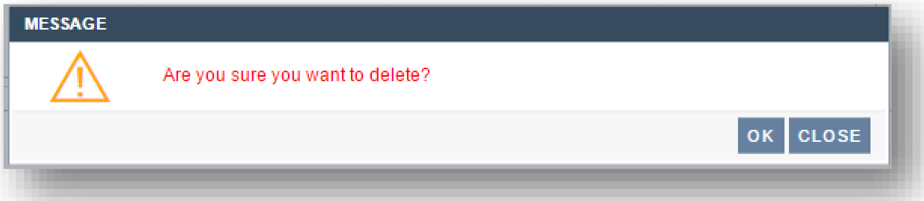
6. Expand the right menu.
7. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.
8. Click on delete image 🗑.



Name	Type	Shedule Type	Subject	Title	Actions
Audit log	Alerts	Hourly	new	test	👁 ✎ 🗑

Show 5 entries Showing 1 to 1 of 1 entries

9. Click **Delete** for the contact to delete. **Are you sure you want to delete the record?** Prompt is display.



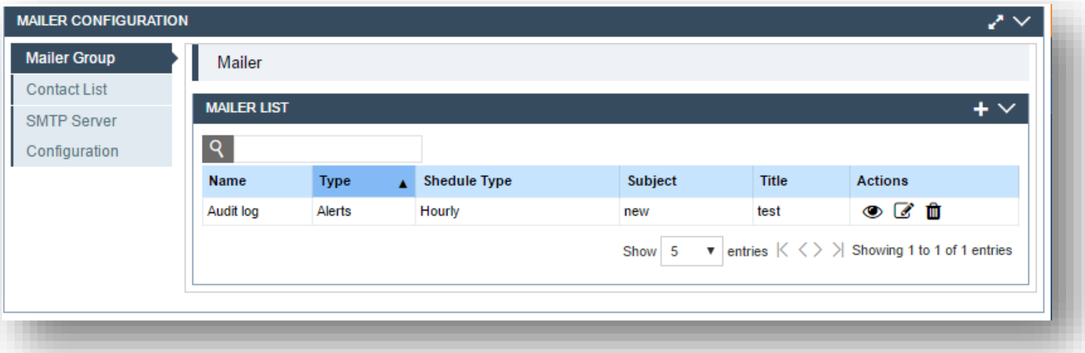
MESSAGE

Are you sure you want to delete?

10. Click **OK**.

Enable/ Disable Mailer Configure

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Mailer Engine Configuration**.
3. User able to activate and deactivate the existing mailer Logs and mailer groups by selecting 👁 / 👁 image respectively.



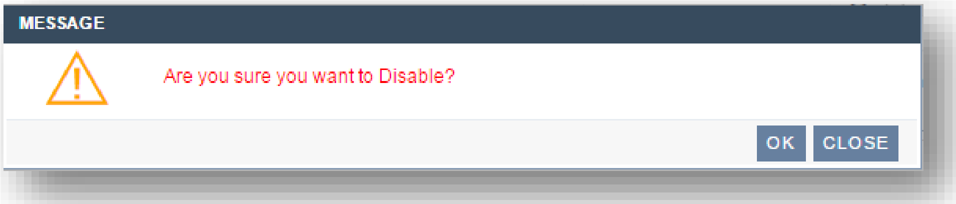
MAILER CONFIGURATION

MAILER LIST

Name	Type	Shedule Type	Subject	Title	Actions
Audit log	Alerts	Hourly	new	test	👁 ✎ 🗑

Show 5 entries Showing 1 to 1 of 1 entries

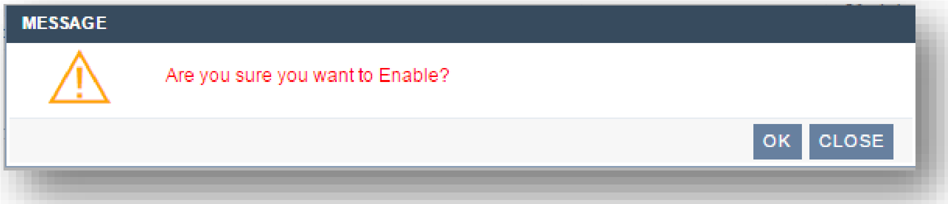
4. To inactive group, click on 👁, Are **you sure you want to InActive?** Prompt is display.



MESSAGE

Are you sure you want to Disable?

5. To Active group click on ![], Are **you sure you want to Active?** Prompt is display.



MESSAGE

Are you sure you want to Enable?

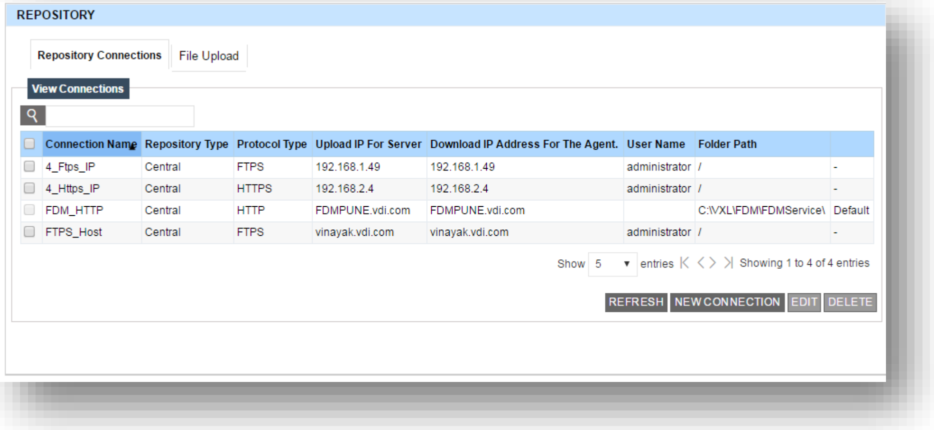
6. Click **OK**.

Working with the Repository

You can create, edit, and delete repository connections. Additionally, you can configure the repository to view connections and details of the connections such as connection name, repository type, SSL type, the server's upload IP, the agent's download IP, username, folder path.

Creating a New Repository Connection

1. Expand the right menu.
2. Click Configuration Setup, then click Configuration Settings, and then click Repository.

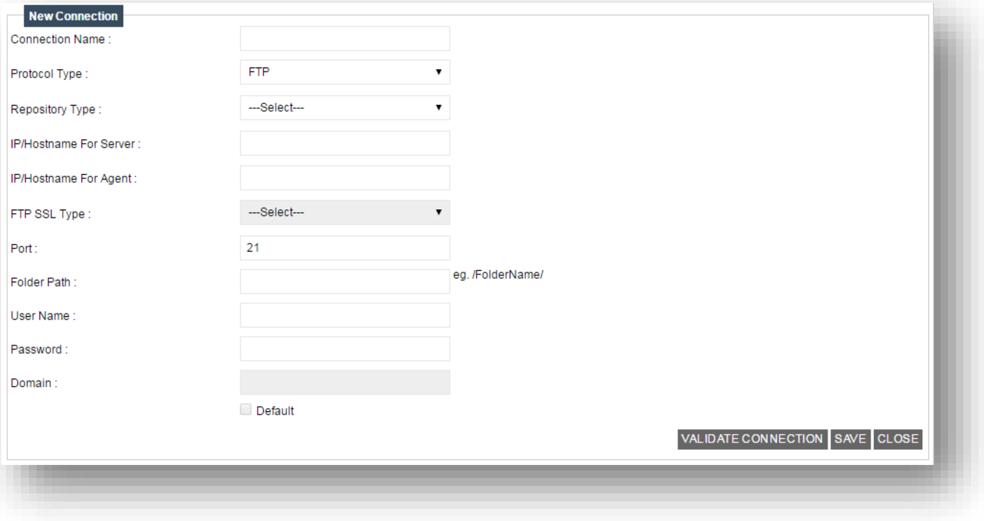


REPOSITORY

□	Connection Name	Repository Type	Protocol Type	Upload IP For Server	Download IP Address For The Agent.	User Name	Folder Path	
□	4_Ftps_IP	Central	FTPS	192.168.1.49	192.168.1.49	administrator	/	-
□	4_Https_IP	Central	HTTPS	192.168.2.4	192.168.2.4	administrator	/	-
□	FDM_HTTP	Central	HTTP	FDMPUNE.vdi.com	FDMPUNE.vdi.com		C:\VXL\FDM\FDMService\	Default
□	FTPS_Host	Central	FTPS	vinayak.vdi.com	vinayak.vdi.com	administrator	/	-

Show 5 entries Showing 1 to 4 of 4 entries

3. On the Repository Connections tab, in View Connections, click New Connection.



New Connection

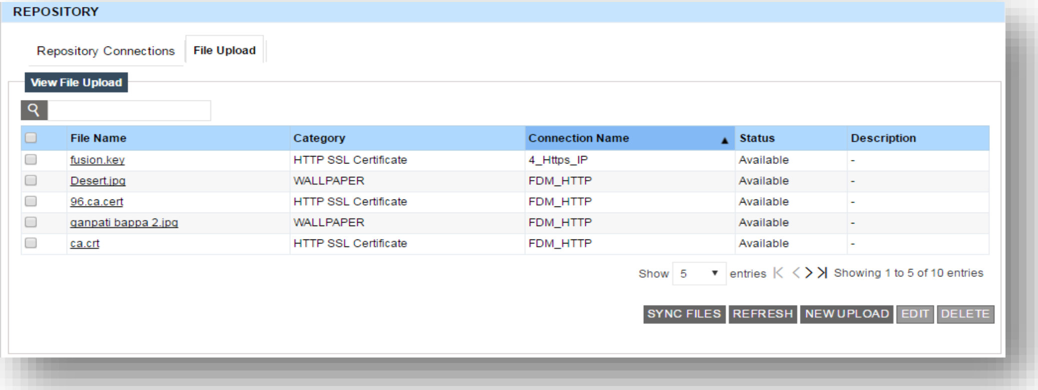
Connection Name :	
Protocol Type :	FTP
Repository Type :	---Select---
IP/Hostname For Server :	
IP/Hostname For Agent :	
FTP SSL Type :	---Select---
Port :	21
Folder Path :	eg. /FolderName/
User Name :	
Password :	
Domain :	
	□ Default

4. In Connection Name, enter a name for the connection.
5. In the Repository Type, select the type of repository.
6. In IP For Server, enter the upload IP for the server.
7. In IP For Agent, enter the download IP for the agent.
8. In the FTP SSL Type list, select the required SSL file transfer type.
9. In Folder Path, enter the required path to the root folder.
10. In User Name and Password, enter the administrator's FTP credentials.
11. To make the connection the default connection, select the Default check box.
12. To validate the connection to the server, click Validate Connection.
13. Click Save.

Uploading a File

- HTTP, CIFS, FTP and FTPS connections can be created in repository manager.
- For HTTP, FTP & FTPS connections it is mandatory to have a connection site created for respective connection type with basic authentication in IIS manager.
- For CIFS connection, specified folder name in connection details should have proper share rights with basic authentication.

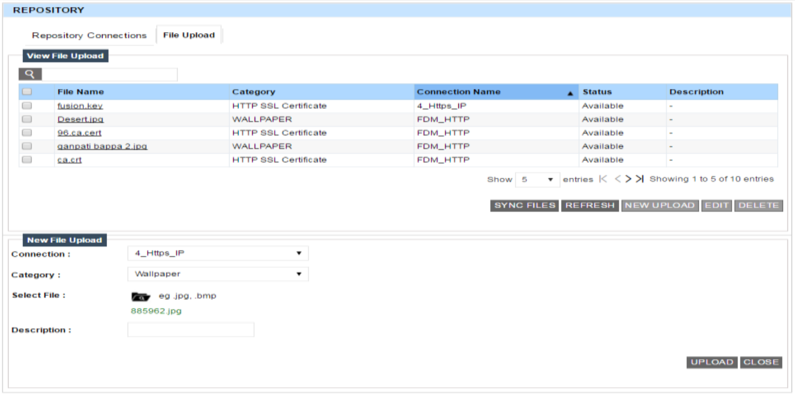
1. Expand the right menu.
2. Click Configuration Setup, then click Configuration Settings, and then click Repository.



□	File Name	Category	Connection Name ▲	Status	Description
□	fusion.key	HTTP SSL Certificate	4_Https_IP	Available	-
□	Desert.jpg	WALLPAPER	FDM_HTTP	Available	-
□	96.ca.cert	HTTP SSL Certificate	FDM_HTTP	Available	-
□	ganpati bappa 2.jpg	WALLPAPER	FDM_HTTP	Available	-
□	ca.crt	HTTP SSL Certificate	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 5 of 10 entries

3. Click the File Upload tab.
4. Click New Upload.
5. In New File Upload, select the repository connection name and category of the connection.
6. In Select File, click to select file to upload.

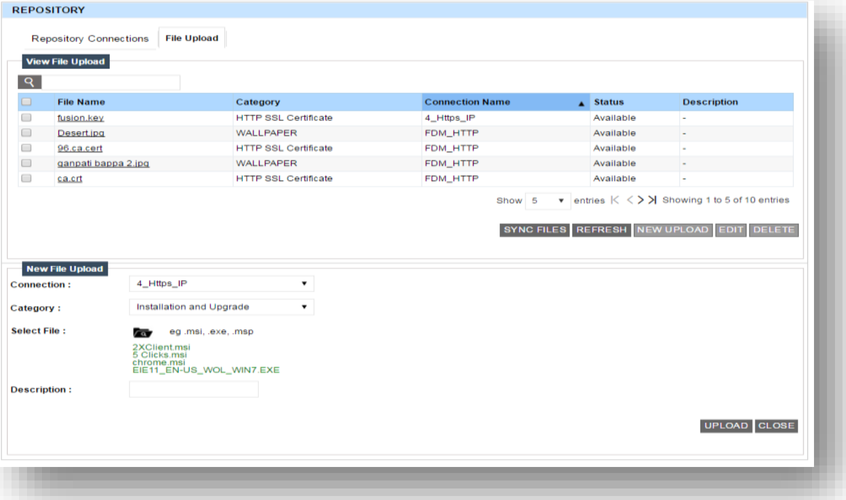


□	File Name	Category	Connection Name ▲	Status	Description
□	fusion.key	HTTP SSL Certificate	4_Https_IP	Available	-
□	Desert.jpg	WALLPAPER	FDM_HTTP	Available	-
□	96.ca.cert	HTTP SSL Certificate	FDM_HTTP	Available	-
□	ganpati bappa 2.jpg	WALLPAPER	FDM_HTTP	Available	-
□	ca.crt	HTTP SSL Certificate	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 5 of 10 entries

Connection : 4_Https_IP
Category : Wallpaper
Select File : eg .jpg, .bmp
885962.jpg
Description :

7. We can upload multiple files at a time.
8. Click Upload.



☐	File Name	Category	Connection Name ▲	Status	Description
☐	fusion.key	HTTP SSL Certificate	4_Https_IP	Available	-
☐	Desert.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	96.ca.cert	HTTP SSL Certificate	FDM_HTTP	Available	-
☐	ganpati bappa 2.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	ca.crt	HTTP SSL Certificate	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 5 of 10 entries

Connection : 4_Https_IP

Category : Installation and Upgrade

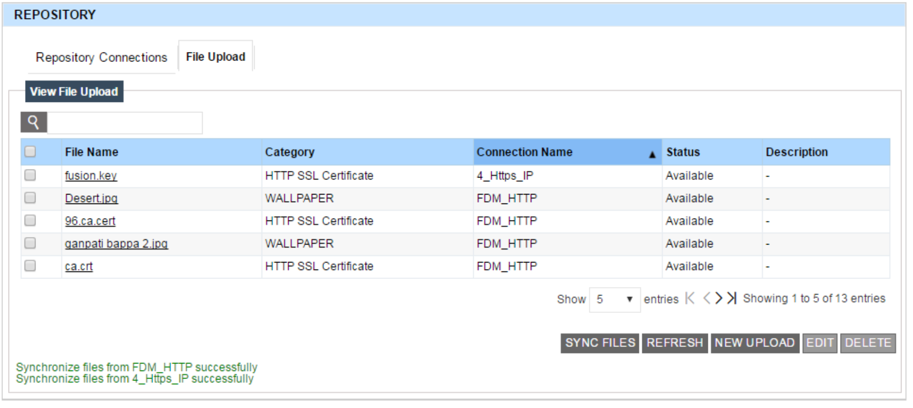
Select File : eg .msi, .exe, .msp

2XClient.msi
5 Clicks.msi
chrome.msi
EIE11_EN-US_WOL_WIN7.EXE

Description :

Sync Files repository files

1. When we are uploading for all connections sync button use to get all files from repository server.
2. Add delete manually click on sync all files were updated.



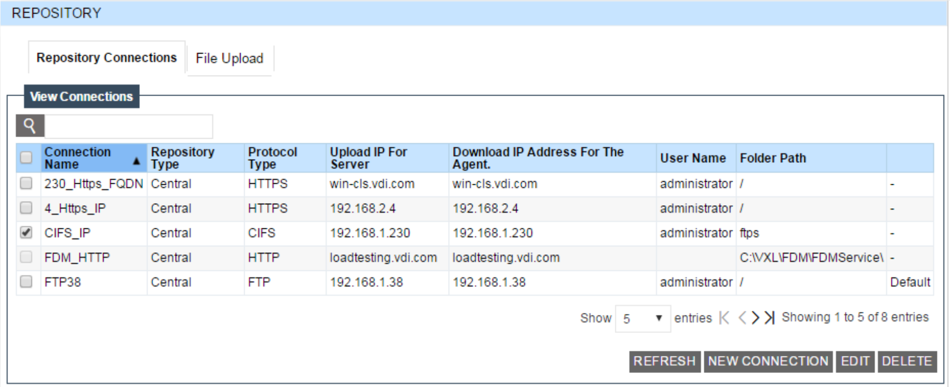
☐	File Name	Category	Connection Name ▲	Status	Description
☐	fusion.key	HTTP SSL Certificate	4_Https_IP	Available	-
☐	Desert.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	96.ca.cert	HTTP SSL Certificate	FDM_HTTP	Available	-
☐	ganpati bappa 2.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	ca.crt	HTTP SSL Certificate	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 5 of 13 entries

Synchronize files from FDM_HTTP successfully
Synchronize files from 4_Https_IP successfully

Editing a Repository Connection

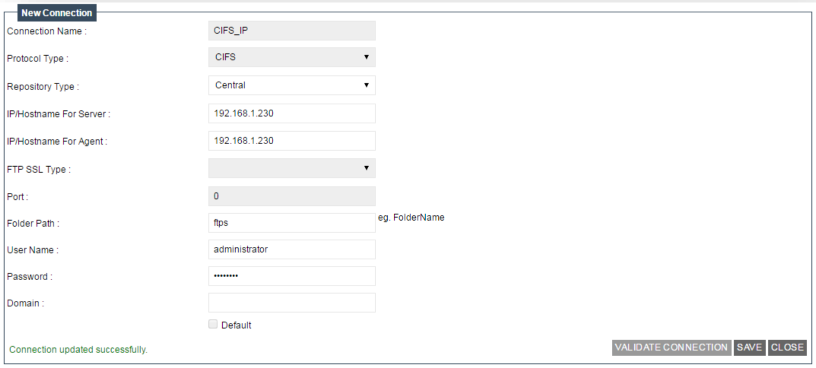
1. Expand the right menu.
2. Click Configuration Setup, then click Configuration Settings, and then click Repository.



☐	Connection Name ▲	Repository Type	Protocol Type	Upload IP For Server	Download IP Address For The Agent.	User Name	Folder Path	
☐	230_Https_FQDN	Central	HTTPS	win-cls.vdi.com	win-cls.vdi.com	administrator	/	-
☐	4_Https_IP	Central	HTTPS	192.168.2.4	192.168.2.4	administrator	/	-
☑	CIFS_IP	Central	CIFS	192.168.1.230	192.168.1.230	administrator	ftps	-
☐	FDM_HTTP	Central	HTTP	loadtesting.vdi.com	loadtesting.vdi.com		C:\VXL\FDM\FDMService\	-
☐	FTP38	Central	FTP	192.168.1.38	192.168.1.38	administrator	/	Default

Show 5 entries Showing 1 to 5 of 8 entries

3. Select Connection.
4. Click Edit.
5. Click Save after updating the Connection.
6. The Connection Updated successfully message is display.

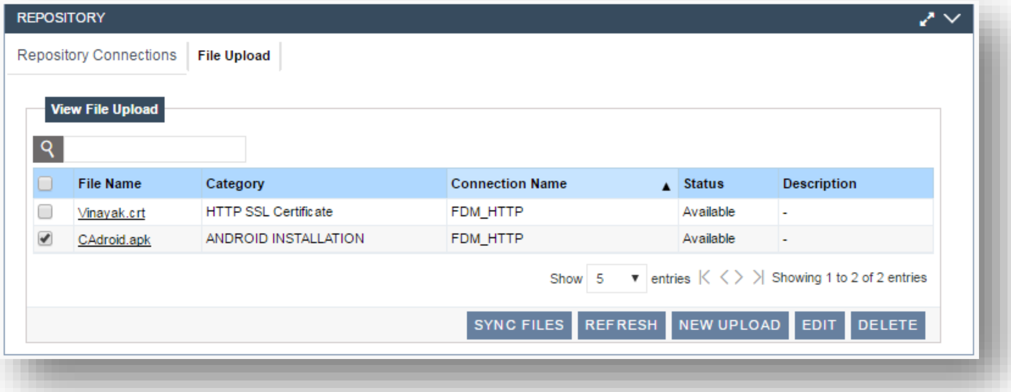


Connection Name :	CIFS_IP
Protocol Type :	CIFS
Repository Type :	Central
IP/Hostname For Server :	192.168.1.230
IP/Hostname For Agent :	192.168.1.230
FTP SSL Type :	
Port :	0
Folder Path :	ftps eg. FolderName
User Name :	administrator
Password :	•••••••••
Domain :	
	☐ Default

Connection updated successfully.

Editing a Uploaded File in Repository Connection

1. Click the File Upload tab.
2. On the File Upload tab, in the Select column, select the file to edit.
3. Click Edit.

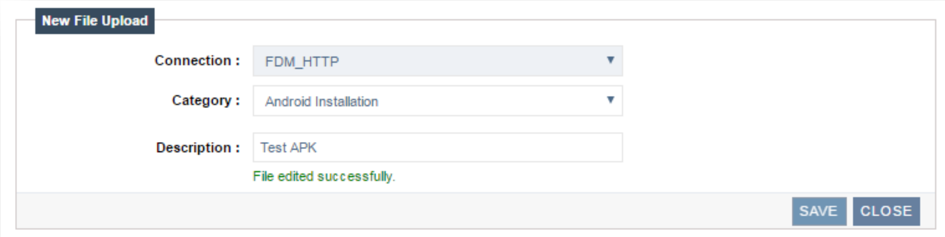


□	File Name	Category	Connection Name ▲	Status	Description
□	Vinayak.crt	HTTP SSL Certificate	FDM_HTTP	Available	-
☑	CAdroid.apk	ANDROID INSTALLATION	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 2 of 2 entries

4. In the New File Upload, change the connection and category as required.
5. Click Upload.

   The File edited successfully message is display.



Connection : FDM_HTTP

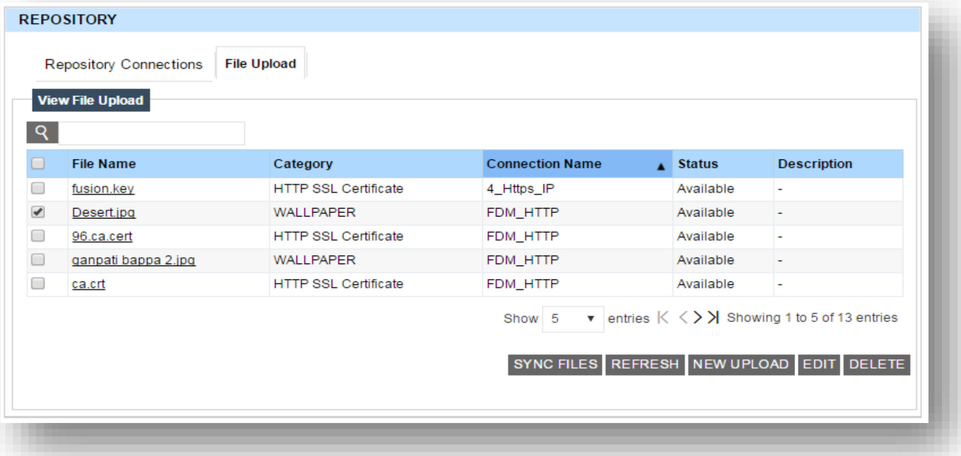
Category : Android Installation

Description : Test APK

File edited successfully.

Deleting a Repository Connection

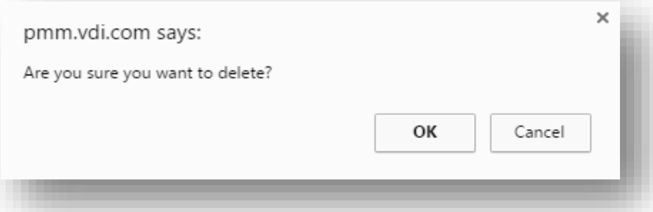
1. Expand the right menu.
2. Click Configuration Setup, then click Configuration Settings, and then click Repository.



☐	File Name	Category	Connection Name ▲	Status	Description
☐	fusion.key	HTTP SSL Certificate	4_Https_IP	Available	-
☑	Desert.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	96.ca.cert	HTTP SSL Certificate	FDM_HTTP	Available	-
☐	ganpati bappa 2.jpg	WALLPAPER	FDM_HTTP	Available	-
☐	ca.crt	HTTP SSL Certificate	FDM_HTTP	Available	-

Show 5 entries Showing 1 to 5 of 13 entries

3. Click the File Upload tab.
4. On the File Upload tab, in the Select column, select the file to delete.
5. Click Delete.
6. Are you sure you want to delete? Prompt is display


pmm.vdi.com says:

Are you sure you want to delete?

7. Click OK.

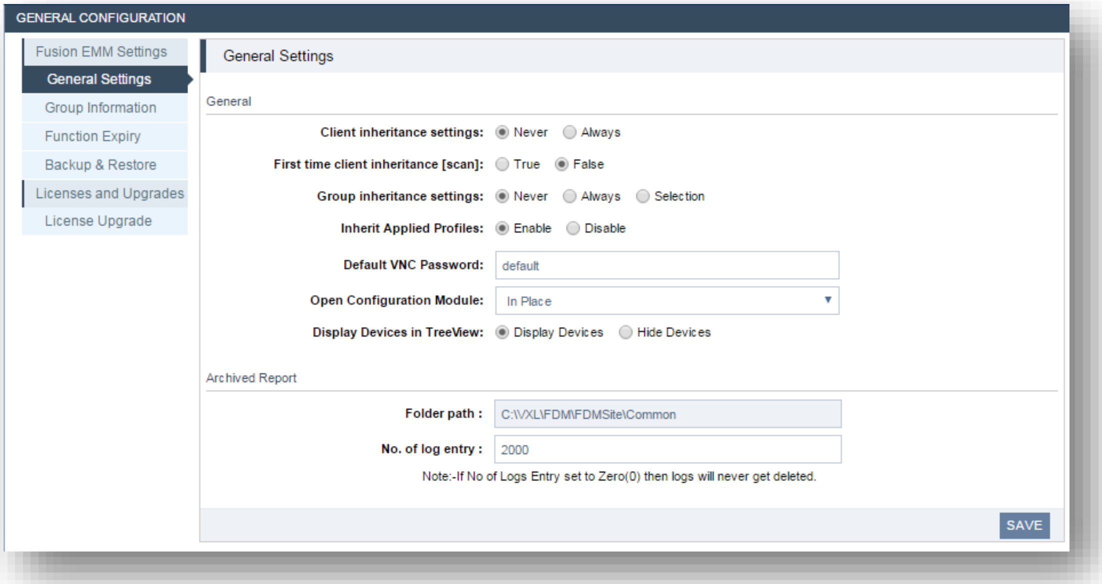
Working with General Configuration

General Configuration enables you to define configuration settings across the application.

Configuring Fusion EMM Settings

Working with General Details

1. Expand the right menu.
2. Click **Configuration Setup**, then click **General Configuration**, then click General Settings.
3. Form Displayed General settings, Archived Report.



General Settings

General

Client inheritance settings: ● Never ○ Always

First time client inheritance [scan]: ○ True ● False

Group inheritance settings: ● Never ○ Always ○ Selection

Inherit Applied Profiles: ● Enable ○ Disable

Default VNC Password: default

Open Configuration Module: In Place ▼

Display Devices in TreeView: ● Display Devices ○ Hide Devices

Archived Report

Folder path : C:\VXL\FDM\FDMSite\Common

No. of log entry : 2000

Note:-If No of Logs Entry set to Zero(0) then logs will never get deleted.

4. Change the general configuration details as required.

   a. **Client Inheritance Settings:** When user select Never after drag drop client not get inherit group settings' user select Always option, after drag drop all settings of parent group get inherit to client.

   b. **First time client Inheritance Settings:** For True option client which get scan after discovery settings defined for default group gets apply to client for Never option it won't get apply.

   c. In **Group Inheritance Settings**, if the **Always** option is selected, the application will not request confirmation when processing group inheritance.
      If the **Never** option is selected, the application will not process group inheritance.

   d. User able to set Default **VNC password.**

   e. **Open Configuration module (popup/In place):** While selection on popup all modules on device manager gets open in popup form or else all module displayed in place format.

   f. **Archived Report**: To set number of logs entries on specified path. While defined entry count displayed in logs data get purged on defined path location.

   g. **Inherit Applied Profiles: Enable/ Disable->** User have to add subgroup after enable selection to inherit parent group setting to subgroup.

      For Disable selection inherit property won't get apply to subgroup.

   h. **Display Devices in Tree View**: User able to Display Devices or Hide Devices from tree view by selecting respective options.

5. Click **Save**.

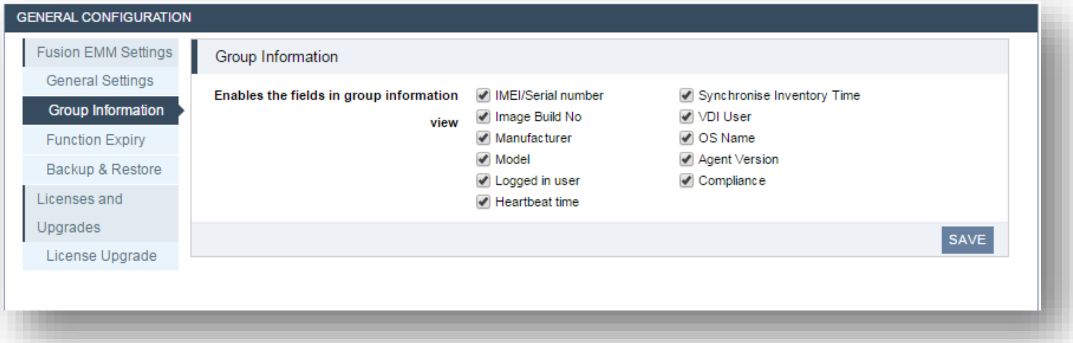
The **Settings applied successfully** message is display.

Working with Group Information

The **Group Information** tab enables you to select the fields to display in the group view on the **Device Manager** page.

To configure the group information

1. Expand the right menu.
2. Click **Configuration Setup**, then click **General Configuration**, click on Group Information.



Enables the fields in group information view

☑ IMEI/Serial number
☑ Image Build No
☑ Manufacturer
☑ Model
☑ Logged in user
☑ Heartbeat time
☑ Synchronise Inventory Time
☑ VDI User
☑ OS Name
☑ Agent Version
☑ Compliance

3. On the **Group Information** tab, select the applicable check boxes to define the fields for display.
4. Click **Save**.

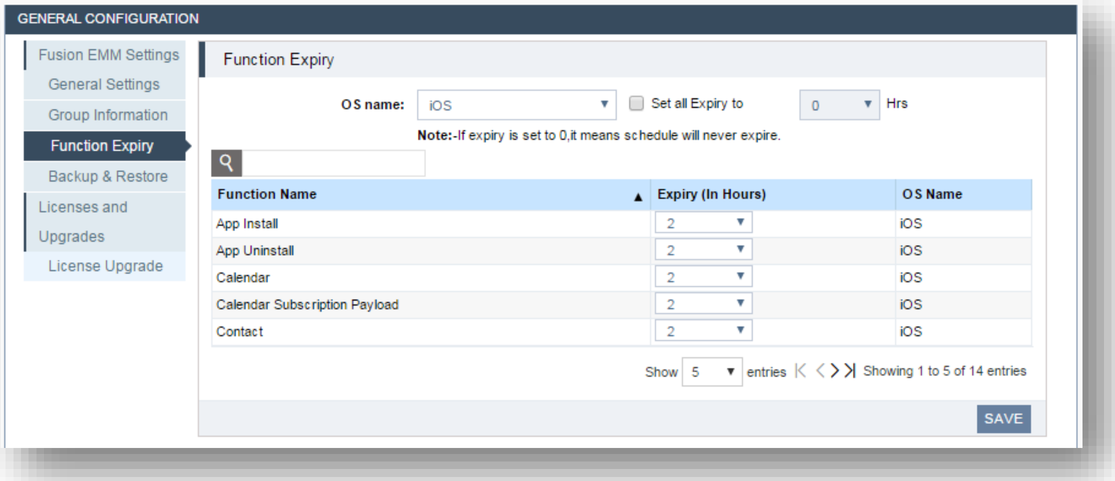
The **Settings applied successfully** message is display.

Working with Function Expiry

Function Expiry enables you to define the expiry time for a function. If the scheduled function is not executed within the defined time interval, the schedule is cancelled automatically.

To configure the function expiry time

1. Expand the right menu.
2. Click **Configuration Setup**, then click **General Configuration**, and then click **Function Expiry**.



OS name: iOS □ Set all Expiry to 0 Hrs

Note:-If expiry is set to 0,it means schedule will never expire.

Function Name	Expiry (In Hours)	OS Name
App Install	2	iOS
App Uninstall	2	iOS
Calendar	2	iOS
Calendar Subscription Payload	2	iOS
Contact	2	iOS

Show 5 entries Showing 1 to 5 of 14 entries

3. In the **OS name** list, select the operating system.
4. In **Enter Function Name**, enter the required function name.
5. Click **Search**.
6. In the **Expiry (in Hours**) column, in the text boxes for each function, enter the expiry time.
7. To set expiry for all functions, select the **Set All Expiry to** check box.
8. The text box to enter the expiry time (hours) is enabled.
9. Enter the expiry time.

- If expiry is set to 0, the schedule for the function will never be cancelled.
- By default, the function expiry of pending and in-process tasks is set to one hour and two hours respectively.
- Function expiry setting changed to allow predefined values from dropdown list to set expiry instead of textboxes.

10. Click **Save**.

The **Settings applied successfully** message is display.

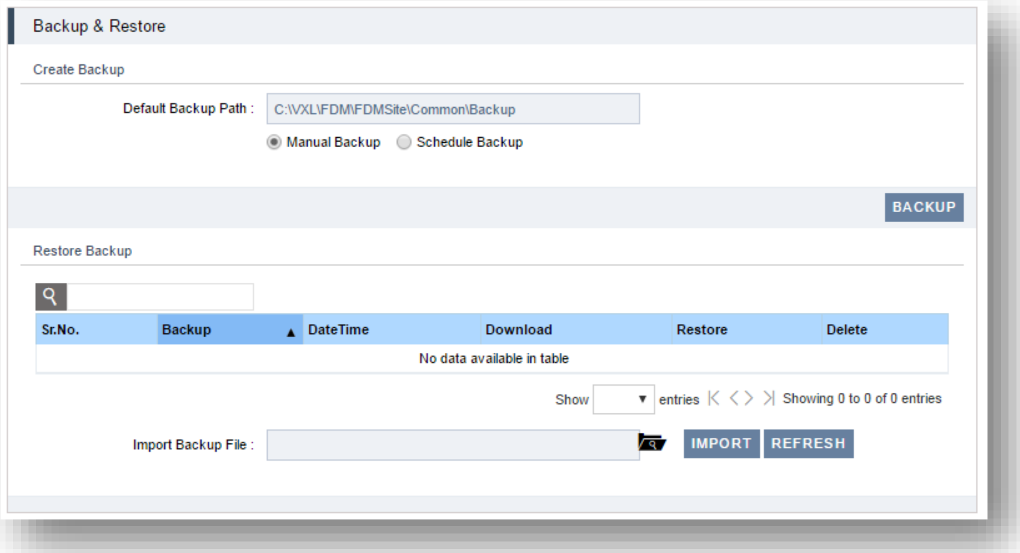
Working with Database Backup and Restore

Database Backup and Restore enables you to take a backup of the database and perform restore operations.

Creating a Database Backup

1. Expand the right menu.

2. Click **Configuration Setup**, then click **General Configuration**, click **Database Backup and Restore**.



Backup & Restore

Create Backup

Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

● Manual Backup ○ Schedule Backup

Restore Backup

Sr.No.	Backup	DateTime	Download	Restore	Delete
No data available in table					

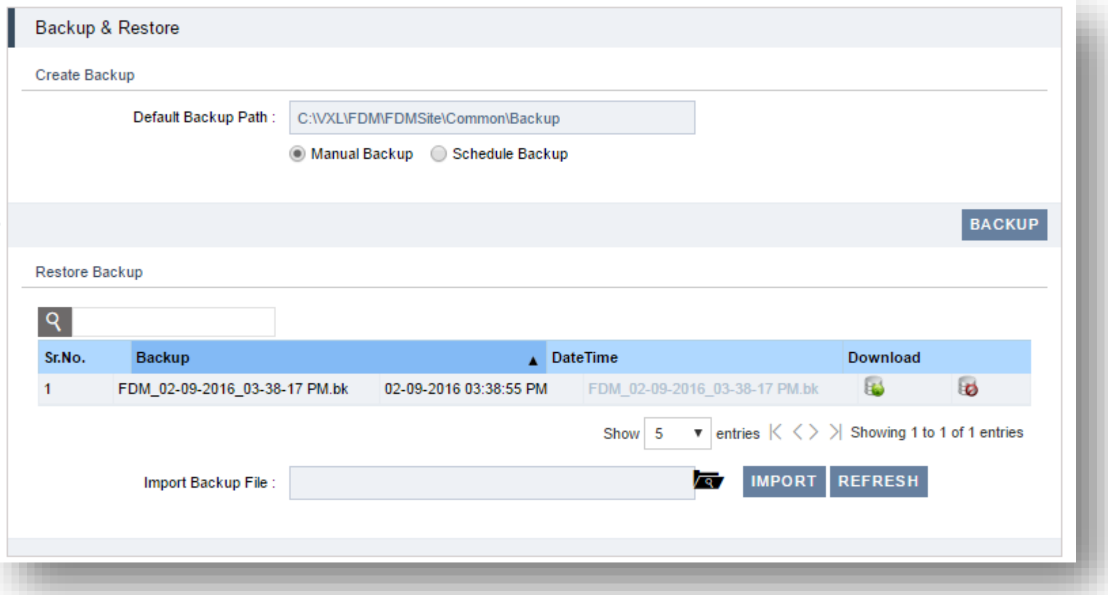
Show entries Showing 0 to 0 of 0 entries

Import Backup File :

3. Click **Backup**.

The **Database backup completed** message is display.

Importing a Backup File



Backup & Restore

Create Backup

Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

● Manual Backup ○ Schedule Backup

BACKUP

Restore Backup

Sr.No.	Backup		DateTime		Download	
1	FDM_02-09-2016_03-38-17 PM.bk	02-09-2016 03:38:55 PM		FDM_02-09-2016_03-38-17 PM.bk		

Show 5 entries Showing 1 to 1 of 1 entries

Import Backup File :

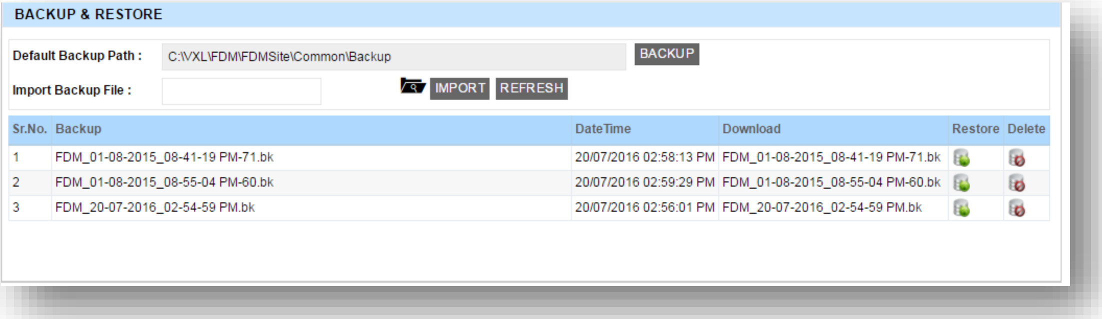
IMPORT REFRESH

1. Click 📂 .
2. Select the file to import.

   The message that the backup file is imported successfully is display.

Restoring the Database

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Database Backup and Restore**.



BACKUP & RESTORE

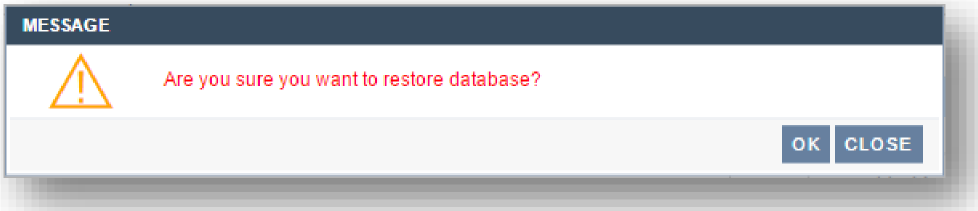
Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

Import Backup File :

Sr.No.	Backup	DateTime	Download	Restore	Delete
1	FDM_01-08-2015_08-41-19 PM-71.bk	20/07/2016 02:58:13 PM	FDM_01-08-2015_08-41-19 PM-71.bk		
2	FDM_01-08-2015_08-55-04 PM-60.bk	20/07/2016 02:59:29 PM	FDM_01-08-2015_08-55-04 PM-60.bk		
3	FDM_20-07-2016_02-54-59 PM.bk	20/07/2016 02:56:01 PM	FDM_20-07-2016_02-54-59 PM.bk		

3. In the **Restore** column, click .
4. **Are you sure you want to restore database?**

   Prompt is display.

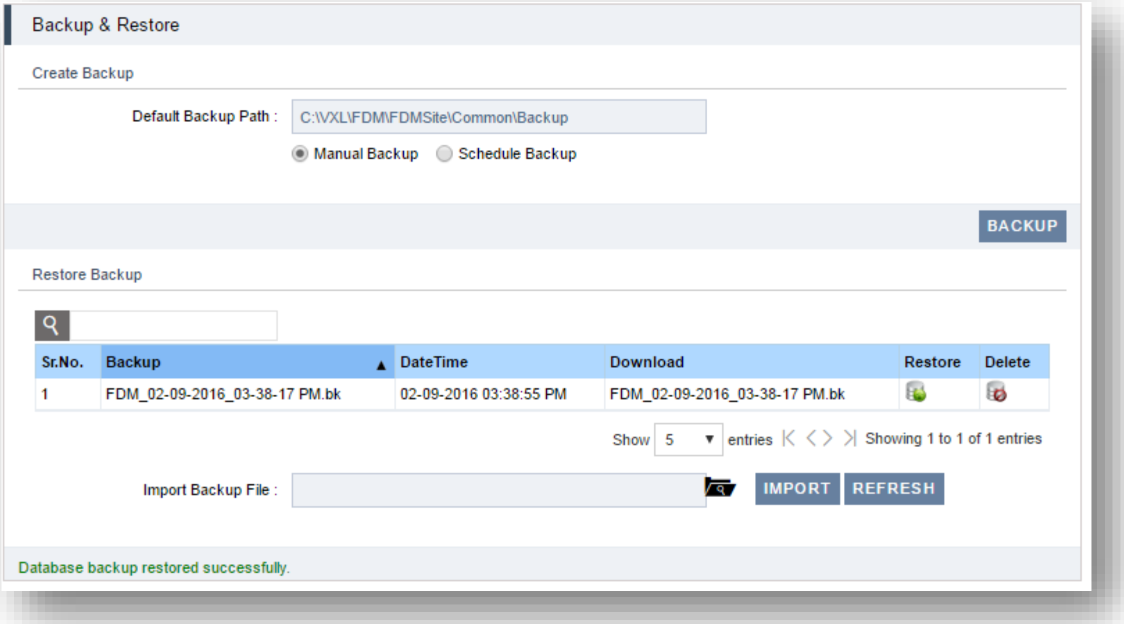


MESSAGE

Are you sure you want to restore database?

5. Click **OK**.

The **Database backup restored successfully** message is display.



Backup & Restore

Create Backup

Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

● Manual Backup ○ Schedule Backup

Restore Backup

Sr.No.	Backup	DateTime	Download	Restore	Delete
1	FDM_02-09-2016_03-38-17 PM.bk	02-09-2016 03:38:55 PM	FDM_02-09-2016_03-38-17 PM.bk		

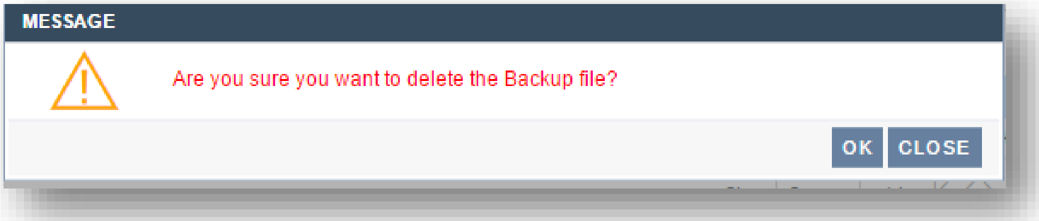
Show 5 entries Showing 1 to 1 of 1 entries

Import Backup File :

Database backup restored successfully.

Deleting a Backup File

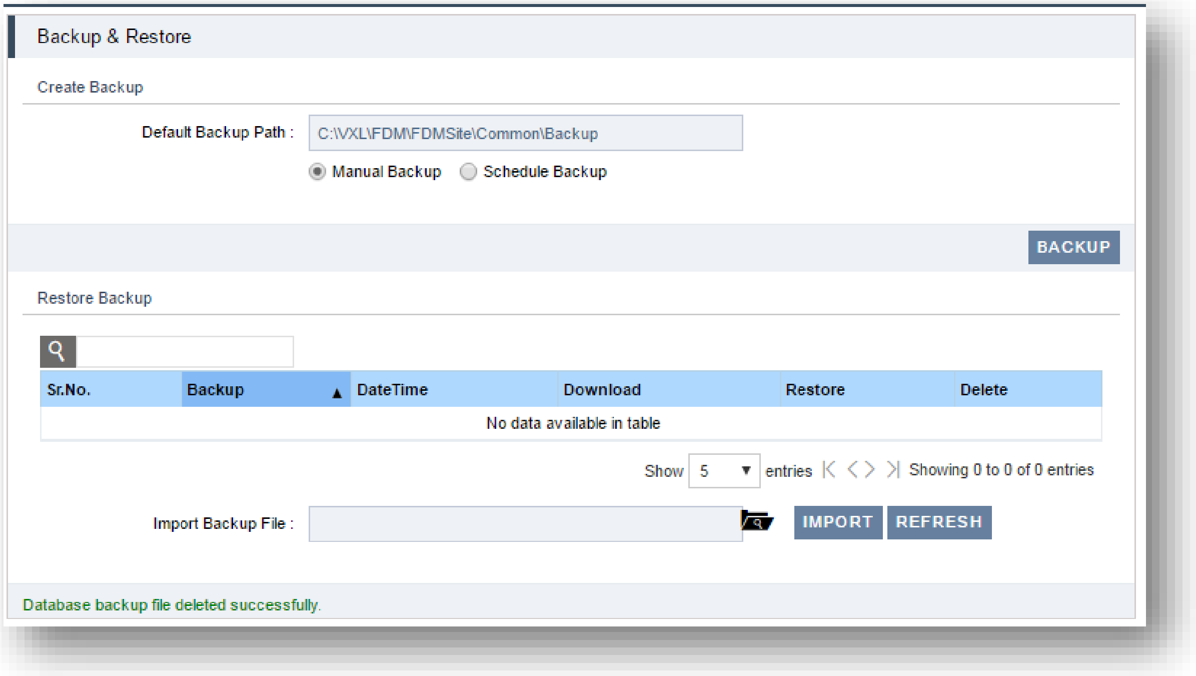
- In the **Delete** column, click .



MESSAGE

Are you sure you want to delete the Backup file?

The **Database backup file deleted successfully** message is display.



Backup & Restore

Create Backup

Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

● Manual Backup ○ Schedule Backup

Restore Backup

Sr.No.	Backup ▲	DateTime	Download	Restore	Delete
No data available in table					

Show 5 entries Showing 0 to 0 of 0 entries

Import Backup File :

Database backup file deleted successfully.

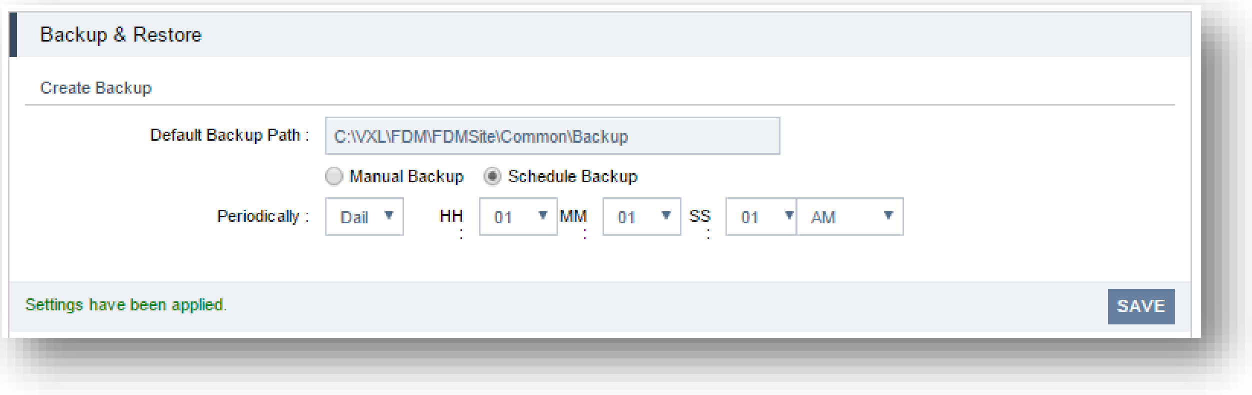
Working with Schedule Database Backup

Schedule Backup enables you to set up a periodic, automatic backup of the database.

To configure the auto-backup

1. Click Schedule Database Backup.
2. Under Automatic, select the frequency and time of the backup.
3. Click **Save**.

   The **Settings applied successfully** message is display.



Backup & Restore

Create Backup

Default Backup Path : C:\VXL\FDM\FDMSite\Common\Backup

○ Manual Backup ● Schedule Backup

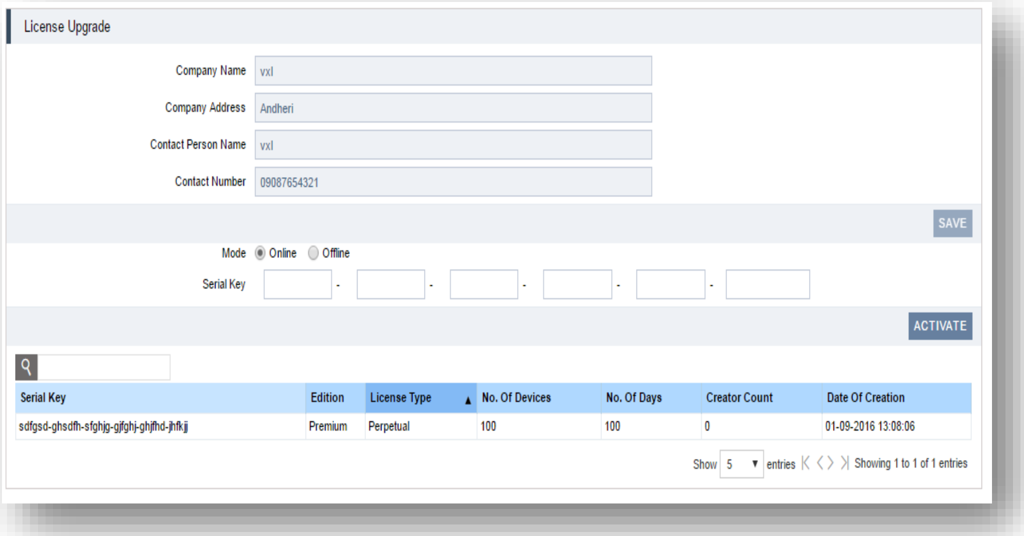
Periodically : Dail HH : 01 MM : 01 SS : 01 AM

Settings have been applied.

Configuring Licenses and Upgrades

Working with License Upgrade

1. Expand RHS Menu.
2. Click **Configuration Setup**, then click **General Configuration** and then click **License and Upgrade.**
3. Select **License Upgrade.**
4. User have to fill all company information with name, address, contact number, person name.
5. Click on SAVE.
6. Company information save successfully message displayed.
7. For licensing Online/ Offline two options displayed.
8. For online selection License team provide serial key for license activation.
9. Click on Activate.



License Upgrade

Company Name	vxl
Company Address	Andheri
Contact Person Name	vxl
Contact Number	09087654321

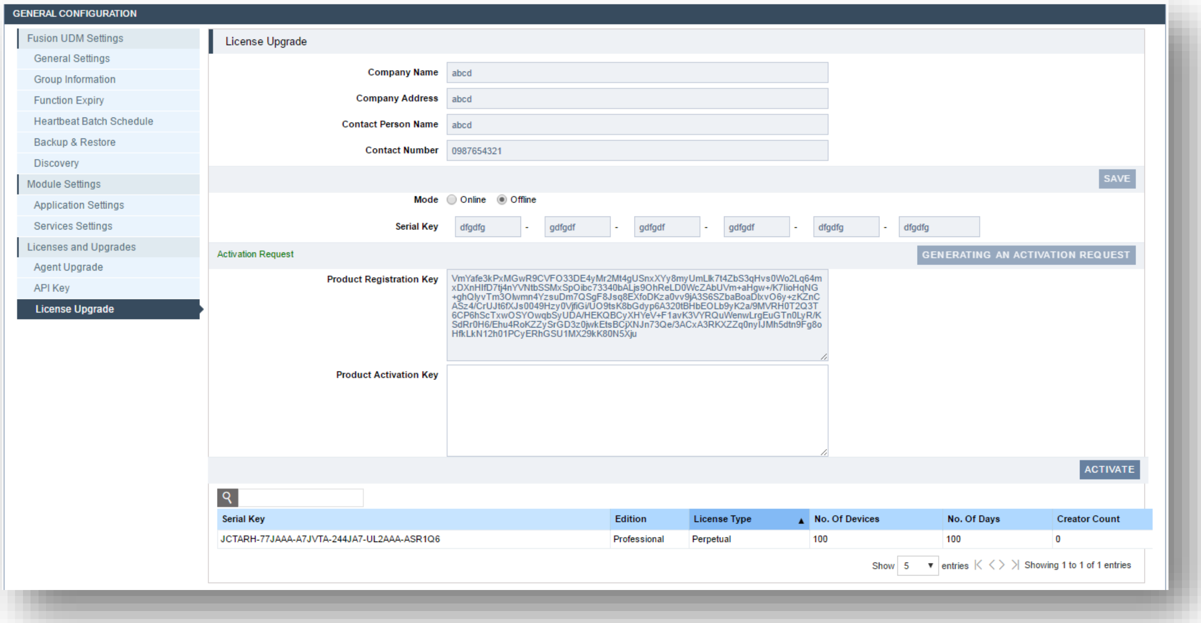
Mode ● Online ○ Offline

Serial Key

Serial Key	Edition	License Type	No. Of Devices	No. Of Days	Creator Count	Date Of Creation
sdfgsd-ghsdfh-sfghjg-gjfghj-ghjfhd-jhfkjj	Premium	Perpetual	100	100	0	01-09-2016 13:08:06

Show 5 entries Showing 1 to 1 of 1 entries

10. For Offline mode, user have to enter provided Serial key.
11. Click on Generating an Activation Request, Activation request message displayed.
12. Product registration key gets generate.
13. Provide Product Registration key to the license team, License team will revert back to you with Product Activation Key.
14. Enter Product Activation Key.
15. Click On ACTIVATE.
16. License upgrade successfully summary message displayed.



License Upgrade

Company Name: abcd

Company Address: abcd

Contact Person Name: abcd

Contact Number: 0987654321

Mode: ○ Online ● Offline

Serial Key: dfgdfg - gdfgdf - gdfgdf - gdfgdf - dfgdfg - dfgdfg

Activation Request

Product Registration Key:

```
VmYafe3kPxMGwR9CVFO33DE4yMr2Mt4gUSnxXYy8myUmLlk7t4ZbS3qHvs0Wo2Lq64m
xDXnHIfD7tj4nYVNtbSSMxSpOibc73340bALjs9OhReLD0WcZAbUVm+aHgw+/K7lioHqNG
+ghQlyvTm3Olwmn4YzsuDm7QSgF8Jsq8EXfoDKza0vv9jA3S6SZbaBoaDlxvO6y+zKZnC
ASz4/CrUJt6fXJs0049Hzy0VjfiGi/UO9tsK8bGdyp6A320tBHbEOLb9yK2a/9MVRH0T2Q3T
6CP6hScTxwOSYOwqbSyUDA/HEKQBCyXHYeV+F1avK3VYRQuWenwLrgEuGTn0LyR/K
SdRr0H6/Ehu4RoKZZySrGD3z0jwkEtsBCjXNJn73Qe/3ACxA3RKXZZq0nyIJMh5dtn9Fg8o
HfkLkN12h01PCyERhGSU1MX29kK80N5Xju
```

Product Activation Key:

Serial Key	Edition	License Type ▲	No. Of Devices	No. Of Days	Creator Count
JCTARH-77JAAA-A7JVTA-244JA7-UL2AAA-ASR1Q6	Professional	Perpetual	100	100	0

Show 5 ▾ entries |< < > >| Showing 1 to 1 of 1 entries

Discovering Devices

For devices to be managed, the first step is to discover and then enroll them for management within Fusion EMM .

Challenges faced in the discovery of network devices include:

- Multiplicity of devices with varied operating systems and categories.
- Multiplicity of network and device topologies, which control access to various network segments such as VLAN.

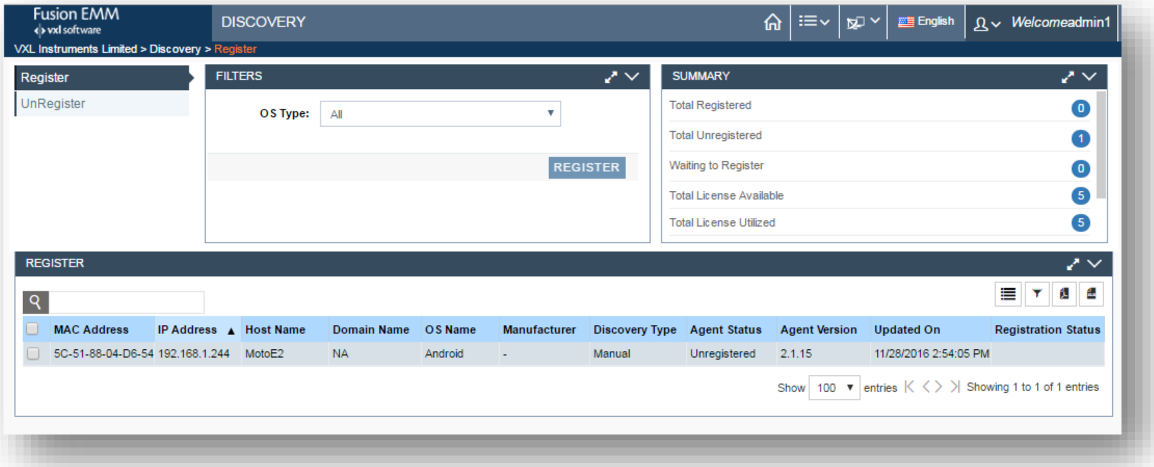
Fusion EMM has a range of different discovery methods that enable administrators to address these challenges.

To open the **DISCOVERY** page, on the toolbar, click 🔍

Filtering list of Devices

To filter the list of devices, click on ▼

1. Click on Add Filter button.



VXL Instruments Limited > Discovery > Register

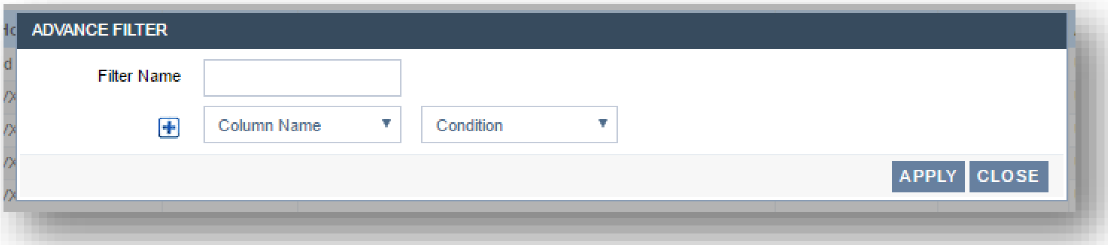
OS Type: All

SUMMARY	
Total Registered	0
Total Unregistered	1
Waiting to Register	0
Total License Available	5
Total License Utilized	5

□	MAC Address	IP Address ▲	Host Name	Domain Name	OS Name	Manufacturer	Discovery Type	Agent Status	Agent Version	Updated On	Registration Status
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2	NA	Android	-	Manual	Unregistered	2.1.15	11/28/2016 2:54:05 PM	

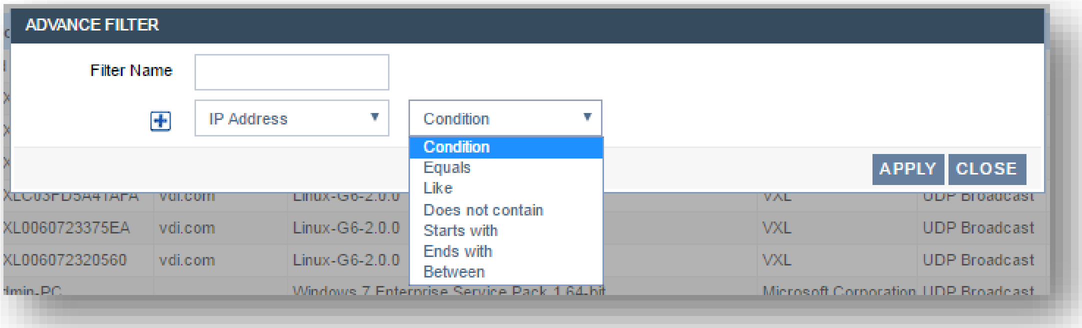
Show 100 entries Showing 1 to 1 of 1 entries

2. Advanced Filter form gets open.

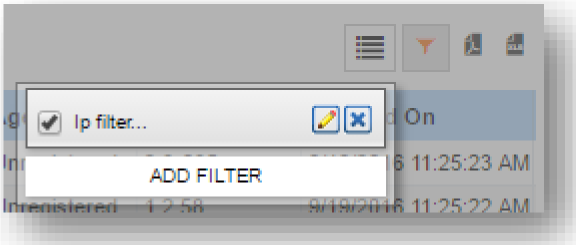


3. In which user, able to filter discovery data with column name with conditions apply.

4. According to column name selections conditions should get displayed.


ADVANCE FILTER
Filter Name
IP Address
Condition
Condition
Equals
Like
Does not contain
Starts with
Ends with
Between
APPLY
CLOSE
XLC03FD5A41AFA vdi.com Linux-G6-2.0.0 VXL UDP Broadcast
XL0060723375EA vdi.com Linux-G6-2.0.0 VXL UDP Broadcast
XL006072320560 vdi.com Linux-G6-2.0.0 VXL UDP Broadcast
dmin-PC Windows 7 Enterprise Service Pack 1 64-bit Microsoft Corporation UDP Broadcast

5. After creation of filter User have to select particular filter to see the result of created filter.



6. After apply filter, color gets change.

7. Click on Edit button to edit created filter.

8. Click on Delete icon to delete created or selected filter.

Discovering Devices

- All divices discovered by this methods is viewed in **Request Initiated** (count) on Register tab.
- Client available in agent initiated table will get listed in the tree view only after it is registered from server.

You can also discover devices by:

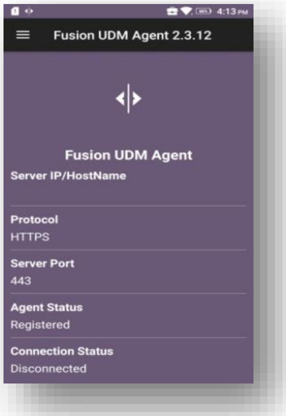
- Manual Device Configuration

Discovering Devices by Manual Device Configuration

The administrator can configure agent settings such as server IP address, port number, group name, heartbeat interval, communication type, on a registered device manually.

To configure the Android agent settings:

- On Agent window left side menu, open the app drawer. Go to **Settings**.
- On opening the Settings page, a prompt for password will be shown.
- By default, the password is "default". (User can change this password from Fusion EMM server > Agent Settings.)
- In Settings page, enter the required details in Remote Server IP/Name, Protocol, Server Port No., and Heartbeat Interval.
- Agent Status & Connection Status values will be shown below.



Server IP/HostName

Protocol
HTTPS

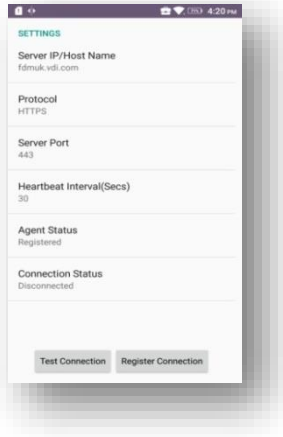
Server Port
443

Agent Status
Registered

Connection Status
Disconnected

- Click on **Test Connection** button to test connection with the server.
- Once the connection is successful with the server, a message is displayed "**Test Connection Successful**" and the certificate is silently installed on the device.
- Now, click on Register Connection button to send a registration request to the server.

- On successful registration, a message is displayed “**Connected to the server successfully**”.



SETTINGS

Server IP/Host Name
fdmuk.vdi.com

Protocol
HTTPS

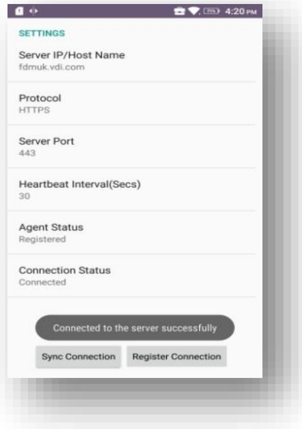
Server Port
443

Heartbeat Interval(Secs)
30

Agent Status
Registered

Connection Status
Disconnected

- Once registration with the server is successful, **Sync Connection** button will appear.
- Now, the client is listed in request initiated section, which needs to be approved on the server.
- Connection Status of the agent will also be displayed in the notification bar on the device.



SETTINGS

Server IP/Host Name
fdmuk.vdi.com

Protocol
HTTPS

Server Port
443

Heartbeat Interval(Secs)
30

Agent Status
Registered

Connection Status
Connected

Connected to the server successfully

Registering Devices

To quickly filter the list, in the **SUMMARY** pane, click the number against the required filter category.

The filter categories are as follows:

- **Total Registered**: The number of all discovered devices
- **Total UnRegistered**: Number of devices registered in *Fusion EMM*
- **Waiting To Register**: Number of devices not registered in *Fusion EMM*
- **Total License Available**: Number of devices with no agent installed
- **Total License Utilized**: Populate the details of MAC address.
- **Total License Acquired**: Number of license purchased
- **Request Initiated**: Number of manually requested devices

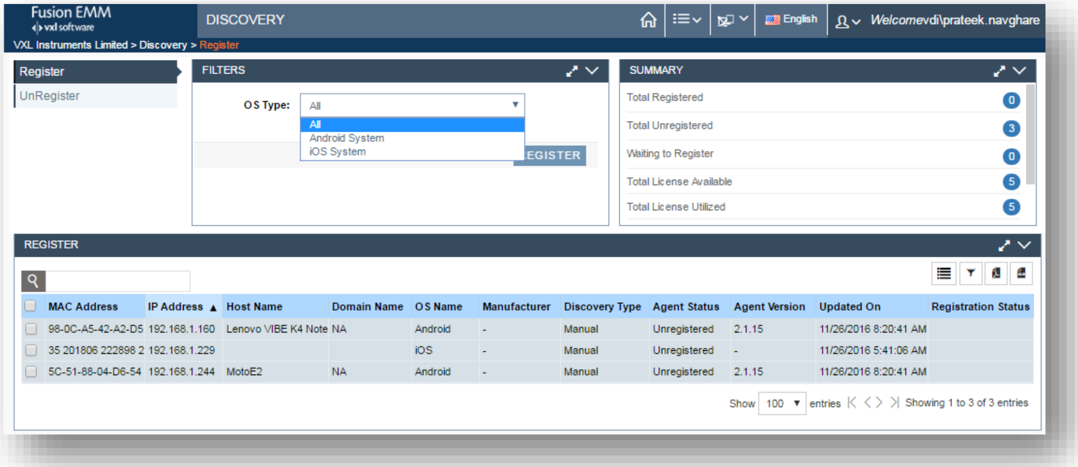
The **Registe**r function registers single or multiple devices with the Fusion EMM software on which the agent is installed.

In filter option for register, there are three options:

1. Agent initiated discovery indicates devices which are listed in Request Initiated (count) on Register tab.
2. Default option is ALL in which all the Android & iOS clients get listed.
3. Agent initiated devices differentiated by colour code.

To register the unregistered devices on the server:

1. In the left menu, click **Register.**
2. In the filter pane, devices can be filter out according to **Source** and **OS Type**.
3. Select the device and Click **Register.**
4. A message **Request for registration of 1 device(s) is sent.**



OS Type: All

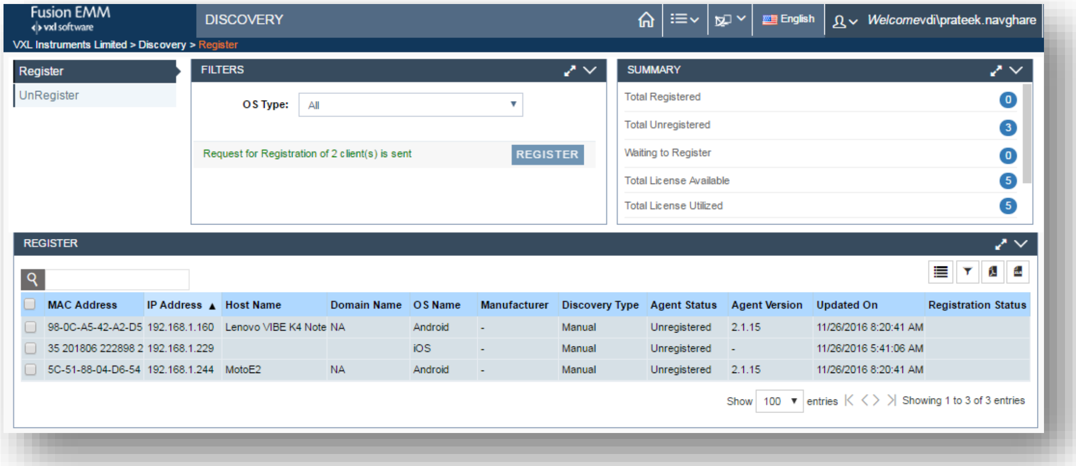
- All
- Android System
- iOS System

SUMMARY	
Total Registered	0
Total Unregistered	3
Waiting to Register	0
Total License Available	5
Total License Utilized	5

□	MAC Address	IP Address ▲	Host Name	Domain Name	OS Name	Manufacturer	Discovery Type	Agent Status	Agent Version	Updated On	Registration Status
□	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	NA	Android	-	Manual	Unregistered	2.1.15	11/26/2016 8:20:41 AM	
□	35 201806 222898 2	192.168.1.229			iOS	-	Manual	Unregistered	-	11/26/2016 5:41:06 AM	
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2	NA	Android	-	Manual	Unregistered	2.1.15	11/26/2016 8:20:41 AM	

Show 100 entries Showing 1 to 3 of 3 entries

5. Wait for a few minutes. The **Agent Status** will change to **Registered**.
6. If the server is unable to send the registration request to a selected IP, **the Request for registration of 1 client(s) failed** message is display.
7. If due to any exception the agent cannot be registered with the Fusion EMM server, the **Agent Status** column displays a **Waiting to register** message and the device is listed in the summary.
8. While registering client, when Agent status is **Waiting to registered**, check **Registration status** for registration progress on device. Below table displaying many more status and their scenarios.
9. Administrator can remove the devices, which are not communicating with the server by selecting devices and perform delete operation.



OS Type: All

Request for Registration of 2 client(s) is sent

SUMMARY	
Total Registered	0
Total Unregistered	3
Waiting to Register	0
Total License Available	5
Total License Utilized	5

□	MAC Address	IP Address ▲	Host Name	Domain Name	OS Name	Manufacturer	Discovery Type	Agent Status	Agent Version	Updated On	Registration Status
□	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	NA	Android	-	Manual	Unregistered	2.1.15	11/26/2016 8:20:41 AM	
□	35 201806 222898 2	192.168.1.229			iOS	-	Manual	Unregistered	-	11/26/2016 5:41:06 AM	
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2	NA	Android	-	Manual	Unregistered	2.1.15	11/26/2016 8:20:41 AM	

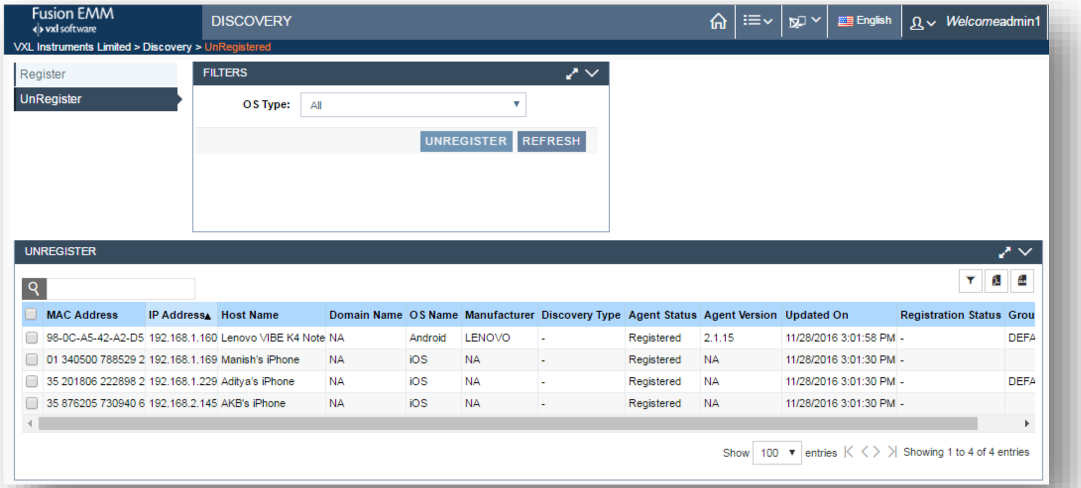
Show 100 entries Showing 1 to 3 of 3 entries

Android:			
ID	Scenario	Result	Status
1	Add client into invalid server and try to register through the device.	FAIL	Error 30: SSL Connection to server failed.

10. Fusion EMM server provides demo license for 10 devices, If registration of devices exceeds more than the demo license show validation message.

Unregistering Devices

1. List of the devices registered to the FDM sever get listed in the **UNREGISTER** tab.
2. In Filter pane, devices can be filter according to OS type.
3. When user select device, and click on **UNREGISTER.**
4. **Device Unregistered successfully** summary message displayed and client get remove from list.
5. **Group name column also added in Unregister table.**
6. Agent status gets change to **Unregister**.



OS Type: All

☐	MAC Address	IP Address▲	Host Name	Domain Name	OS Name	Manufacturer	Discovery Type	Agent Status	Agent Version	Updated On	Registration Status	Grou
☐	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	NA	Android	LENOVO	-	Registered	2.1.15	11/28/2016 3:01:58 PM	-	DEFA
☐	01 340500 788529 2	192.168.1.169	Manish's iPhone	NA	iOS	NA	-	Registered	NA	11/28/2016 3:01:30 PM	-	
☐	35 201806 222898 2	192.168.1.229	Aditya's iPhone	NA	iOS	NA	-	Registered	NA	11/28/2016 3:01:30 PM	-	DEFA
☐	35 876205 730940 6	192.168.2.145	AKB's iPhone	NA	iOS	NA	-	Registered	NA	11/28/2016 3:01:30 PM	-	

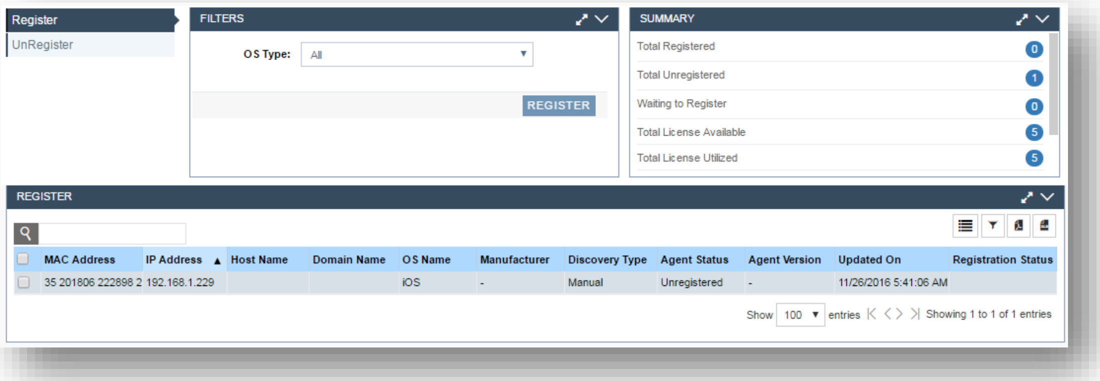
Show 100 entries Showing 1 to 4 of 4 entries

Performing Common Operations

Sorting Data in a Column

You can sort the data displayed in the table in on any column The **View** feature has been used as an example.

You can sort similarly sort the data in the **Register and Unregister** views.



Register
UnRegister

FILTERS

OS Type: All

REGISTER

SUMMARY

Total Registered	0
Total Unregistered	1
Waiting to Register	0
Total License Available	5
Total License Utilized	5

REGISTER

□	MAC Address	IP Address ▲	Host Name	Domain Name	OS Name	Manufacturer	Discovery Type	Agent Status	Agent Version	Updated On	Registration Status
□	35 201806 222898 2	192.168.1.229			iOS	-	Manual	Unregistered	-	11/26/2016 5:41:06 AM	

Show 100 entries Showing 1 to 1 of 1 entries

To sort data in ascending or descending order, in the required column’s header, click ▲ or ▼.

Exporting Data to PDF or Excel

You can also export the data displayed in the table to PDF or Excel.

For information about exporting data to PDF or Excel, see “Performing Common Operations” in” Getting Started”.

Configuring Mobile Device Management

Configuring Setup for Android Device

MDM is a way to ensure employees stay productive and do not breach corporate policies. Many organizations control activities of their employees using MDM products/services. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on device, enforcing corporate policies, integrating and managing mobile devices including laptops and handhelds of various categories. MDM implementations may be either on-premises or cloud-based.

MDM functionality can include over-the-air distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smart phones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, etc. Most recently, laptops and desktops have been added to the list of systems supported, as Mobile Device Management becomes more about basic device management and less about the mobile platform itself. MDM tools are leveraged for both company-owned and employee-owned (BYOD) devices across the enterprise or mobile devices owned by consumers. Consumer Demand for BYOD is now requiring a greater effort for MDM and increased security for both the devices and the enterprise they connect to, especially since employers and employees have different expectations on the type of restrictions that should be applied to mobile devices.

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of a mobile communications network while minimizing cost and downtime.

With mobile devices becoming ubiquitous and applications flooding the market, mobile monitoring is growing in importance. Numerous vendors help mobile device manufacturers, content portals and developers, test and monitor the delivery of their mobile content, applications and services. This testing of content is done real time by simulating the action of thousands of customers and detecting and correcting bugs in the applications.

MDM for mobile security

All MDM products are built with an idea of Containerization. The MDM Container is secured using latest crypto techniques (AES-256 or more preferred). All the corporate data like email, documents, enterprise application are encrypted and processed inside the container. This ensures that corporate data is separated from user's personal data on the device. Additionally, encryption for entire device and/or SD Card can also be enforced depending on MDM product capability.

Secure email: MDM products allow organization to integrate their existing email setup to be easily integrated with MDM environment. This provided flexibility of configuring Email-over-air. Secure Docs: It is frequently seen that, employees copy attachments downloaded from corporate email to their personal devices and then misuse it. MDM can easily restrict/disable clipboard usage in/out of Secure Container; forwarding attachments to external domains can be restricted, downloading/saving attachments on SD Card. This ensures corporate data is not left insecure.

Secure browser: Using secure browser can avoid many potential security risks. Every MDM solution comes with built-in custom browser. Administrator can disable native browsers to force user to use Secure Browser, which is also inside the MDM container. URL filtering can be enforced to add additional productivity measure.

Secure app catalogue: Organization can distribute, manage, and upgrade applications on employee's device using App Catalogue. It allows applications to be pushed on user device directly from the App Store or push an enterprise developed private application through the App Catalogue. This provides an option for the organization to deploy devices in Kiosk Mode or Lock-Down Mode.

Additional MDM features

There are plenty of other features depending on which MDM product is chosen:

- Policy Enforcing: There are multiple types of policies which can be enforced on MDM users.
  - Personal Policy: According to corporate environment, highly customizable.
  - Device Platform specific: policies for advanced management of Android, IOS, Windows and Blackberry devices.
  - Compliance Policies/Rules
- VPN configuration
- Application Catalogue
- Pre-defined Wi-Fi and Hotspot settings
- Jailbreak/Root detection
- Remote Wipe of corporate data
- Remote Wipe of entire device
- Device remote locking
- Remote messaging/buzz
- Disabling native apps on device

EMM Configuration

Enterprise Mobility Management (EMM)

The Android for Work application sharing and authentication framework is designed for mobile enterprise environments to provide seamless device and app management for enterprise devices - for mixed personal or corporate-only use. With new Android mobile management capabilities integrated with existing EMM solutions, Android for Work Managed Profiles are easily configured and provisioned by the respective EMM's device policy controller app, to separate and provide a strong boundary between personal and corporate apps. Device and profile scoped policies and Work apps are remotely distributed from the authorized EMM console registered with Google Play, authorized on behalf of their enterprise customers.

To integrate with Android for Work and receive approval to launch a production Android for Work solution, interested EMM prospects should join the EMM community to become an EMM community participant.

Solution sets

The Android for Work community offers flexible integration options that suit a variety of use cases, all of which are implementations of the following Android for Work solution sets:

- Work Profile
- Work Managed Device
- COSU
- MAM
- EMM participants must meet the requirements of at least one of these solutions sets.

Work Profile

1. Enabling a work profile allows organizations to manage the business data and applications they care about, but leave everything else on a device under the user's control. Administrators control work profiles, which are kept separate from personal accounts, apps, and data. Work profiles allow an IT department to securely manage a work environment without restricting users from using their device for personal apps and data.

2. By default, work profile notifications and app icons have a red briefcase so they’re easy to distinguish from personal apps.

3. To set up a work profile you must have your Enterprise Mobility Management (EMM) provider’s **controller application** installed on your device. Your EMM provider will supply you with the latest application. The device policy controller sets up the work profile on Android 5.0+ devices. On Android 4.0–4.4 devices, the device policy controller prompts users to install the Android for Work App to separate the personal and work space on their device.

BYOD

1. BYOD is short for Bring Your Own Device.
2. In the consumerization of IT, BYOD, or bring your own device, is a phrase that has become widely adopted to refer to employees who bring their own computing devices – such as smartphones, laptops and tablets – to the workplace for use and connectivity on the secure corporate network.
3. A BYOD policy can take many different forms. Some organizations cut back on corporate-issued PCs and laptops, instead giving employees a stipend to purchase and maintain technology equipment of their choosing, rules in a BYOD policy often vary depending on a user’s role in the organization, his or her specific device, application requirements and other factors.
4. BYOD (bring your own device) is the increasing trend toward employee-owned devices within a business. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace.
5. Employee-owned devices are sometimes sanctioned by the company and supported alongside devices that are owned by the business. In other cases, employee-owned devices are part of the parallel system known as shadow IT: hardware or software within an enterprise that is not supported by the organization’s central IT department.
6. Whether employee-owned hardware and software are supported or not, they pose security risks to the organization if they connect to the corporate network or access corporate data. To minimize the risk and accommodate consumer technologies, many businesses are implementing BYOD policies.
7. Advantages

- Lower Costs – The most obvious benefit to a company using BYOD is that it means they don't have to purchase a significant amount of costly devices in order for employees to be able to do eLearning.
- Technology Familiarity – Most people tend to be familiar with their own devices.

Technology Overview

Android for Work on Lollipop relies on four major components:

1. A Managed Profile, inside of which is installed an EMM's Device Policy Client (DPC) and a Managed Play Store Client, for communications with EMM policy servers and the Play for Work cloud, respectively. The Managed Profile contains the "Work" applications and data and is separated from the user's personal space in a managed work profile scenario.

2. A Managed Google Domain, which allows a customer to access Google Play for Work in order to manage application distribution to users included a customer's domain. It allows creation of Managed Google Accounts (e.g. user@customer.com) for corporate users which are used to log into the Managed Google Play Client and other Google services in a Managed Profile.

3. Play for Work, which is a managed version of the Play Store that is tied to a company's Managed Google Domain. From here, an IT admin can choose applications to approve for domain-wide distribution, purchase licenses in bulk for paid applications, and set up internal applications for distribution.

4. An EMM Partner, which provides the management layer for applying policies and actions to devices enrolled in Android for Work. In addition, the EMM pulls domain application data from Play for Work and provides a pane for distribution of approved applications to the Managed Play Client on target devices.

Managed Profile

User profiles are an existing feature of the Android platform. Jelly Bean (4.2) introduced the concept of multiple users and profile switching to Android, and the Managed Profile is built on top of this idea. A Lollipop device can simultaneously contain two profiles: a personal, unmanaged profile and the Managed Profile. Both profiles are associated with discrete, SELinux-backed user accounts. Versus the multiple profile support model from previous versions of Android, Android for Work in Lollipop introduces two new abilities:

1. Both profiles are simultaneously logged in

2. One of the profiles (the Managed Profile) contains an EMM DPC to enforce policies specified by the enterprise.

Because both profiles are logged in at once, the user never needs to explicitly log out of the personal profile to access the Managed Profile (or vice versa)

Profile Owner vs. Device Owner

With the profiles model, Android for Work can scale to either BYOD or corporate-liable (CL) use cases. The EMM DPC will only reside in the Managed Profile, and will thus only be able to enforce policies within that context. The scope of the Managed Profile context depends on whether a personal account exists on the device.

Corporate-liable Use Case

If the Managed Profile is the only profile on the device (i.e. if it was the first profile set up at initial boot of the device), it is designated as a Work Managed Device, and the EMM DPC is designated the Device Owner. The entire device will effectively be scoped to EMM control. In this use case, the admin will be able to erase the entire device and control device level settings (such as disallowing factory reset and USB tethering).

BYOD Use Case

For BYOD or mixed-use scenarios, the user will have two profiles on the device. One will be associated with a personal Google account, while the Managed Profile will be tied to the Managed Google Account.

Data Separation

Each profile is backed by its own data store on the device's internal storage, and the two data stores cannot directly access one another. The Android OS determines which data store an application should be accessing by evaluating the context in which it is running.

For example, if a user launches the badged Chrome icon, all application data for Chrome (bookmarks, settings, etc.) will come from the Managed Profile's data store. However, if the user launches the unbadged, personal Chrome instance, the application will not be allowed access to any of the Chrome data in the managed data store.

It is important to note that there do not have to be multiple copies of the same APK installed on each profile in this model. Even if an application is present in both profiles, the OS will use a single APK and allow that APK to access the appropriate data store based on context.

Configuration Setup for Google MDM

In general, the EMM console is the mechanism through which an enterprise manages its entire mobile fleet (platform-agnostic). This will also be the place that a customer's IT admin goes to manage policies for Android for Work. Policy files are generated by the EMM console and sent down to the device-side DPC, which will then enforce the policies within the Managed Profile.

AFW EMM ENROLMENT

Android for work enrollment can be done using two different accounts.

1. Android for Work Account

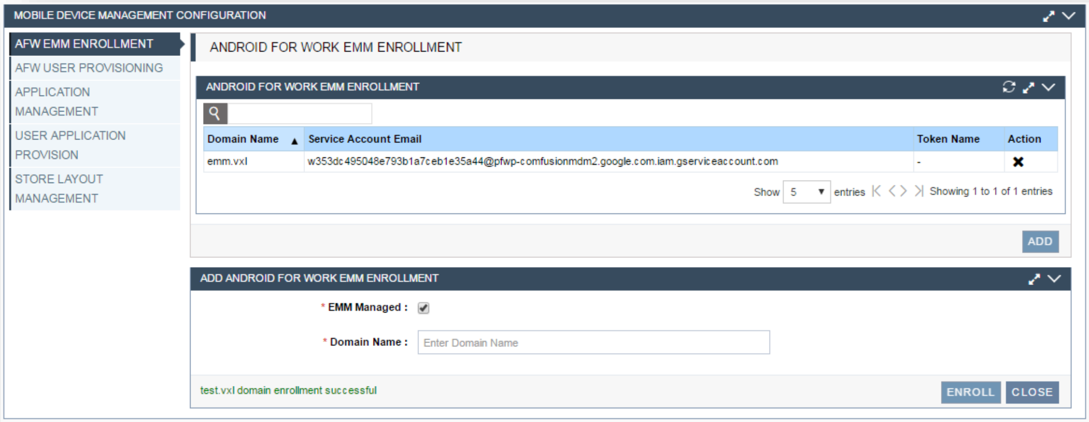
2. Google Account

Android for Work accounts:

Customer can have as many Android for Work Accounts enterprises as they need, for example one per region or department. An administrator initiates the process of creating an enterprise, and you bind the enterprise to your Android for Work solution.

Steps for AFW EMM enrollment using Google account:

1. Select Configuration Setup -> Google MDM Configuration.
2. Select **AFW EMM Enrollment**.
3. Click on **Add**.
4. Check the **EMM Managed** checkbox.


MOBILE DEVICE MANAGEMENT CONFIGURATION
AFW EMM ENROLLMENT
AFW USER PROVISIONING
APPLICATION MANAGEMENT
USER APPLICATION PROVISION
STORE LAYOUT MANAGEMENT
ANDROID FOR WORK EMM ENROLLMENT
ANDROID FOR WORK EMM ENROLLMENT
ADD
ADD ANDROID FOR WORK EMM ENROLLMENT
ENROLL
CLOSE

Domain Name ▲	Service Account Email	Token Name	Action
emm.vxl	w353dc495048e793b1a7ceb1e35a44@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖

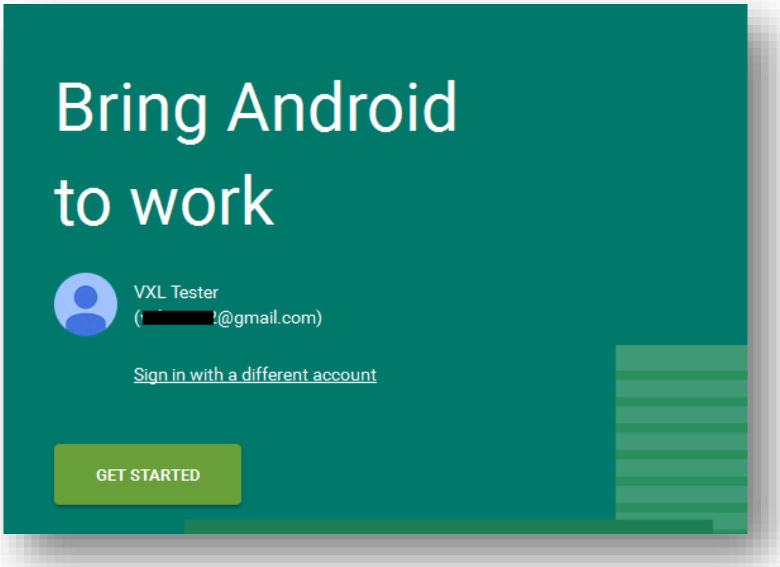
Show 5 ▼ entries Showing 1 to 1 of 1 entries

* EMM Managed : ☑

* Domain Name : Enter Domain Name

test.vxl domain enrollment successful

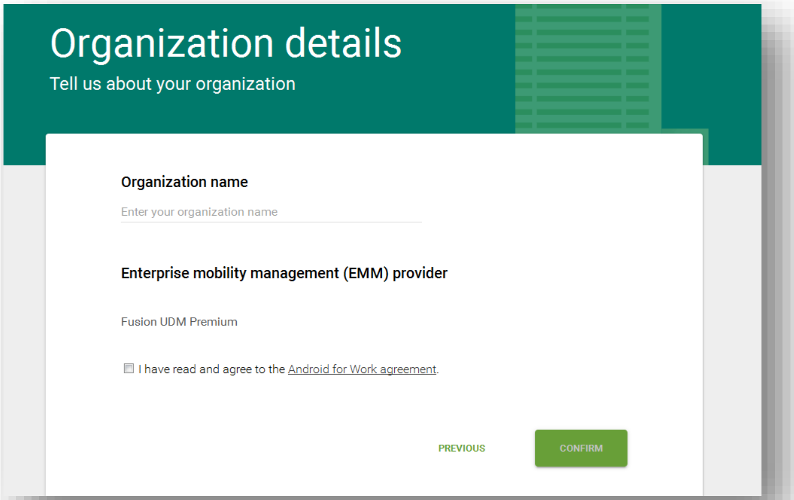
5. Enter **Domain name.**
6. Click on **Enroll**.
7. User is redirected to an Android for Work sign-up UI hosted by Google Play.



Bring Android to work

VXL Tester
([redacted]@gmail.com)

8. Provide the details about the enterprise in the sign-up UI page.

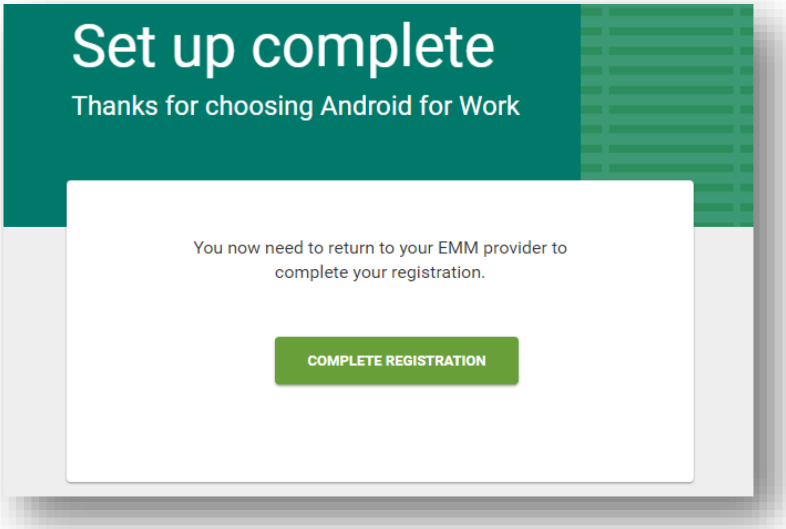


Organization details
Tell us about your organization

Organization name
Enter your organization name

Enterprise mobility management (EMM) provider
Fusion UDM Premium

□ I have read and agree to the Android for Work agreement.

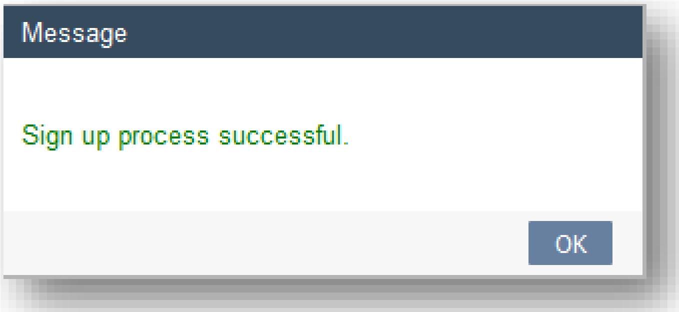


Set up complete

Thanks for choosing Android for Work

You now need to return to your EMM provider to complete your registration.

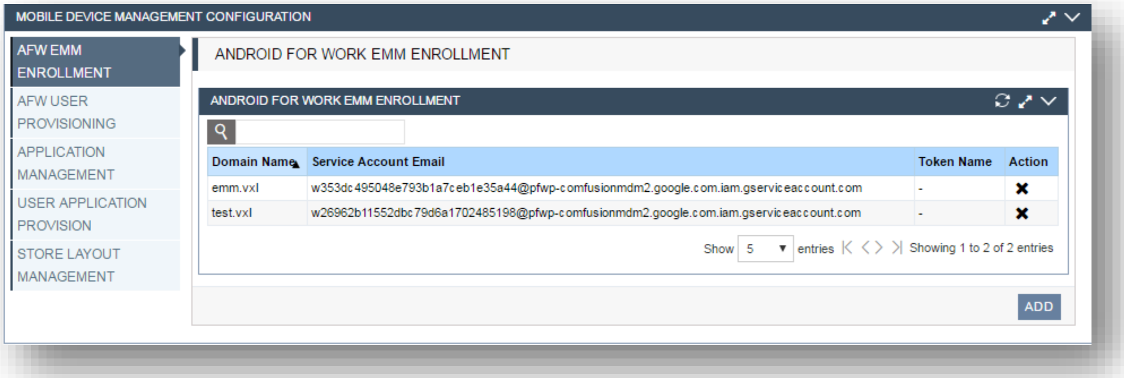
9. Once the sign-up process is completed successfully, a popup is shown with the successful message.



Message

Sign up process successful.

10. The service account gets enrolled.
11. Click **Reload** button to update the domain list.



ANDROID FOR WORK EMM ENROLLMENT

ANDROID FOR WORK EMM ENROLLMENT

Domain Name	Service Account Email	Token Name	Action
emm.vxl	w353dc495048e793b1a7ceb1e35a44@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖
test.vxl	w26962b11552dbc79d6a1702485198@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖

Show 5 entries Showing 1 to 2 of 2 entries

12. You can also delete an existing account by clicking on Delete button next to it.

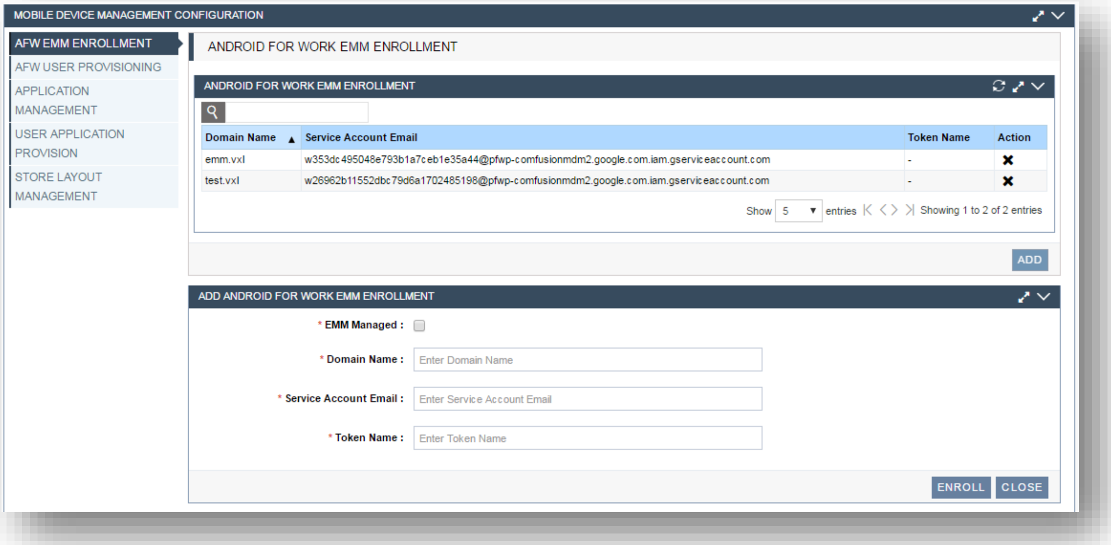
Google accounts:

It's the process of domain binding with MDM as required details for enrollment like Domain Name Service account email, Token, Server JSON, Client JSON, Client secret key, API key, Project ID store which would be obtain by following the process defined in the Installation Guide.

Steps for AFW EMM enrollment using Google account:

1. Select Configuration Setup -> Google MDM Configuration.
2. Select **AFW EMM Enrollment**.
3. Click on **Add**.
4. Uncheck the **EMM Managed** checked.
5. Enter **Domain name**, **Service Account Email** and **Token name**.
6. Click on **Enroll**.
7. The service account gets enrolled.

   You can also delete an existing account by clicking on Delete button next to it.



ANDROID FOR WORK EMM ENROLLMENT

ANDROID FOR WORK EMM ENROLLMENT

Domain Name ▲	Service Account Email	Token Name	Action
emm.vxl	w353dc495048e793b1a7ceb1e35a44@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖
test.vxl	w26962b11552dbc79d6a1702485198@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖

Show 5 ▾ entries Showing 1 to 2 of 2 entries

ADD ANDROID FOR WORK EMM ENROLLMENT

* EMM Managed :	□
* Domain Name :	Enter Domain Name
* Service Account Email :	Enter Service Account Email
* Token Name :	Enter Token Name

You can configure an existing account by clicking on Configure button next to it.

The following details are to be entered for configuration:

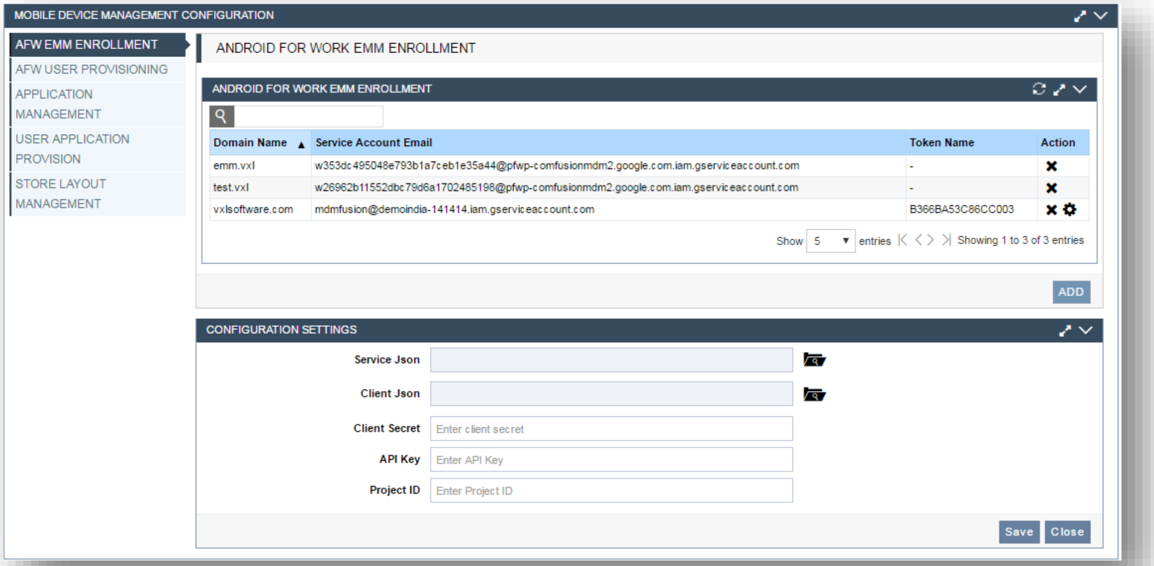
1. **Service Json**: A service account represents a Google Cloud service identity. A .json file of enrolled domain is to be uploaded.
2. **Client Json**: Service account clients are created when domain-wide delegation is enabled on a service account. A .json file of enrolled domain is to be uploaded.

3. **Client secret**: OAuth2 uses the client secret mechanism as a means of authorizing a client. It acts as a secret passphrase that proves to the authentication server that the client app is authorized to make a request on behalf of the user.
4. **API Key**: You need an API key to call certain Google APIs. The API key identifies your project.
5. **Product ID**: The ID of the project that owns the service account.

Steps for configuring the service account:

1. Click the **Configuration** button.
2. Upload the **Service json** file.
3. Upload the **Client json** file.
4. Enter the **Client secret key**, **API key** and **Product ID**.

   Settings saved successfully message is displayed.


MOBILE DEVICE MANAGEMENT CONFIGURATION
AFW EMM ENROLLMENT
AFW USER PROVISIONING
APPLICATION MANAGEMENT
USER APPLICATION PROVISION
STORE LAYOUT MANAGEMENT
ANDROID FOR WORK EMM ENROLLMENT
ANDROID FOR WORK EMM ENROLLMENT

Domain Name ▲	Service Account Email	Token Name	Action
emm.vxl	w353dc495048e793b1a7ceb1e35a44@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖
test.vxl	w26962b11552dbc79d6a1702485198@pfwp-comfusionmdm2.google.com.iam.gserviceaccount.com	-	✖
vxlsoftware.com	mdmfusion@demoindia-141414.iam.gserviceaccount.com	B366BA53C86CC003	✖ ⚙

Show 5 entries Showing 1 to 3 of 3 entries

Service Json
Client Json
Client Secret: Enter client secret
API Key: Enter API Key
Project ID: Enter Project ID

AFW USER PROVISIONING

Android for Work account:

When an organization doesn't use managed Google Accounts, the recommended method is the Android for Work Accounts method, where the user installs the DPC from Google Play. The DPC can add Android for Work Accounts to a legacy device, similar to the way it adds the account to a work profile.

Android for Work Accounts provide a lightweight identity model for organizations that aren't currently using Google Apps. Android for Work Accounts:

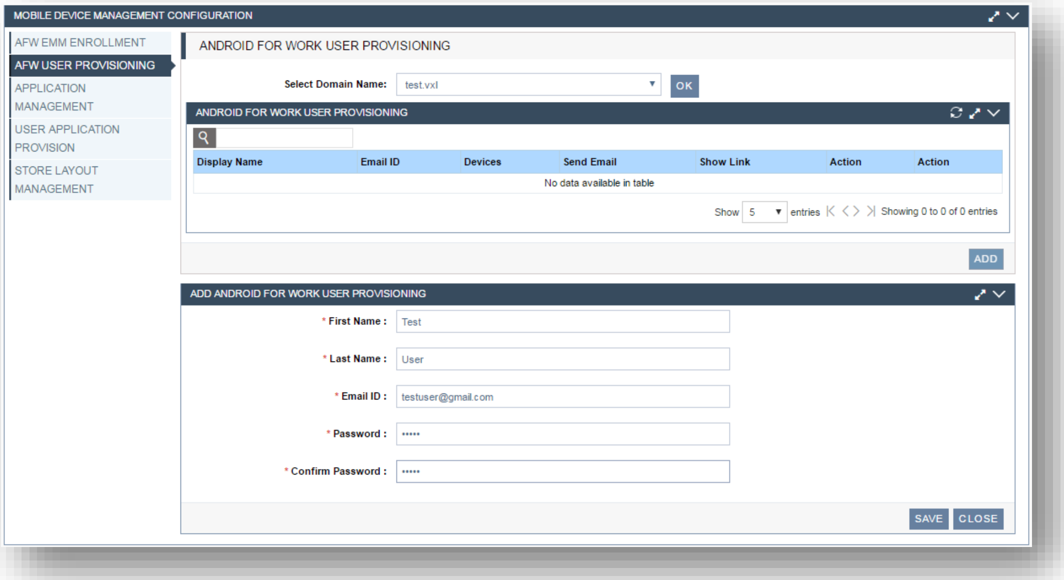
- Are not tied to domains, and your customers can structure them how they like within an organization
- Are quick to set up, no verification required.
- Are entirely managed by the EMM, no complex sync required

An Android for Work Accounts enterprise is a set of user, device, and administrator accounts that aren't linked to a domain name in any way. An organization can have multiple Android for Work Accounts enterprises. For example, departments or regions within an organization might set up separate Android for Work Accounts enterprises.

Fusion EMM console should provide a way for IT administrators to create QR codes for the devices they want to provision. The IT administrator sends the QR codes to their end users, and the end users provision their devices by scanning the QR codes.

- QR code provisioning doesn't require a Google identity, such as a Google domain or Google Account.
- Organizations that use Android for Work, but don't use Google Apps, don't have a Google identity.

1. Select **Domain name** from dropdown list.
2. Click on Add button to add more users in the selected domain.



ANDROID FOR WORK USER PROVISIONING

Select Domain Name: test.vxl

ANDROID FOR WORK USER PROVISIONING

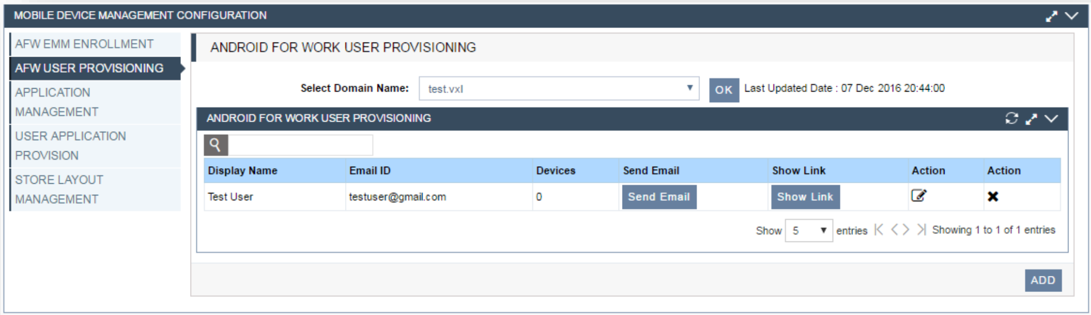
Display Name	Email ID	Devices	Send Email	Show Link	Action	Action
No data available in table						

Show 5 entries Showing 0 to 0 of 0 entries

ADD ANDROID FOR WORK USER PROVISIONING

* First Name :	Test
* Last Name :	User
* Email ID :	testuser@gmail.com
* Password :	•••••
* Confirm Password :	•••••

3. Enter the **First name**, **Last name**, **Email ID** and **Password**.
4. On clicking Save button, it will add the user details in the selected domain users list.



MOBILE DEVICE MANAGEMENT CONFIGURATION

ANDROID FOR WORK USER PROVISIONING

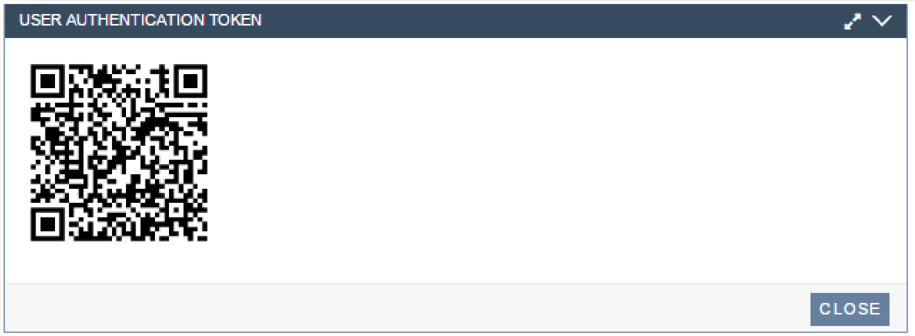
Select Domain Name: test.vxl OK Last Updated Date : 07 Dec 2016 20:44:00

ANDROID FOR WORK USER PROVISIONING

Display Name	Email ID	Devices	Send Email	Show Link	Action	Action
Test User	testuser@gmail.com	0	Send Email	Show Link	✎	✖

Show 5 entries Showing 1 to 1 of 1 entries

5. To receive the code in email, click on **Send Email** button.
6. To view a QR code, click on **Show Link** button.



USER AUTHENTICATION TOKEN

7. Scan the QR code to enroll the device in the domain.

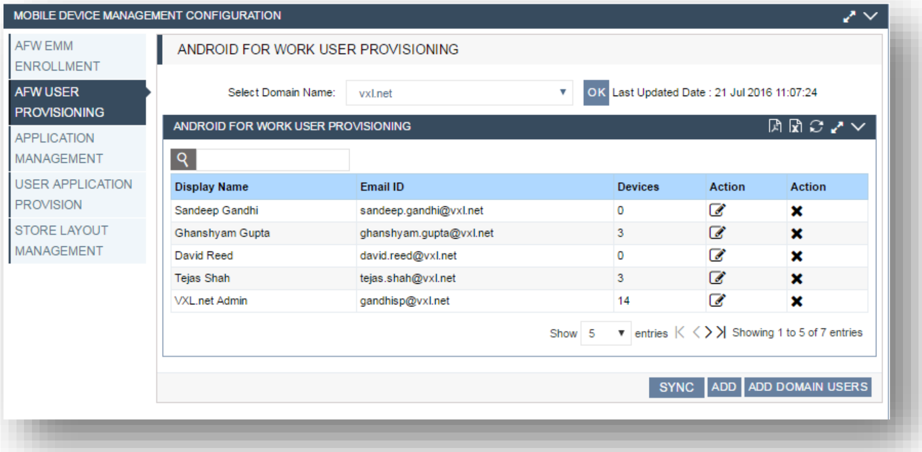
   (Refer Android Agent Registration using AFW account in Fusion EMM Installation Guide)

Google account:

The provisioning system usually takes information about employees from the Human Resource (HR) system. E.g. if a new employee is entered into the HR system the provisioning system detects that and pulls the information. This information is processed to determine a set of roles that each user should have. The roles determine which accounts the user should have and such accounts are created. All of that usually happens in a matter of seconds. Therefore, everything is prepared for the user to work on the very first day. Similar processes also apply when user is transferred to another department, when his responsibilities change and when he leaves the company.

It can take data from Customer Relationship Management (CRM) system and create accounts for customers. As provisioning can also maintain passwords this usually reduces the load of customer support centres. Provisioning can synchronize user accounts in portal and service provider environments. Provisioning is especially useful in cloud environments to manage very large number of accounts in many applications - something that is not feasible to do manually. Identity provisioning is without any doubt a foundation of Identity and Access Management.

1. Select **Domain name** from dropdown list.
2. User list with respective selected domain gets listed out.
3. Click on **Sync** to sync user provisioning data from the selected domain.



ANDROID FOR WORK USER PROVISIONING

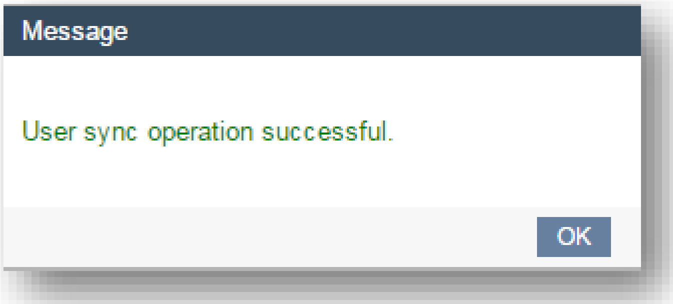
Select Domain Name: vxl.net ▼ Last Updated Date : 21 Jul 2016 11:07:24

ANDROID FOR WORK USER PROVISIONING

Display Name	Email ID	Devices	Action	Action
Sandeep Gandhi	sandeep.gandhi@vxl.net	0	✎	✖
Ghanshyam Gupta	ghanshyam.gupta@vxl.net	3	✎	✖
David Reed	david.reed@vxl.net	0	✎	✖
Tejas Shah	tejas.shah@vxl.net	3	✎	✖
VXL.net Admin	gandhisp@vxl.net	14	✎	✖

Show 5 ▼ entries Showing 1 to 5 of 7 entries

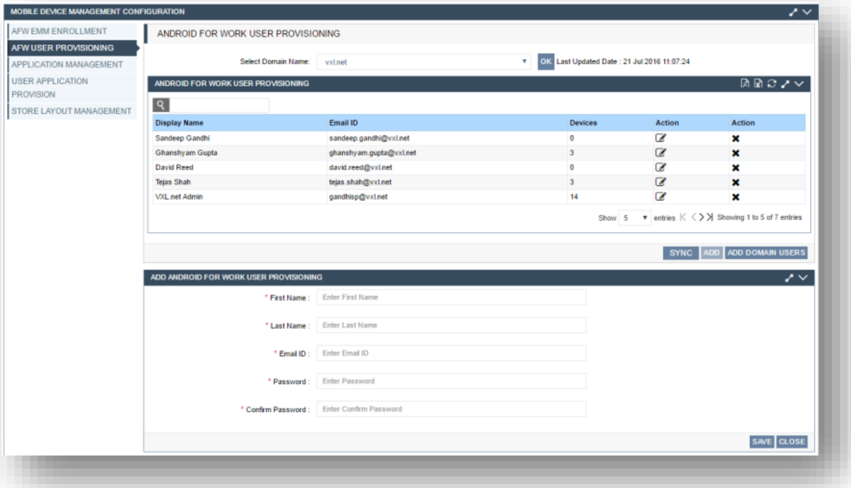
4. Once sync process is completed, success message is displayed.



Message

User sync operation successful.

5. User is able to add single user to the list by clicking on **Add** button.
6. Enter **First name**, **Last name**, **Email ID** and **Password**.
7. Click on **Save** to save the entered data.



MOBILE DEVICE MANAGEMENT CONFIGURATION

ANDROID FOR WORK USER PROVISIONING

Select Domain Name: vxl.net OK Last Updated Date : 21 Jul 2016 11:07:24

ANDROID FOR WORK USER PROVISIONING

Display Name	Email ID	Devices	Action	Action
Sandeep Gandhi	sandeep.gandhi@vxl.net	0	✎	✖
Ghanshyam Gupta	ghanshyam.gupta@vxl.net	3	✎	✖
David Reed	david.reed@vxl.net	0	✎	✖
Tejas Shah	tejas.shah@vxl.net	3	✎	✖
VXL.net Admin	gandhisp@vxl.net	14	✎	✖

Show 5 entries Showing 1 to 5 of 7 entries

ADD ANDROID FOR WORK USER PROVISIONING

* First Name : Enter First Name

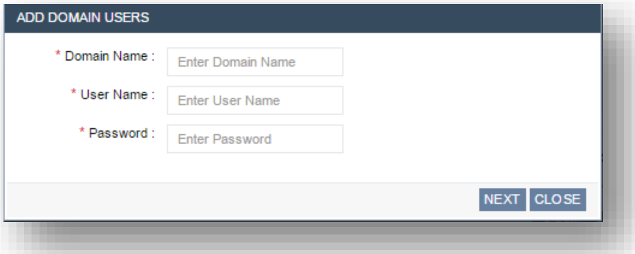
* Last Name : Enter Last Name

* Email ID : Enter Email ID

* Password : Enter Password

* Confirm Password : Enter Confirm Password

8. To add users from a domain, click on **Add Domain Users** button.
9. Enter **Domain name**, **Username** and **Password**.
10. Domain users get added to the list.



ADD DOMAIN USERS

* Domain Name : Enter Domain Name

* User Name : Enter User Name

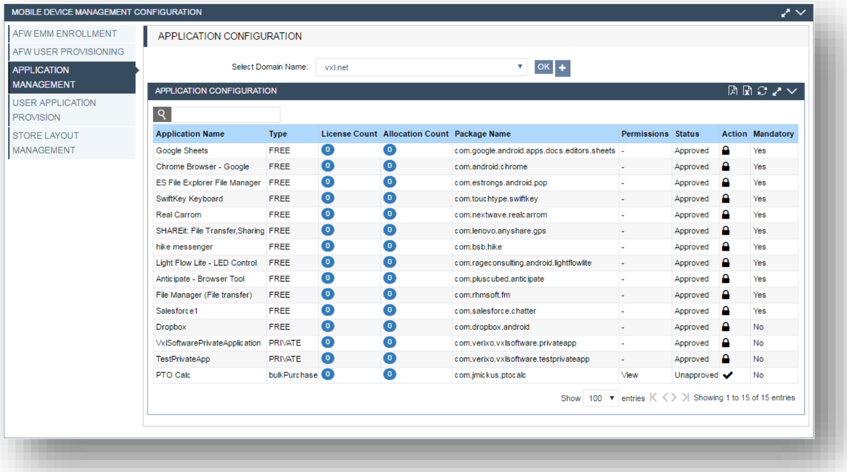
* Password : Enter Password

APPLICATION MANAGEMENT

Applications in Android for Work are managed via Google Play for Work, which provides full Play catalog access to an enterprise. IT admins can explicitly approve applications for use in Managed Profiles, and also have options for bulk purchasing of paid application licenses via Play for Work.

Once applications have been approved, the admin can use the Fusion EMM console to distribute applications in one of two ways. The first way is to collate the approved applications into subsets (called “collections”) and push them down to the Managed Play Store Client on target devices.

1. Select Domain from dropdown list
2. Install/ Uninstall software list with package name, License count, Permissions, Status, Actions, Type get listed out.



MOBILE DEVICE MANAGEMENT CONFIGURATION
AFW EMM ENROLLMENT
AFW USER PROVISIONING
APPLICATION MANAGEMENT
USER APPLICATION PROVISION
STORE LAYOUT MANAGEMENT
APPLICATION CONFIGURATION
OK
+
APPLICATION CONFIGURATION

Select Domain Name: vxl.net

Application Name	Type	License Count	Allocation Count	Package Name	Permissions	Status	Action	Mandatory
Google Sheets	FREE	0	0	com.google.android.apps.docs.editors.sheets	-	Approved	🔒	Yes
Chrome Browser - Google	FREE	0	0	com.android.chrome	-	Approved	🔒	Yes
ES File Explorer File Manager	FREE	0	0	com.estrongs.android.pop	-	Approved	🔒	Yes
SwiftKey Keyboard	FREE	0	0	com.touchtype.swiftkey	-	Approved	🔒	Yes
Real Carrom	FREE	0	0	com.nextwave.realcarrom	-	Approved	🔒	Yes
SHAREit: File Transfer,Sharing	FREE	0	0	com.lenovo.anyshare.gps	-	Approved	🔒	Yes
hike messenger	FREE	0	0	com.bsb.hike	-	Approved	🔒	Yes
Light Flow Lite - LED Control	FREE	0	0	com.rageconsulting.android.lightflowlite	-	Approved	🔒	Yes
Anticipate - Browser Tool	FREE	0	0	com.pluscubed.anticipate	-	Approved	🔒	Yes
File Manager (File transfer)	FREE	0	0	com.rhmsoft.fm	-	Approved	🔒	Yes
Salesforce1	FREE	0	0	com.salesforce.chatter	-	Approved	🔒	Yes
Dropbox	FREE	0	0	com.dropbox.android	-	Approved	🔒	No
VxlSoftwarePrivateApplication	PRIVATE	0	0	com.verixo.vxlsoftware.privateapp	-	Approved	🔒	No
TestPrivateApp	PRIVATE	0	0	com.verixo.vxlsoftware.testprivateapp	-	Approved	🔒	No
PTO Calc	bulkPurchase	0	0	com.jmickus.ptocalc	View	Unapproved	✓	No

Show 100 ▾ entries |< < > >| Showing 1 to 15 of 15 entries

Additionally, an Admin has the ability to silently install and uninstall applications into target Managed Profiles through Google Play. This allows for seamless management of application deployments without requiring any end-user intervention.

Bulk Purchasing (License)

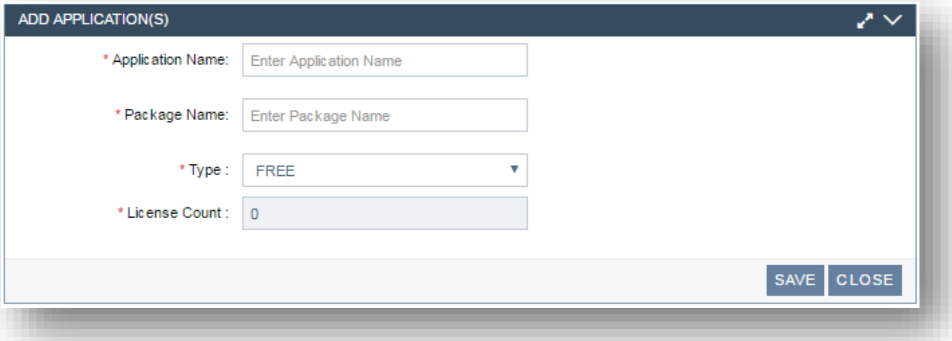
- Aside from permissions acceptance, an admin must also purchase licenses prior to approving a paid application.
- Purchases can be conducted with a credit card or online payment (Google Wallet).

Device Policy Client (DPC)

- The Device Policy Client is the EMM's client-side component. Even though it only resides in the Managed Profile, it is the only managed application to be downloaded from the personal Play Store.
- This is because the DPC must be installed on the device prior to the initial setup of the Managed Profile.
- Once it is installed, the user can launch the DPC and enter their EMM credentials to begin the Android for Work enrolment process.
- Following completion of the setup flow, the DPC will be badged and scoped only to the Managed Profile context by the OS.
- If the DPC is removed from the device, the entire Managed Profile will disappear along with it. The Managed Profile cannot exist unless there is a DPC running inside of it to enforce policy compliance.

Adding an Application

In order to add an application manually into the application list, you need to select the domain first in which you want to add an application and then click the Add + button. The add application form will be displayed.


ADD APPLICATION(S)

* Application Name: Enter Application Name

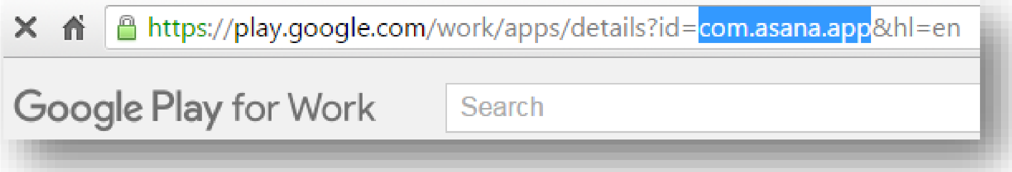
* Package Name: Enter Package Name

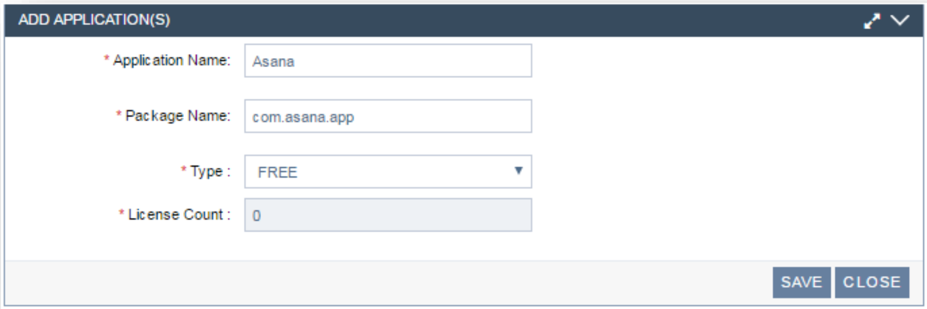
* Type : FREE

* License Count : 0

Simultaneously, you will need to login into Google Play for Work page (https://play.google.com/work/). Visit the page of the app you want to add into your company domain. Refer the browser URL of the app page. The name mentioned in the '*id=*' section is the required package name of that particular application.

For example: If you visit page of 'Asana' app, the browser URL is (https://play.google.com/store/apps/details?id=com.asana.app&hl=en). In this case, the package name would be **com.asana.app**


https://play.google.com/work/apps/details?id=com.asana.app&hl=en


ADD APPLICATION(S)

* Application Name: Asana

* Package Name: com.asana.app

* Type : FREE

* License Count : 0

1. On the Add Application form, enter the **Application Name.**

2. Enter the **Package Name** which you have copied from Play for Work application page.
3. Select the **Type** of the app.
4. Click **Save** to save the entered details**.**

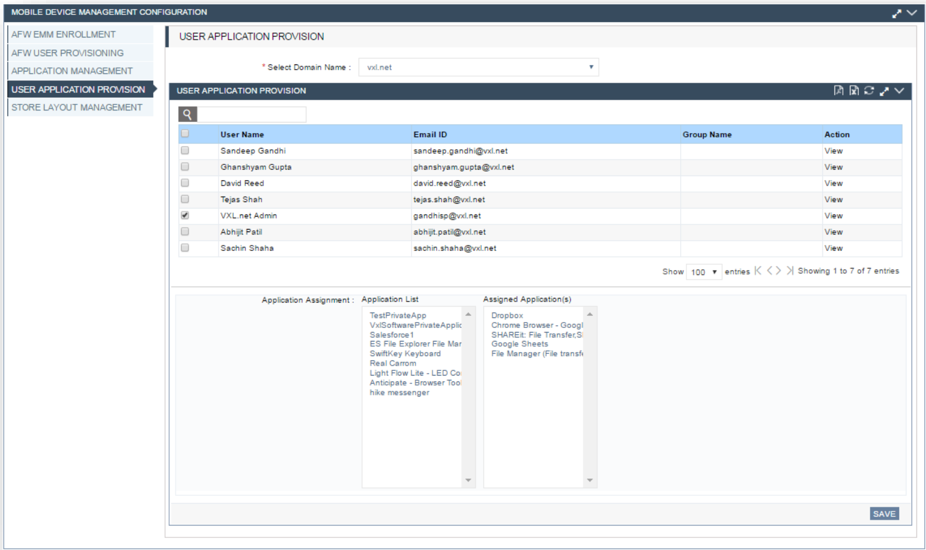
   Application saved successfully message is displayed.

The added application will now be listed in the application table below that particular domain.

USER APPLICATION PROVISION

In User Application Provisioning, we can assign applications to various users which were previously approved by the company.

1. Select the **Domain name**.
2. Select the **users** to which applications are to be assigned.
3. The list of company approved applications of the respective selected domain will be displayed in the list below.
4. Select the **applications** to be assigned for the selected user.
5. On click of **Save**, summary details popup is displayed showing that the product set is assigned to the users.



MOBILE DEVICE MANAGEMENT CONFIGURATION
AFW EMM ENROLLMENT
AFW USER PROVISIONING
APPLICATION MANAGEMENT
USER APPLICATION PROVISION
STORE LAYOUT MANAGEMENT
USER APPLICATION PROVISION

* Select Domain Name : vxl.net

USER APPLICATION PROVISION

□	User Name	Email ID	Group Name	Action
□	Sandeep Gandhi	sandeep.gandhi@vxl.net		View
□	Ghanshyam Gupta	ghanshyam.gupta@vxl.net		View
□	David Reed	david.reed@vxl.net		View
□	Tejas Shah	tejas.shah@vxl.net		View
☑	VXL.net Admin	gandhisp@vxl.net		View
□	Abhijit Patil	abhijit.patil@vxl.net		View
□	Sachin Shaha	sachin.shaha@vxl.net		View

Show 100 entries Showing 1 to 7 of 7 entries

Application Assignment :

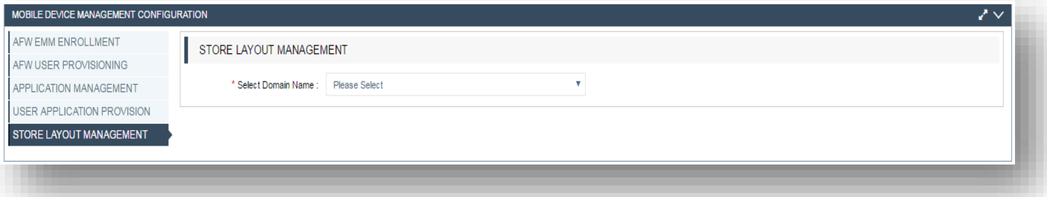
Application List:
TestPrivateApp
VxlSoftwarePrivateApplic
Salesforce1
ES File Explorer File Mar
SwiftKey Keyboard
Real Carrom
Light Flow Lite - LED Co
Anticipate - Browser Tool
hike messenger

Assigned Application(s):
Dropbox
Chrome Browser - Googl
SHAREit: File Transfer,S
Google Sheets
File Manager (File transf

STORE LAYOUT MANAGEMENT

Google Play for Work lets you design and create a store layout unique to your users' needs. After you give your users access to apps, you can group the apps into clusters to be display on pages in the Google Play for Work storefront.

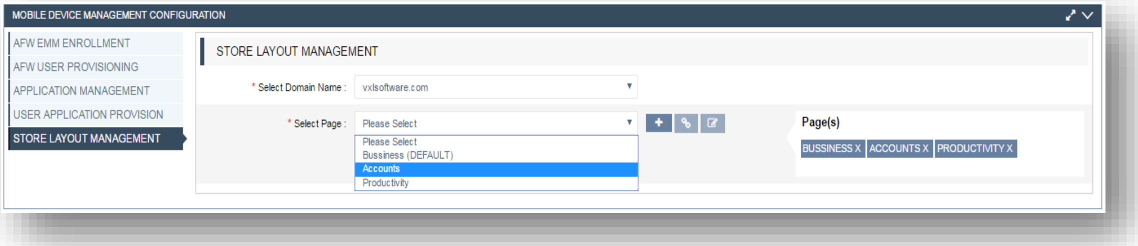
The Google Play EMM API Reference has information on the resources and associated methods you use to design a store layout.



STORE LAYOUT MANAGEMENT

* Select Domain Name : Please Select

Localized names for pages and clusters



STORE LAYOUT MANAGEMENT

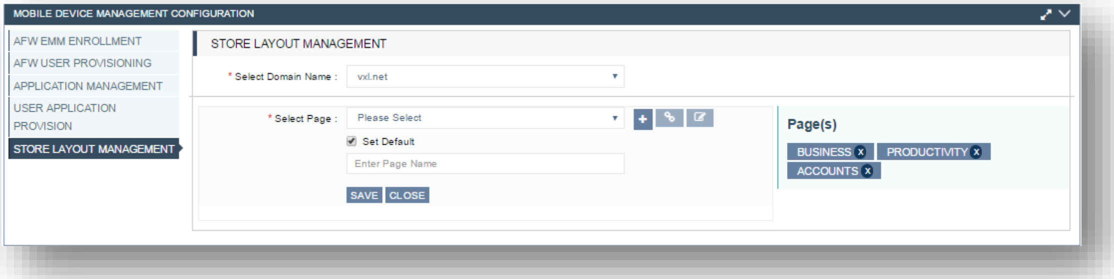
* Select Domain Name : vxlsoftware.com

* Select Page : Please Select

Page(s)

BUSSINESS X ACCOUNTS X PRODUCTIVITY X

Google Play for Work store layout supports localized names for store pages and store clusters. When you create a page or cluster you provide a list of supported locales, as IETF language tags, and associated localized names. If a user's locale is not on the supported list, the system will chose a close match if one is available.



STORE LAYOUT MANAGEMENT

* Select Domain Name : vxl.net

* Select Page : Please Select

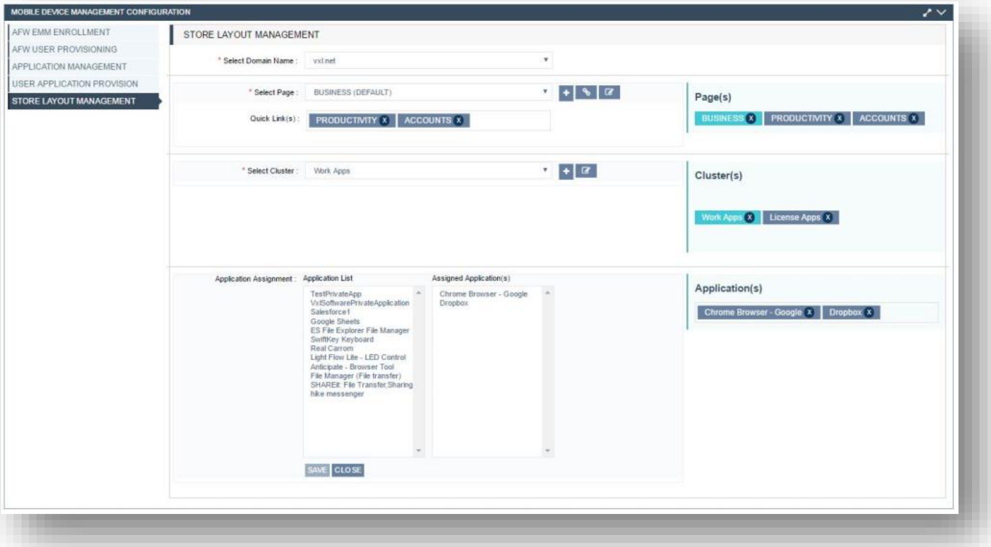
☑ Set Default

Enter Page Name

Page(s)

BUSINESS X PRODUCTIVITY X ACCOUNTS X

As an EMM, you can create a unique customized store layout for each of your customers. A typical layout consists of a set of pages to display to users in the Google Play for Work store front. Each page you create contains one or more clusters, and each cluster contains a set of apps. Because you select which apps are in a cluster, you can use the clusters to group related apps together.



STORE LAYOUT MANAGEMENT

* Select Domain Name : vxl.net

* Select Page : BUSINESS (DEFAULT)

Quick Link(s) : PRODUCTIVITY x ACCOUNTS x

Page(s): BUSINESS x PRODUCTIVITY x ACCOUNTS x

* Select Cluster : Work Apps

Cluster(s): Work Apps x License Apps x

Application Assignment :

Application List:
TestPrivateApp
VxlSoftwarePrivateApplication
Salesforce1
Google Sheets
ES File Explorer File Manager
SwiftKey Keyboard
Real Carrom
Light Flow Lite - LED Control
Anticipate - Browser Tool
File Manager (File transfer)
SHAREit: File Transfer,Sharing
hike messenger

Assigned Application(s):
Chrome Browser - Google
Dropbox

Application(s): Chrome Browser - Google x Dropbox x

For example, you could create a page just for work apps that contains a Document cluster and a Planning cluster. The Document cluster might contain apps such as Google Docs, Google Sheets, and Google Slides, and the Planning cluster could contain work tracking, calendar, and meeting planner apps.

Unbind/Unenrolment of the domain

In order to enroll the domain again, first you need to unbind/unenroll the domain which was previously enrolled.

To unbind a domain, go to AFW EMM Enrolment -> click the Unbind ☒ button next to the account name you want to unbind.

Once your domain is successfully unenrolled from the server, the token which was previously used for enrollment is expired. You will now be able to generate a new token from Google admin console page.

Refer Step 5.2 in Configuring Enterprise Service Account (ESA) section regarding how to generate a new token.

It is highly recommended to save the token details before uninstalling the Fusion EMM server.

Policy Controls & Distribution

All Android for Work policies will be configure at the EMM console level. The presentation of these policy settings may vary slightly depending on the EMM but there is a standard set of APIs available that will allow the EMM to manage the certain components of the Managed Profile.

The below is not a fully exhaustive list, but covers the basic policies that can be configured in the Managed Profile via an EMM console:

- **Device Passcode**
    - Length
    - Strength
    - Maximum failed attempts
    - Expiration
- **Data Separation & Sharing**
    - Allow export of work contacts to personal profile
    - Allow full notifications/force redacted notifications in managed applications
    - Allow/disallow copy & paste
- **Profile Settings**
    - Enable/disable camera for applications in a Work Profile
    - Manage inter-app communication between profiles
    - Installation of certificates into Managed Profile Key store
    - Disallow uninstallation of applications in a Work Profile
- **Device Settings (if Managed Profile is Device Owner)**
    - Enable/disable USB debugging
    - Allow/disallow factory reset
    - Allow/disallow tethering
    - Allow/disallow side-loading of application
- **Application Specific - Chrome Browser Settings**
    - Allow/disallow cookies
    - Allow/disallow images
    - Allow/disallow JavaScript
    - Allow/disallow popups
    - Default homepage
    - Default search provider
    - Enable/disable safe browsing
    - Enable/disable history

- Enable/disable incognito mode
- Whitelist/blacklist URLs (for access, or for JavaScript/pop ups/cookies/etc.)

- **Application Specific - Divide Productivity**
  - Mail provisioning settings (username, password, host etc.)
  - Default signature
  - Max attachment size
  - S/MIME signing and encryption certificates

In addition to the policies mentioned on the previous page, the IT admin will also configure any specific Application Restrictions via the EMM console.

Installation and Enrollment of Fusion EMM Agent

Installation of Android agent

There are two ways to install the Fusion EMM Agent.

1) Auto-downloading the Fusion EMM agent using Google verified domain account.

2) Downloading the Fusion EMM Agent from Play Store.

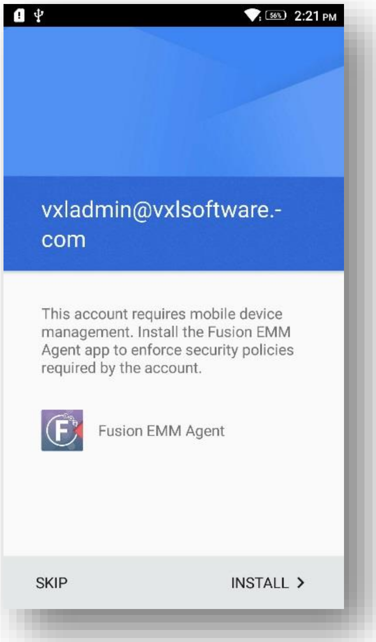
Both the ways are explained in below steps.

Auto-downloading by Google verified domain account

There are two ways by which user can auto-download the Fusion EMM Agent on the device.

With factory reset

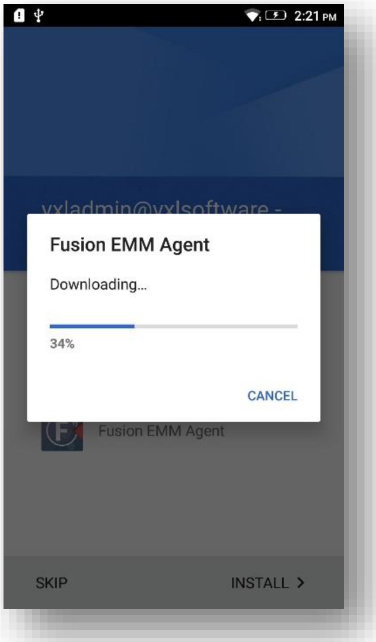
1. Enter credentials to add Google account.
2. If it is a work account, installation popup is displayed to install the app.
3. Domain DPC will be automatically downloaded (Fusion EMM Agent application).



vxladmin@vxlsoftware.-com

This account requires mobile device management. Install the Fusion EMM Agent app to enforce security policies required by the account.

Fusion EMM Agent

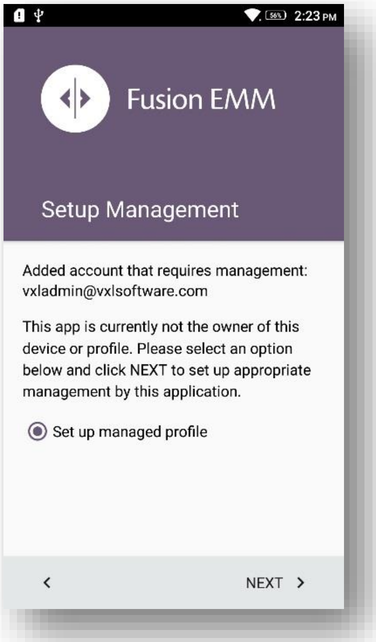


Fusion EMM Agent

Downloading...

34%

4. Work profile provisioning gets started (same domain account will be used for migration).



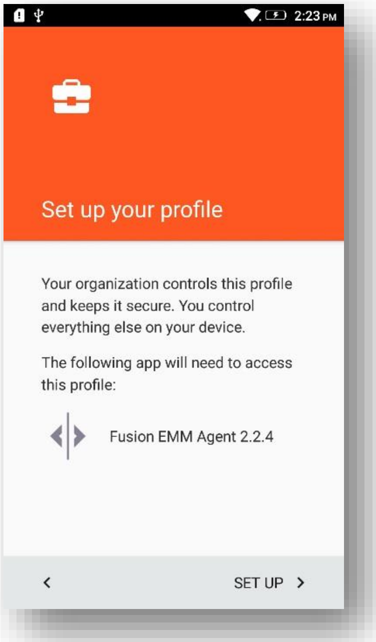
Fusion EMM

Setup Management

Added account that requires management: vxladmin@vxlsoftware.com

This app is currently not the owner of this device or profile. Please select an option below and click NEXT to set up appropriate management by this application.

◉ Set up managed profile



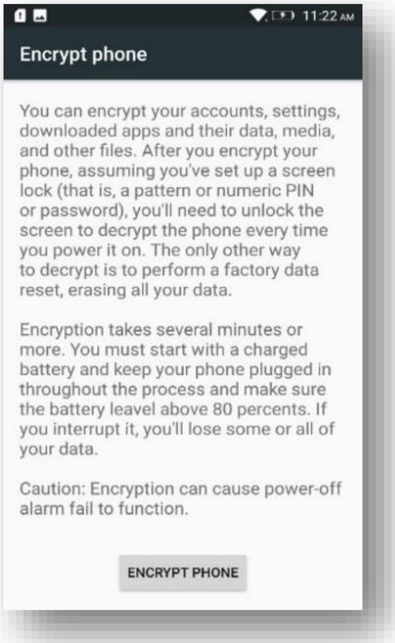
Set up your profile

Your organization controls this profile and keeps it secure. You control everything else on your device.

The following app will need to access this profile:

Fusion EMM Agent 2.2.4

5. Device encryption will begin.



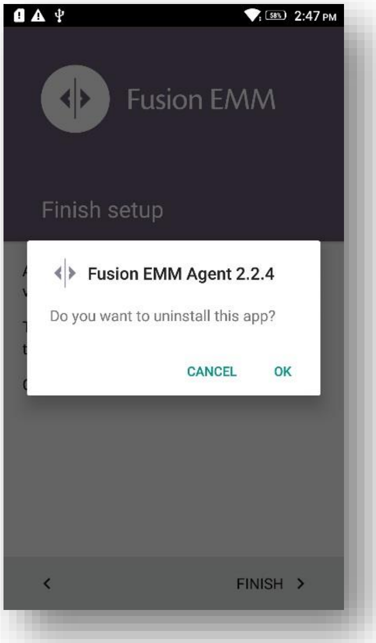
Encrypt phone

You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. After you encrypt your phone, assuming you've set up a screen lock (that is, a pattern or numeric PIN or password), you'll need to unlock the screen to decrypt the phone every time you power it on. The only other way to decrypt is to perform a factory data reset, erasing all your data.

Encryption takes several minutes or more. You must start with a charged battery and keep your phone plugged in throughout the process and make sure the battery leavel above 80 percents. If you interrupt it, you'll lose some or all of your data.

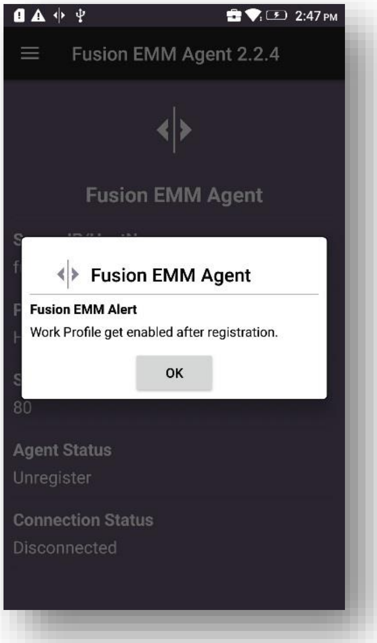
Caution: Encryption can cause power-off alarm fail to function.

6. After successful encryption, device provisioning gets completed.
7. Work profile gets created successfully.
8. A popup is displayed on the device for confirmation regarding the personal-side agent. Personal-side agent can be un-installed at this point. Only work-profile agent will be present on the device.



Fusion EMM Agent 2.2.4

Do you want to uninstall this app?



Fusion EMM Agent

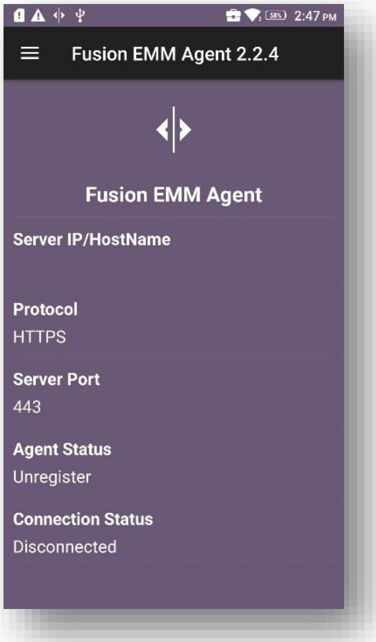
Fusion EMM Alert

Work Profile get enabled after registration.

Agent Status
Unregister

Connection Status
Disconnected

9. Fusion EMM Agent application gets started instantly. An alert is displayed informing about enabling the work profile once the device is successfully registered on the server.



Fusion EMM Agent 2.2.4

Fusion EMM Agent

Server IP/HostName

Protocol
HTTPS

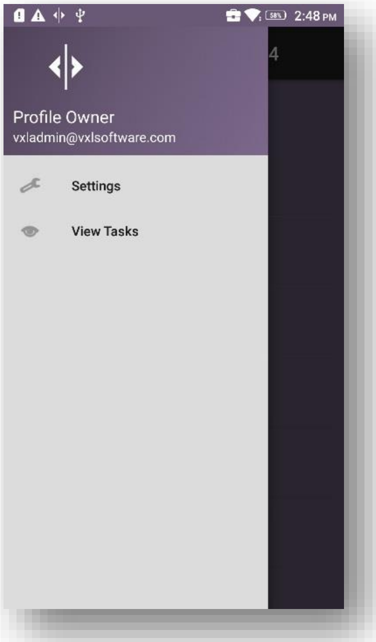
Server Port
443

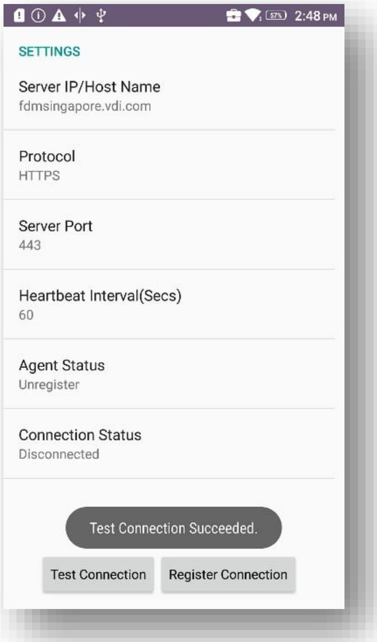
Agent Status
Unregister

Connection Status
Disconnected

10. Access the app drawer and enter the appropriate details in **Settings** page.

    Test connection with the server.





SETTINGS

Server IP/Host Name
fdmsingapore.vdi.com

Protocol
HTTPS

Server Port
443

Heartbeat Interval(Secs)
60

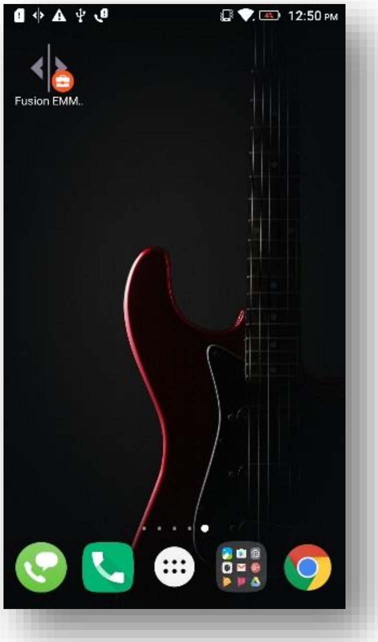
Agent Status
Unregister

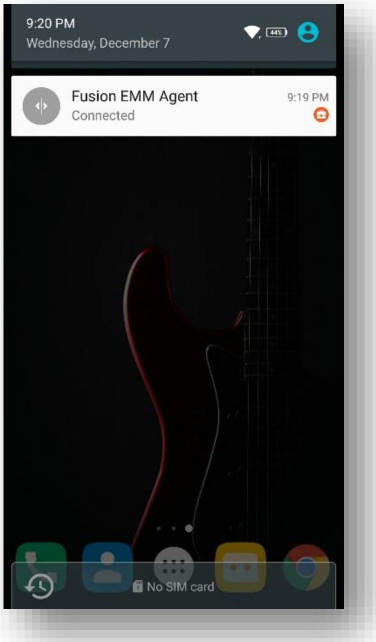
Connection Status
Disconnected

Test Connection Succeeded.

11. Once the test connection is successful, click on Register connection to send a registration request to the server.

12. Fusion EMM Agent icon gets created in the application list and connection status is shown in the notification bar.



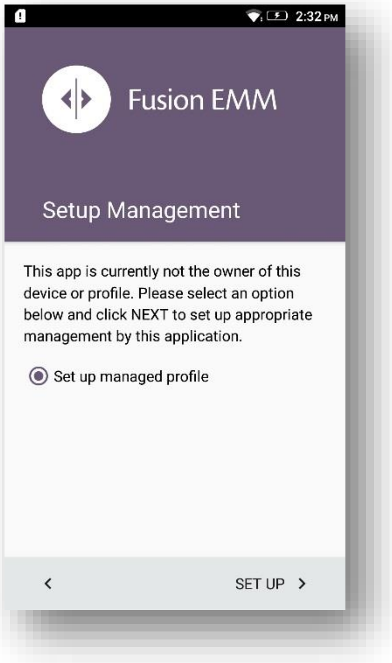


Without factory reset

1. On the device, navigate to Settings -> Accounts -> Enter credentials to add Google verified domain account.
2. Domain DPC will be automatically downloaded (Fusion EMM Agent application).
3. Installation popup is displayed to install the app.
4. Work profile provisioning gets started (same domain account will be used for migration).
5. If the device is not encrypted, user is prompted to encrypt.
6. Device provisioning gets completed.
7. Work profile gets created successfully.
8. Fusion EMM Agent application gets started instantly. An alert is displayed informing about enabling the work profile once the device is successfully registered on the server.
9. Access the app drawer and enter the appropriate details in **Settings** page.
   Test connection with the server.
10. Once the test connection is successful, click on Register connection to send a registration request to the server.
11. Fusion EMM Agent icon gets created in the application list and connection status is shown in the notification bar.

Downloading the Fusion EMM Agent from Play Store

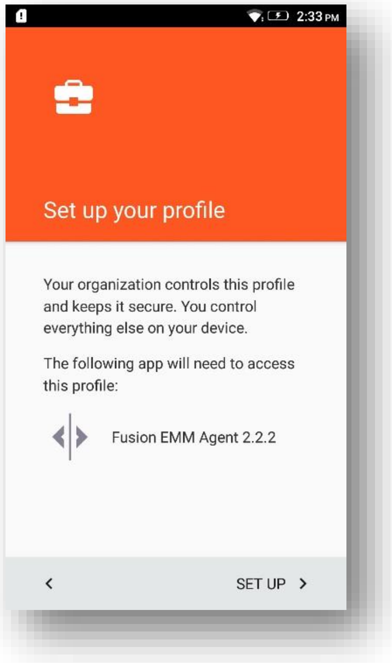
1. Download the 'Fusion EMM Agent' from Google Play Store.
2. After agent installation is complete, the managed profile setup gets started.



Setup Management

This app is currently not the owner of this device or profile. Please select an option below and click NEXT to set up appropriate management by this application.

● Set up managed profile



Set up your profile

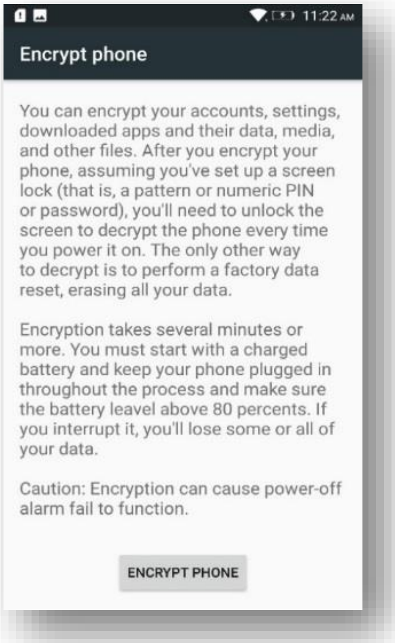
Your organization controls this profile and keeps it secure. You control everything else on your device.

The following app will need to access this profile:

Fusion EMM Agent 2.2.2

3. If the device is not encrypted, user is prompted to encrypt and account migration process begins.

   Account migration is explained in detail further.



11:22 AM

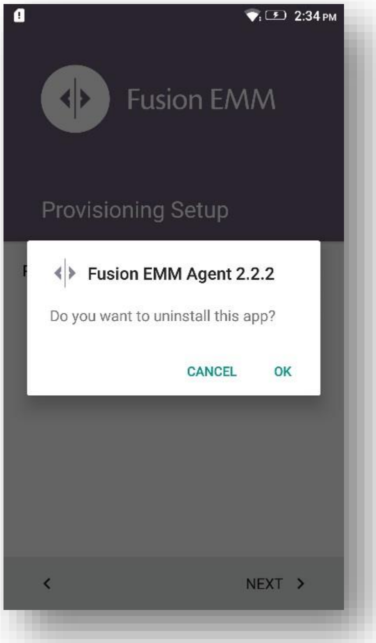
Encrypt phone

You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. After you encrypt your phone, assuming you've set up a screen lock (that is, a pattern or numeric PIN or password), you'll need to unlock the screen to decrypt the phone every time you power it on. The only other way to decrypt is to perform a factory data reset, erasing all your data.

Encryption takes several minutes or more. You must start with a charged battery and keep your phone plugged in throughout the process and make sure the battery leavel above 80 percents. If you interrupt it, you'll lose some or all of your data.

Caution: Encryption can cause power-off alarm fail to function.

4. A popup is displayed on the device for confirmation regarding the personal-side agent. Personal-side agent can be un-installed at this point. Only work-profile agent will be present on the device.



2:34 PM

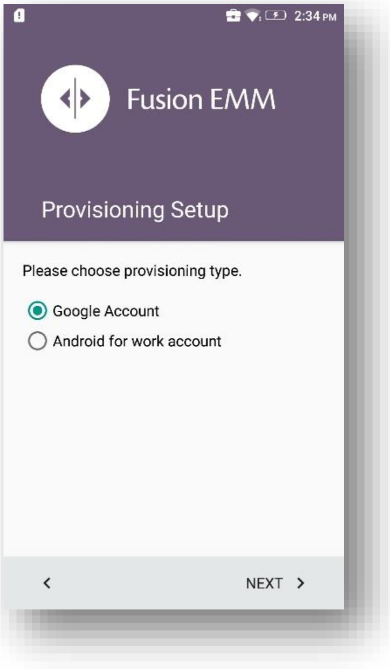
Fusion EMM

Provisioning Setup

Fusion EMM Agent 2.2.2

Do you want to uninstall this app?

5. User can choose the provisioning type by which the managed account is to be created.



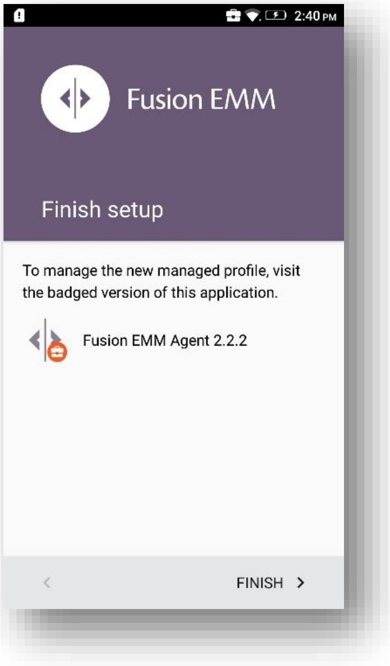
Provisioning Setup

Please choose provisioning type.

● Google Account
○ Android for work account

6. The first method is by using a Google account.

   User will enter the credentials of the Google verified domain account. Follow the instructions and the work profile creation is completed.



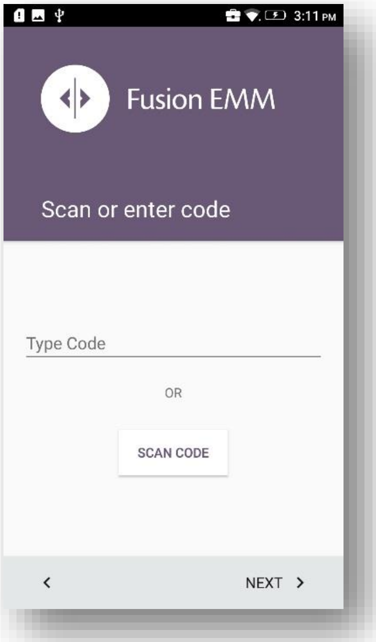
Finish setup

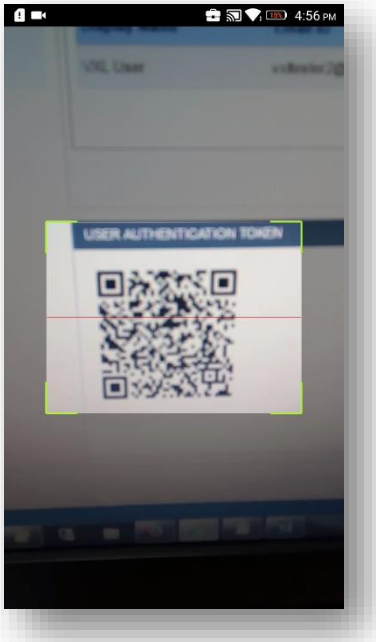
To manage the new managed profile, visit the badged version of this application.

Fusion EMM Agent 2.2.2

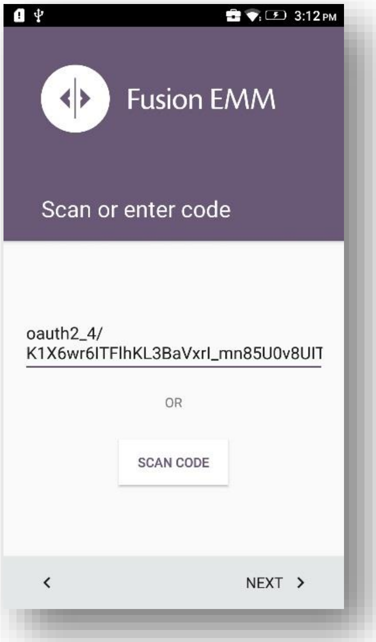
7. The second method is by using Android for Work account.

Here, user can enter the code manually on device or scan a QR code from device which is generated from Fusion EMM server.



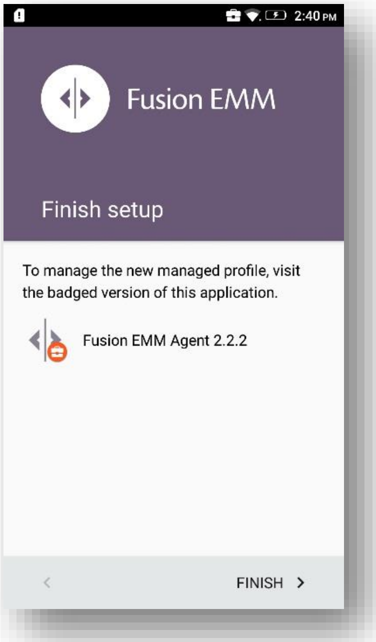


8. Once the QR code is scanned successfully, a code is auto-generated and displayed on the device.



oauth2_4/
K1X6wr6ITFlhKL3BaVxrl_mn85U0v8UIT

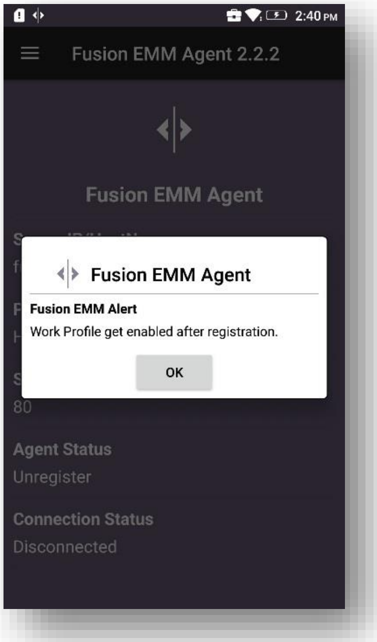
9. Click on Next button to continue with work-profile creation.
10. Finish the setup and Fusion EMM agent application gets started instantly. An alert is displayed informing about enabling the work profile once the device is successfully registered on the server.



Finish setup

To manage the new managed profile, visit the badged version of this application.

Fusion EMM Agent 2.2.2



Fusion EMM Agent

Fusion EMM Alert

Work Profile get enabled after registration.

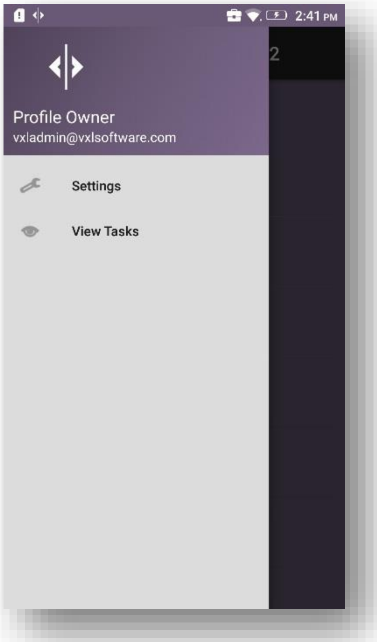
80

Agent Status
Unregister

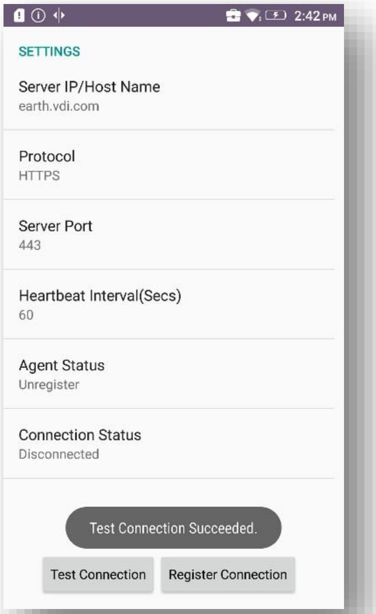
Connection Status
Disconnected

11. Access the app drawer and enter the appropriate details in **Settings** page.

    Test connection with the server.



Profile Owner
vxladmin@vxlsoftware.com



SETTINGS

Server IP/Host Name
earth.vdi.com

Protocol
HTTPS

Server Port
443

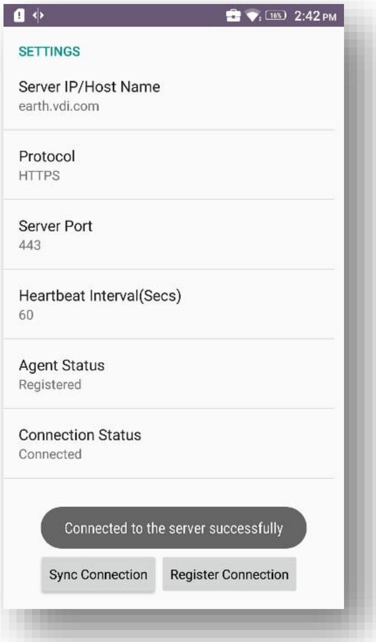
Heartbeat Interval(Secs)
60

Agent Status
Unregister

Connection Status
Disconnected

Test Connection Succeeded.

12. Once the test connection is successful, click on Register connection to send a registration request to the server.



SETTINGS

Server IP/Host Name
earth.vdi.com

Protocol
HTTPS

Server Port
443

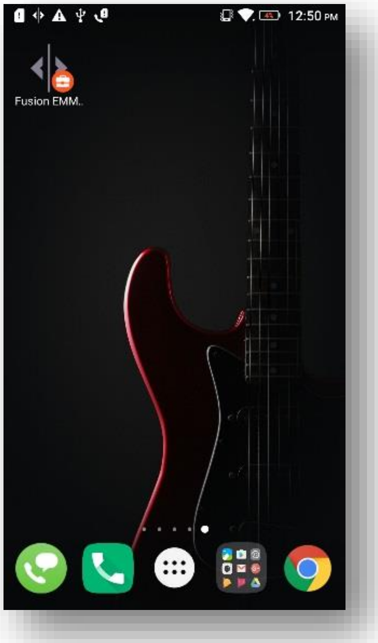
Heartbeat Interval(Secs)
60

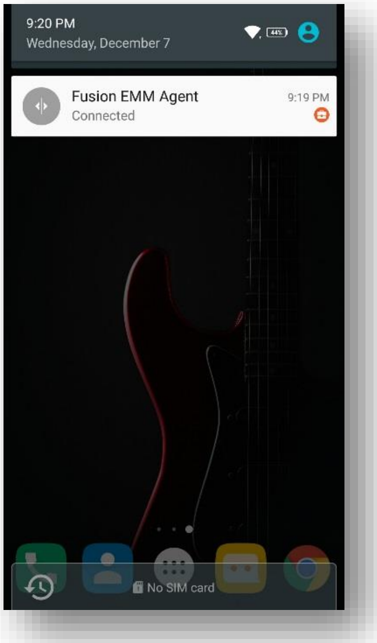
Agent Status
Registered

Connection Status
Connected

Connected to the server successfully

13. Fusion EMM Agent icon gets created in the application list and connection status is shown in the notification bar.





Fusion EMM Agent 9:19 PM
Connected

Installation/ Enrollment of iOS Profile

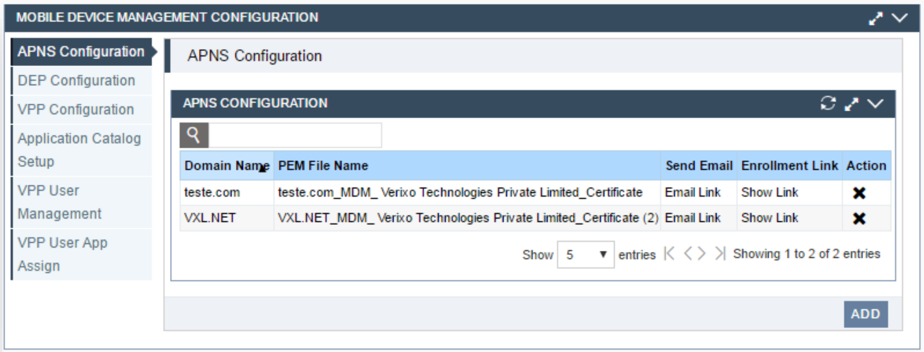
Enables the user to Enroll and Register the device in two ways:

- APNS Configuration
- DEP Configuration

APNS Configuration

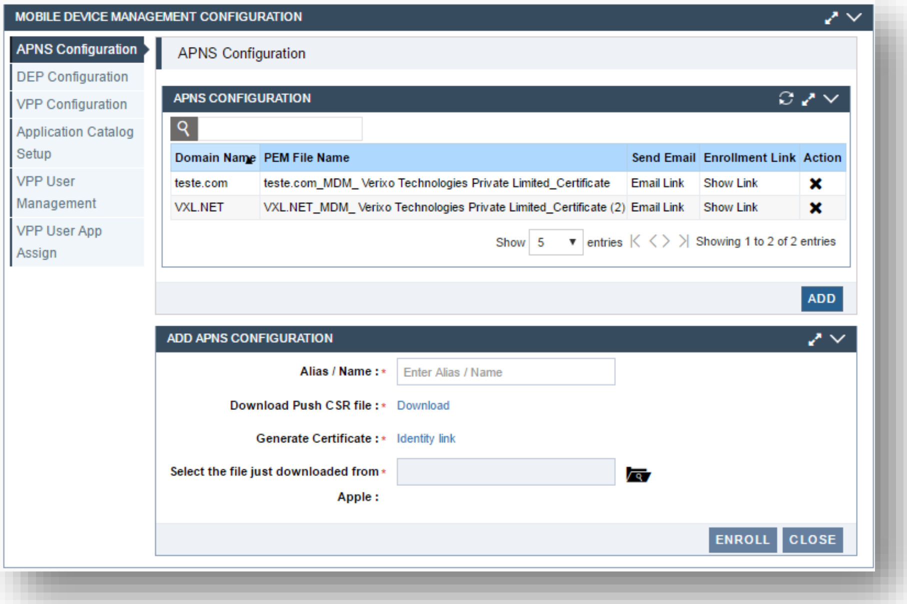
User needs to follow APNS Configuration for iOS device enrolment process.

1. Navigate to Fusion EMM Server -> Configuration Setup -> Apple MDM Configuration -> APNS Configuration
2. Click on the Add button



Domain Name	PEM File Name	Send Email	Enrollment Link	Action
teste.com	teste.com_MDM_ Verixo Technologies Private Limited_Certificate	Email Link	Show Link	✖
VXL.NET	VXL.NET_MDM_ Verixo Technologies Private Limited_Certificate (2)	Email Link	Show Link	✖

3. Download the Apple push .csr file.



Domain Name	PEM File Name	Send Email	Enrollment Link	Action
teste.com	teste.com_MDM_ Verixo Technologies Private Limited_Certificate	Email Link	Show Link	✖
VXL.NET	VXL.NET_MDM_ Verixo Technologies Private Limited_Certificate (2)	Email Link	Show Link	✖

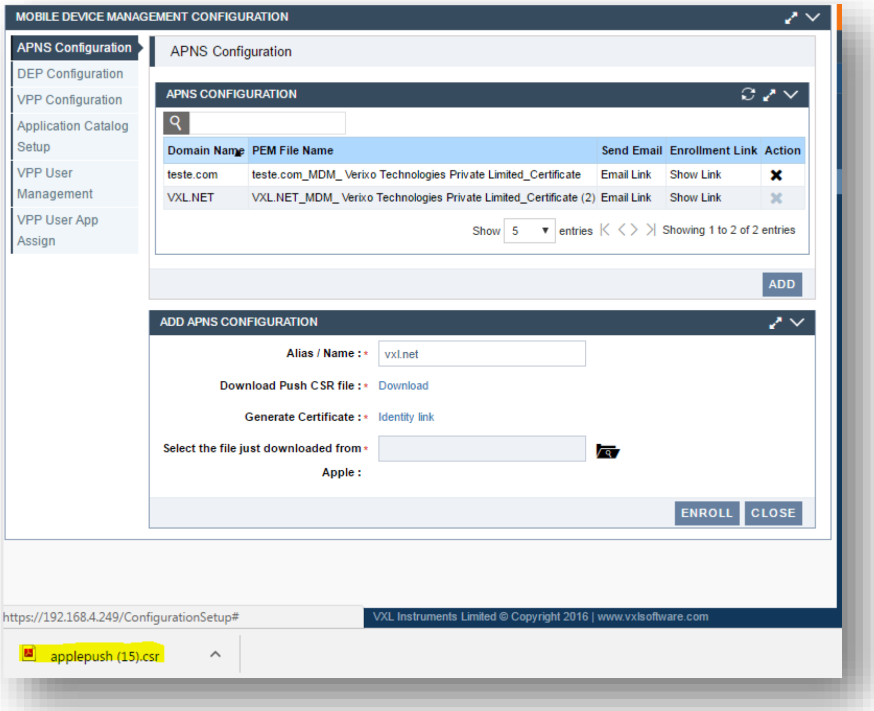
Show 5 entries Showing 1 to 2 of 2 entries

Alias / Name : * Enter Alias / Name

Download Push CSR file : * Download

Generate Certificate : * Identity link

Select the file just downloaded from * Apple :



Domain Name	PEM File Name	Send Email	Enrollment Link	Action
teste.com	teste.com_MDM_ Verixo Technologies Private Limited_Certificate	Email Link	Show Link	✖
VXL.NET	VXL.NET_MDM_ Verixo Technologies Private Limited_Certificate (2)	Email Link	Show Link	✖

Show 5 entries Showing 1 to 2 of 2 entries

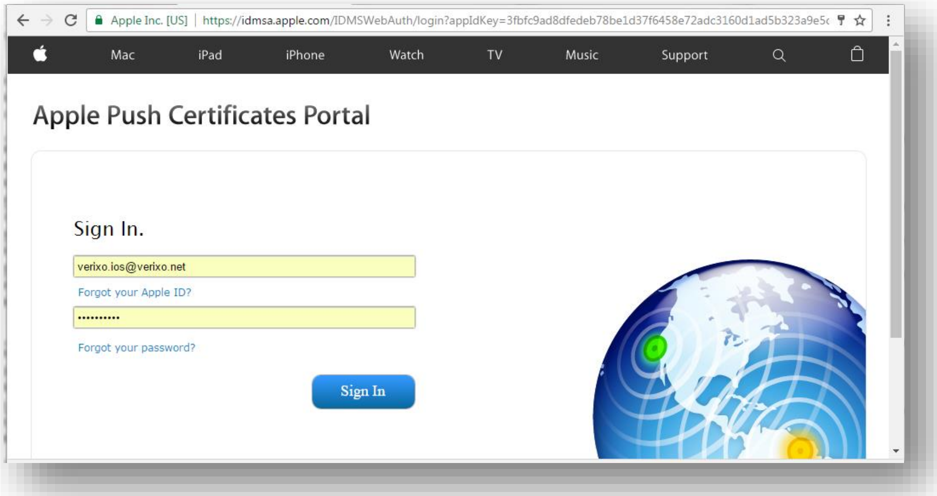
Alias / Name : * vxl.net

Download Push CSR file : * Download

Generate Certificate : * Identity link

Select the file just downloaded from * Apple :

4. Visit https://identity.apple.com/pushcert/
5. Sign-in using an enterprise account.


Apple Inc. [US] | https://idmsa.apple.com/IDMSWebAuth/login?appIdKey=3fbfc9ad8dfedeb78be1d37f6458e72adc3160d1ad5b323a9e5c

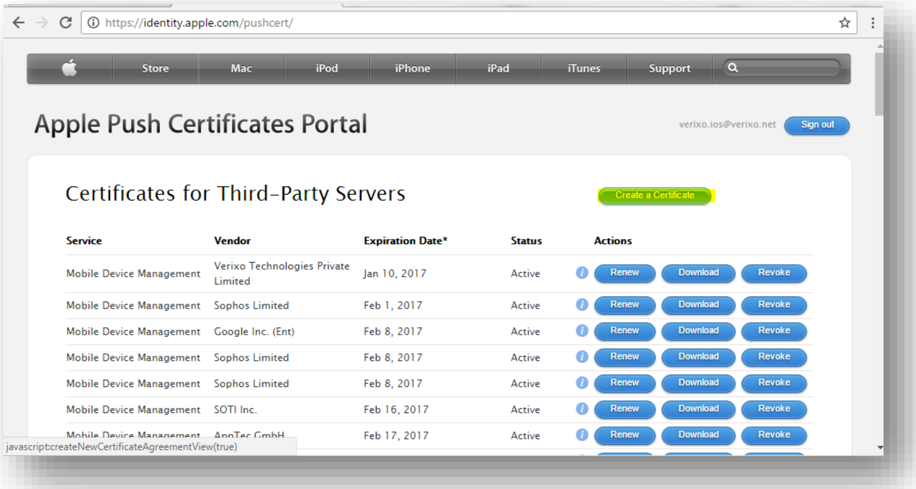
Apple Push Certificates Portal

Sign In.

verixo.ios@verixo.net

••••••••••

6. Click on ‘Create Certificate’.


https://identity.apple.com/pushcert/

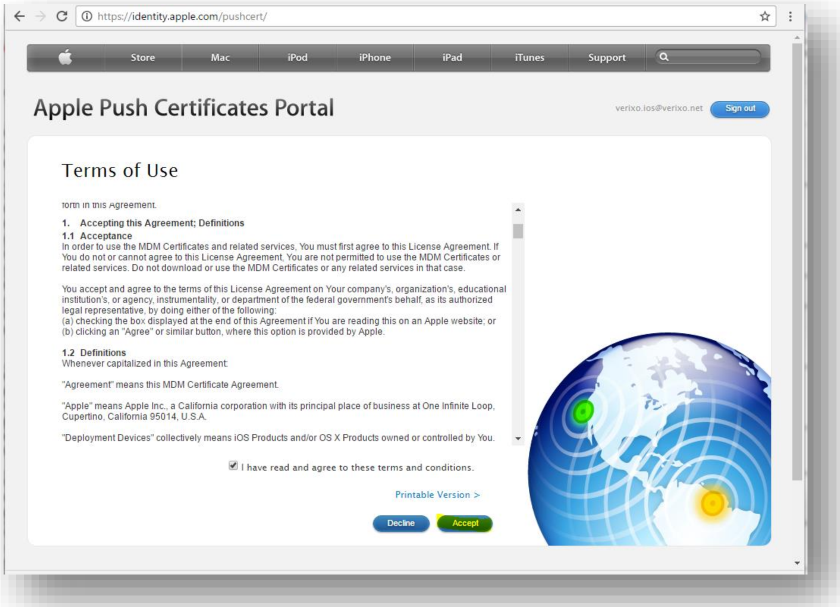
Apple Push Certificates Portal

verixo.ios@verixo.net

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Verixo Technologies Private Limited	Jan 10, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 1, 2017	Active	Renew Download Revoke
Mobile Device Management	Google Inc. (Ent)	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	SOTI Inc.	Feb 16, 2017	Active	Renew Download Revoke
Mobile Device Management	AppTec GmbH	Feb 17, 2017	Active	Renew Download Revoke

javascript:createNewCertificateAgreementView(true)



Apple Push Certificates Portal

Terms of Use

forth in this Agreement.

1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational institution's, or agency, instrumentality, or department of the federal government's behalf, as its authorized legal representative, by doing either of the following:
(a) checking the box displayed at the end of this Agreement if You are reading this on an Apple website; or
(b) clicking an "Agree" or similar button, where this option is provided by Apple.

1.2 Definitions

Whenever capitalized in this Agreement:

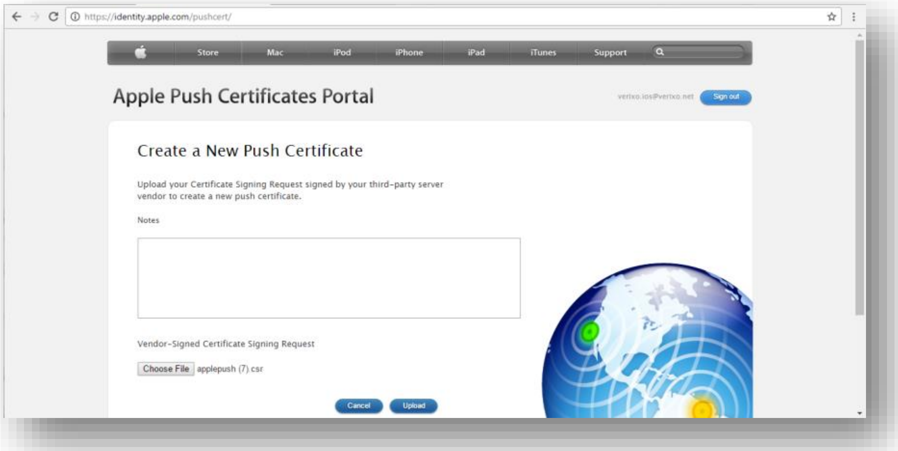
"Agreement" means this MDM Certificate Agreement.

"Apple" means Apple Inc., a California corporation with its principal place of business at One Infinite Loop, Cupertino, California 95014, U.S.A.

"Deployment Devices" collectively means iOS Products and/or OS X Products owned or controlled by You.

☑ I have read and agree to these terms and conditions.

7. Click on Upload & Browse downloaded .csr file.



Apple Push Certificates Portal

Create a New Push Certificate

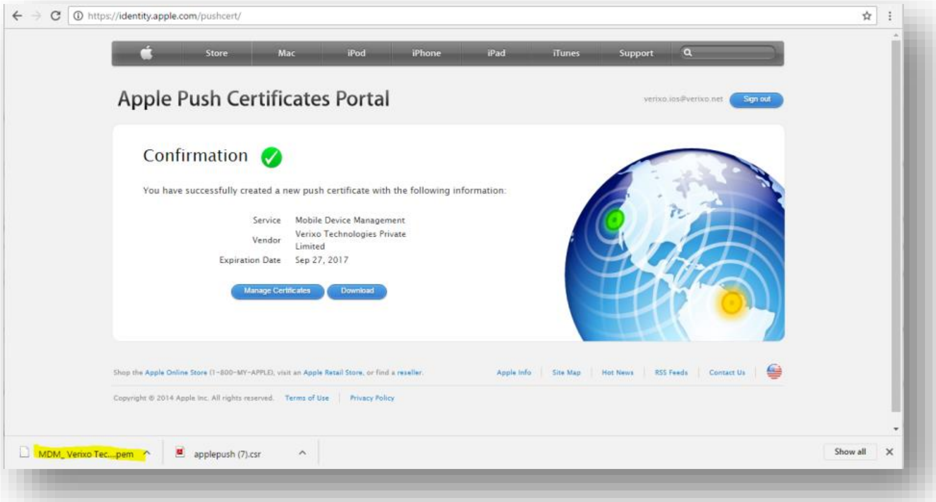
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

applepush (7).csr

8. Click on the Download button.
9. .pem file gets downloaded.
10. Navigate to Fusion EMM server -> APNS -> click on Add



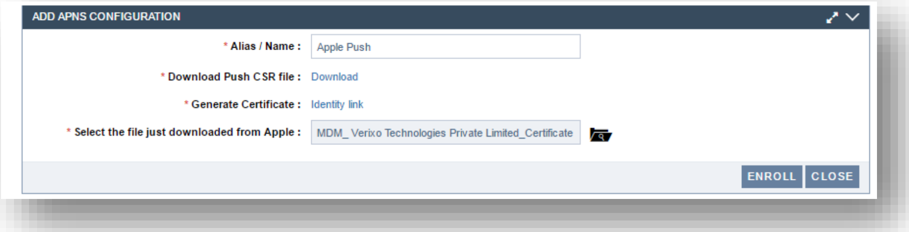
Apple Push Certificates Portal

Confirmation ✓

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	Verixo Technologies Private Limited
Expiration Date	Sep 27, 2017

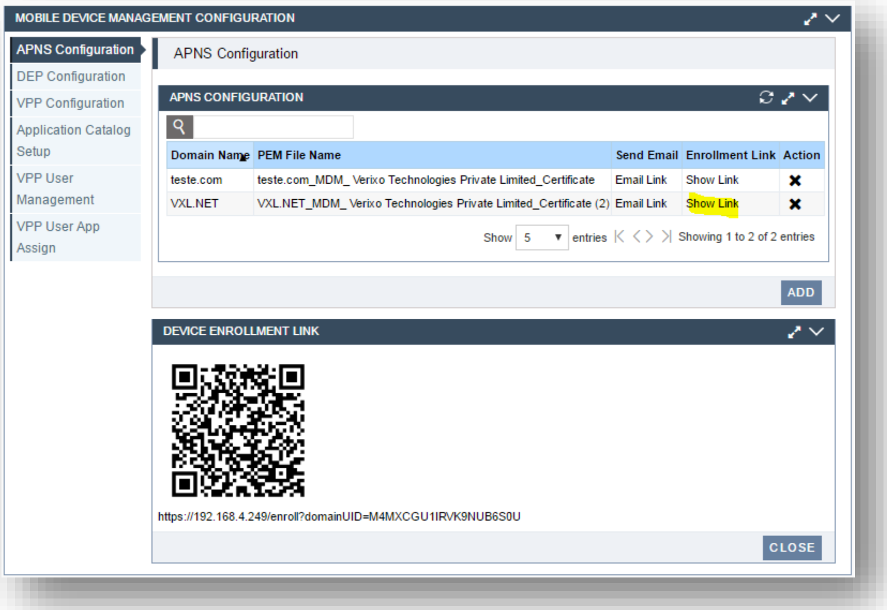
11. Browse to the .pem file which the user downloaded from Apple Push Certificates Portal.
12. Click on Enroll.
13. In the data table, enrolment link gets created with PEM name as description.



ADD APNS CONFIGURATION

* Alias / Name :	Apple Push
* Download Push CSR file :	Download
* Generate Certificate :	Identity link
* Select the file just downloaded from Apple :	MDM_ Verixo Technologies Private Limited_Certificate

14. Click on Show Link.



Domain Name	PEM File Name	Send Email	Enrollment Link	Action
teste.com	teste.com_MDM_ Verixo Technologies Private Limited_Certificate	Email Link	Show Link	✖
VXL.NET	VXL.NET_MDM_ Verixo Technologies Private Limited_Certificate (2)	Email Link	Show Link	✖

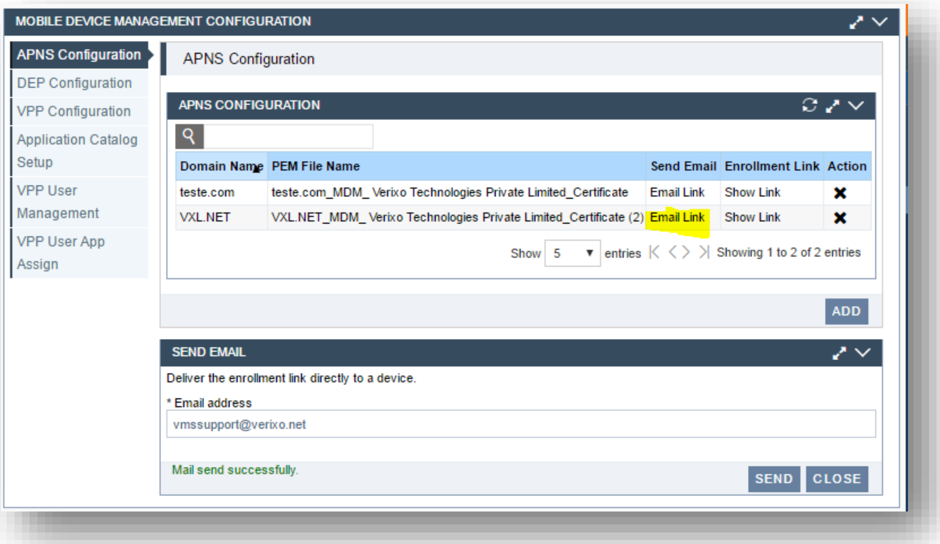
Show 5 entries Showing 1 to 2 of 2 entries

https://192.168.4.249/enroll?domainUID=M4MXCGU1IRVK9NUB6S0U

15. QR Code & Enrolment link gets displayed.

16. User is able to scan the QR Code from device using the QR scanning app or manually enter the URL given on the device browser.

17. User is also able to send the link by email by clicking on the email link and entering a valid email ID where the user wishes to send.



Domain Name	PEM File Name	Send Email	Enrollment Link	Action
teste.com	teste.com_MDM_ Verixo Technologies Private Limited_Certificate	Email Link	Show Link	✖
VXL.NET	VXL.NET_MDM_ Verixo Technologies Private Limited_Certificate (2)	Email Link	Show Link	✖

Show 5 entries Showing 1 to 2 of 2 entries

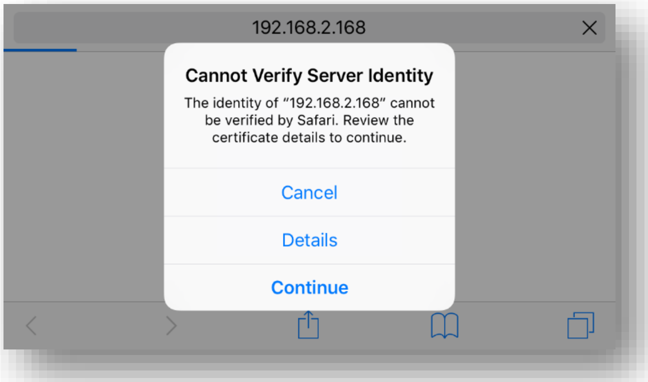
Deliver the enrollment link directly to a device.

* Email address

vmssupport@verixo.net

Mail send successfully.

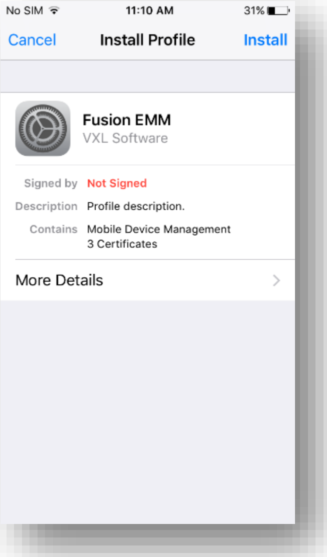
18. After entering or emailing the URL or scanning the QR Code, the user interaction popup is displayed.


192.168.2.168

Cannot Verify Server Identity

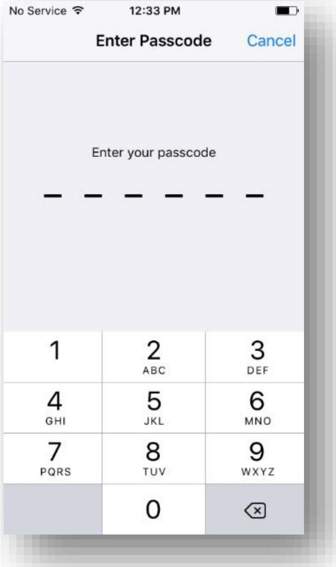
The identity of "192.168.2.168" cannot be verified by Safari. Review the certificate details to continue.

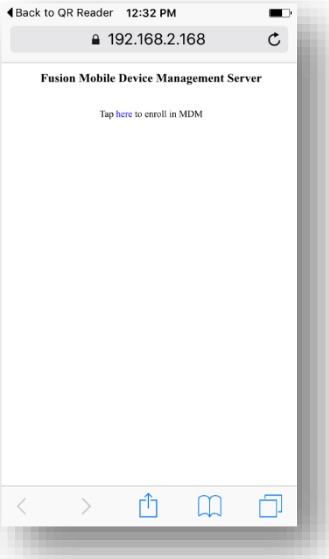
19. Click on Continue and proceed to the Installation process.



Fusion EMM
VXL Software

Signed by: Not Signed
Description: Profile description.
Contains: Mobile Device Management, 3 Certificates



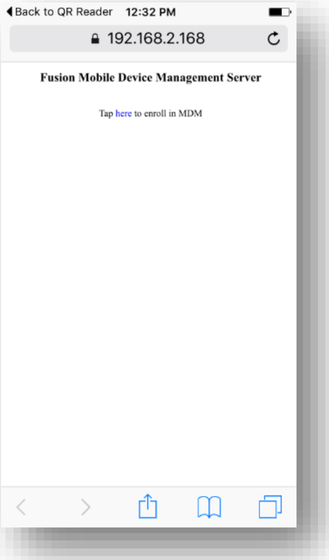


◀Back to QR Reader 12:32 PM

192.168.2.168

Fusion Mobile Device Management Server

Tap here to enroll in MDM

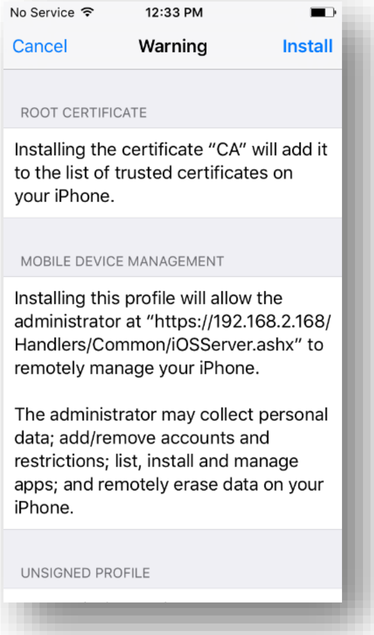


◀Back to QR Reader 12:32 PM

192.168.2.168

Fusion Mobile Device Management Server

Tap here to enroll in MDM



No Service 12:33 PM

Cancel **Warning** Install

ROOT CERTIFICATE

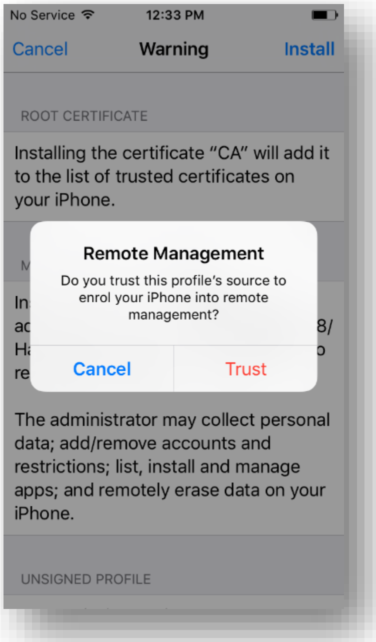
Installing the certificate “CA” will add it to the list of trusted certificates on your iPhone.

MOBILE DEVICE MANAGEMENT

Installing this profile will allow the administrator at “https://192.168.2.168/Handlers/Common/iOSServer.ashx” to remotely manage your iPhone.

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

UNSIGNED PROFILE



No Service 12:33 PM

Cancel **Warning** Install

ROOT CERTIFICATE

Installing the certificate “CA” will add it to the list of trusted certificates on your iPhone.

Remote Management

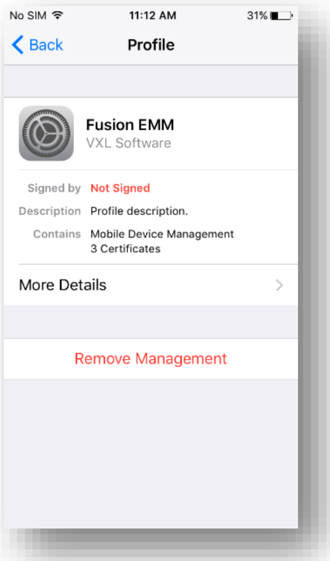
Do you trust this profile’s source to enrol your iPhone into remote management?

Cancel Trust

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

UNSIGNED PROFILE

20. After this click on ‘Done’.
21. On the Fusion EMM server, navigate to Discovery and click on register.
22. Select the device and click on register. The client gets registered successfully.
23. After configuring the profile on the iOS device, it will get listed in the General settings as displayed in the screen shot below:



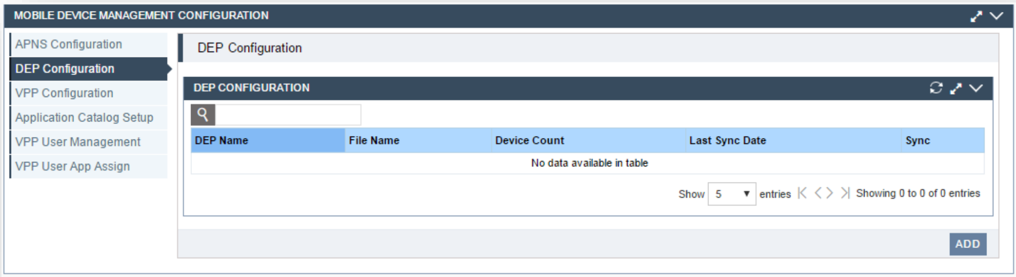
Fusion EMM
VXL Software

Signed by Not Signed
Description Profile description.
Contains Mobile Device Management
3 Certificates

DEP Configuration

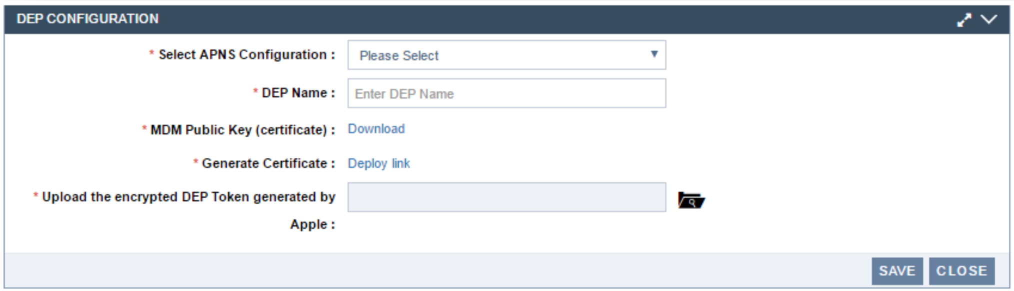
Apple's Device Enrollment Program is a way to automatically enroll a large number of devices wirelessly. DEP is a feature available only to paid accounts.

1. Navigate to Configuration Setup -> Apple MDM Configuration -> DEP Configuration



DEP Name	File Name	Device Count	Last Sync Date	Sync
		No data available in table		

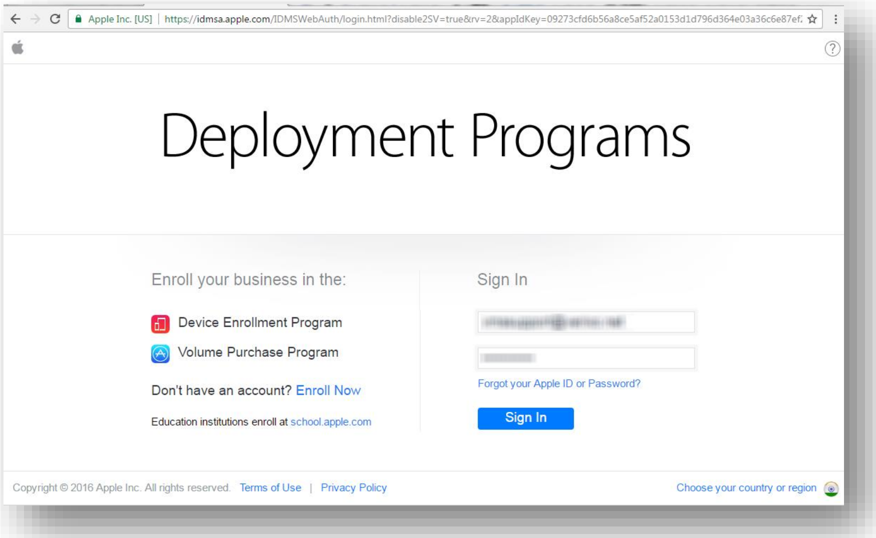
2. Click on Add.



DEP CONFIGURATION

* Select APNS Configuration : Please Select
* DEP Name : Enter DEP Name
* MDM Public Key (certificate) : Download
* Generate Certificate : Deploy link
* Upload the encrypted DEP Token generated by Apple :

3. Select APNS configuration from the drop down list which has been already created by the user in APNS configuration step above.
4. Enter DEP name.
5. Download MDM public key certificate (.crt file)
6. To get DEP token, click on Deploy link displayed against the Generate certificate field.



Apple Inc. [US] | https://idmsa.apple.com/IDMSWebAuth/login.html?disable2SV=true&rv=2&appIdKey=09273cfd6b56a8ce5af52a0153d1d796d364e03a36c6e87ef

Deployment Programs

Enroll your business in the:

Device Enrollment Program

Volume Purchase Program

Don't have an account? Enroll Now

Education institutions enroll at school.apple.com

Sign In

[redacted]

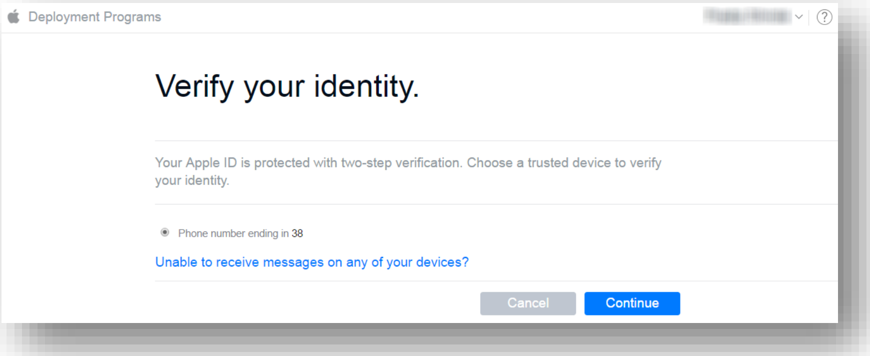
[redacted]

Forgot your Apple ID or Password?

Copyright © 2016 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

Choose your country or region

7. Choose a country as per requirement (e.g. United Kingdom)
8. Sign-in using a valid authentication and proceed to two step verification.



Deployment Programs [redacted]

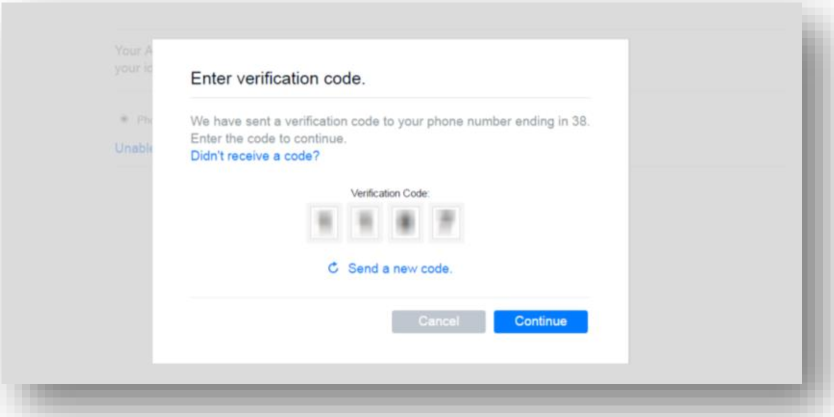
Verify your identity.

Your Apple ID is protected with two-step verification. Choose a trusted device to verify your identity.

● Phone number ending in 38

Unable to receive messages on any of your devices?

9. Enter the verification code received on the registered mobile number and proceed.



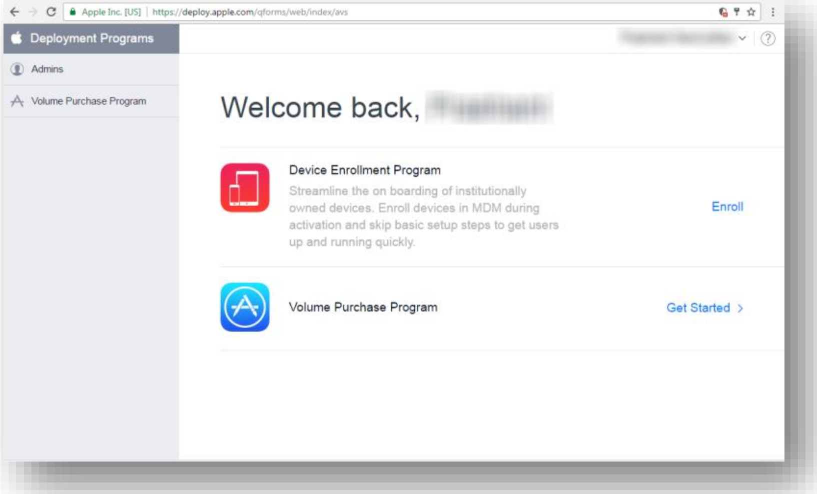
Enter verification code.

We have sent a verification code to your phone number ending in 38. Enter the code to continue.

Didn't receive a code?

Verification Code: [redacted]

10. Click on Get started of Device Enrollment program.



Apple Inc. [US] | https://deploy.apple.com/qforms/web/index/avs

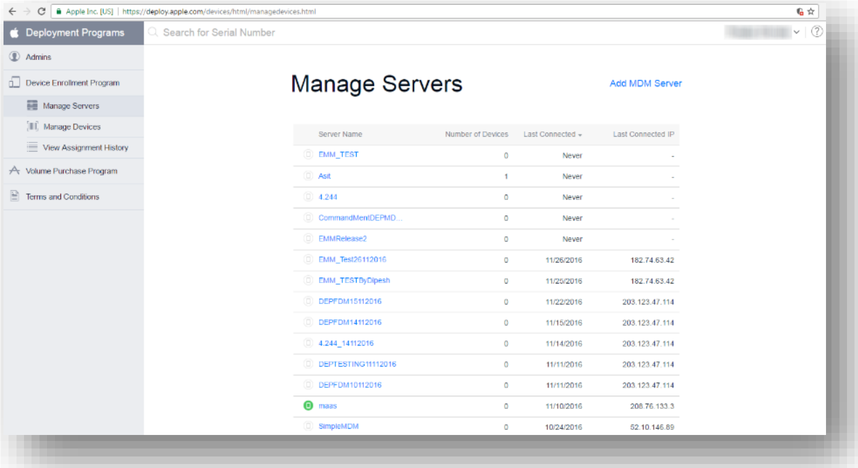
Welcome back, [redacted]

Device Enrollment Program

Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.

Volume Purchase Program

11. Complete MDM server list will be displayed.

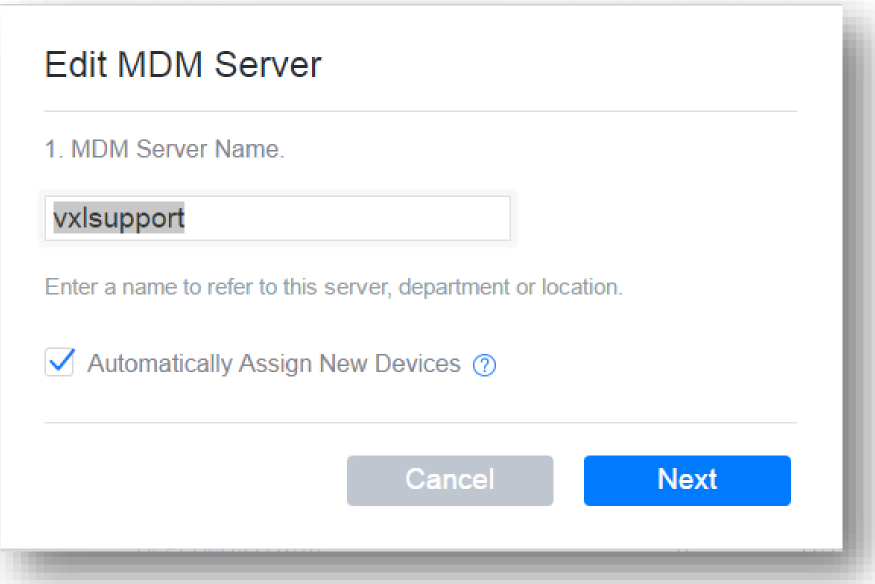


Manage Servers

Server Name	Number of Devices	Last Connected	Last Connected IP
EMM_TEST	0	Never	-
Asit	1	Never	-
4.244	0	Never	-
CommandMentDEPMD...	0	Never	-
EMMRelease2	0	Never	-
EMM_Test26112016	0	11/26/2016	182.74.63.42
EMM_TESTByDipesh	0	11/25/2016	182.74.63.42
DEPFDM15112016	0	11/22/2016	203.123.47.114
DEPFDM14112016	0	11/15/2016	203.123.47.114
4.244_14112016	0	11/14/2016	203.123.47.114
DEPTESTING11112016	0	11/11/2016	203.123.47.114
DEPFDM10112016	0	11/11/2016	203.123.47.114
maas	0	11/10/2016	208.76.133.3
SimpleMDM	0	10/24/2016	52.10.146.89

12. Click on Add MDM server.

13. Enter MDM server name and click on Next.



Edit MDM Server

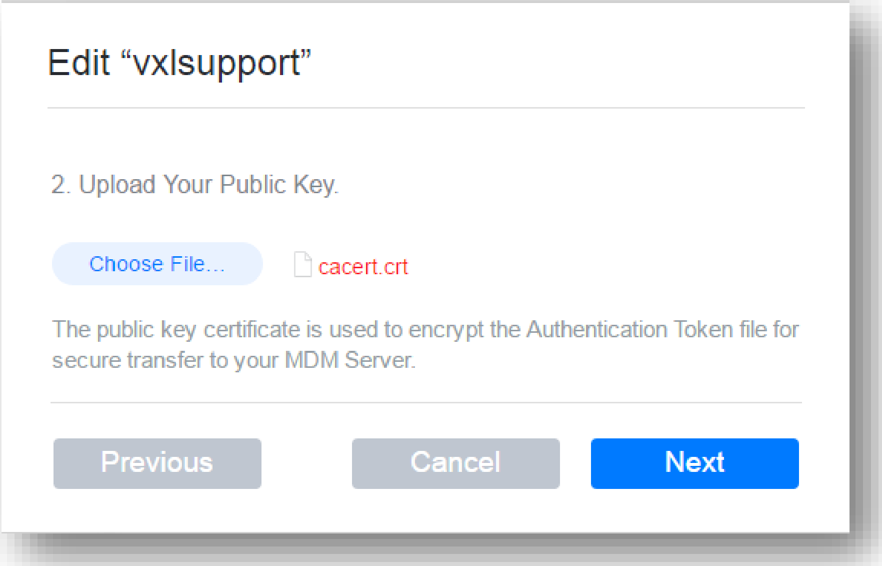
1. MDM Server Name.

vxlsupport

Enter a name to refer to this server, department or location.

☑ Automatically Assign New Devices

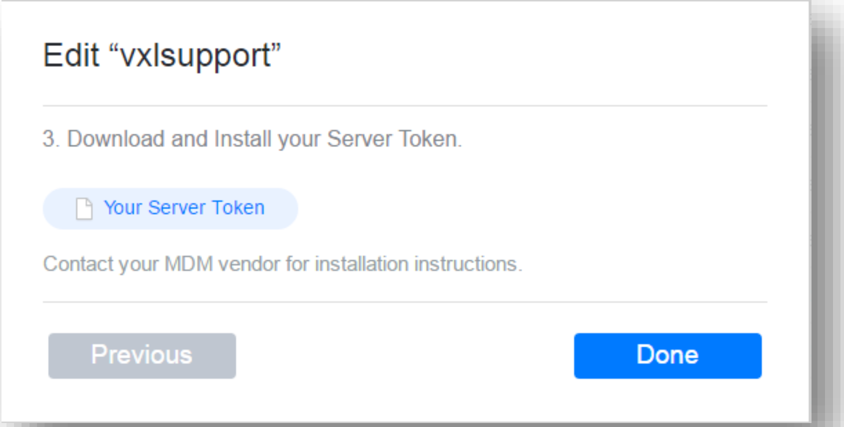
14. Upload the certificate which the user downloaded in Step 6 and click on Next.


Edit “vxlsupport”

2. Upload Your Public Key.

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

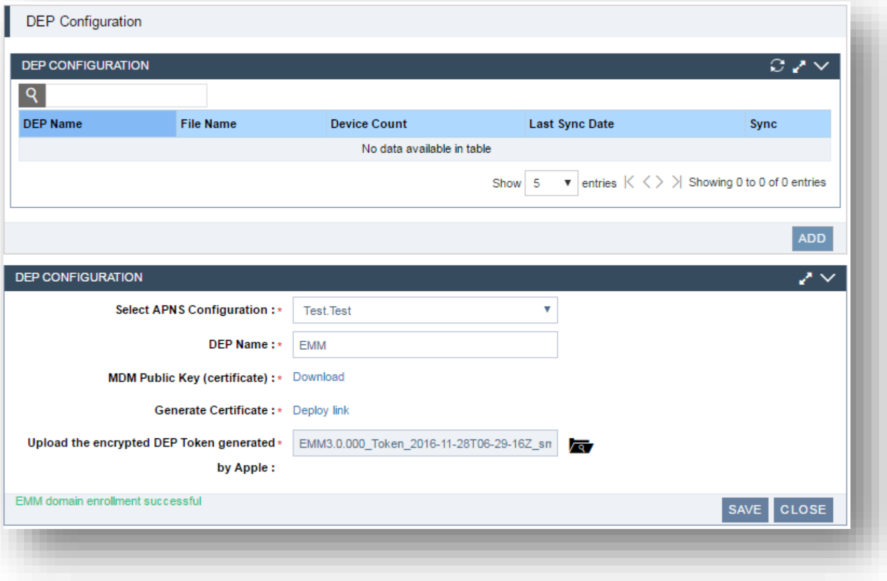
15. User has to download the DEP server token (.p7m file)


Edit “vxlsupport”

3. Download and Install your Server Token.

Contact your MDM vendor for installation instructions.

16. Upload the DEP server token in DEP configuration form which the user downloaded in Step 15.
17. Click on save.



DEP Configuration

DEP CONFIGURATION

DEP Name	File Name	Device Count	Last Sync Date	Sync
No data available in table				

Show 5 entries Showing 0 to 0 of 0 entries

ADD

DEP CONFIGURATION

Select APNS Configuration :* Test.Test

DEP Name :* EMM

MDM Public Key (certificate) :* Download

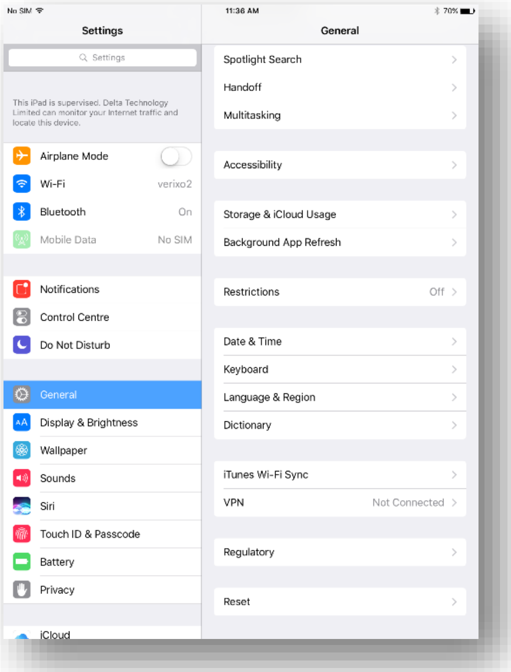
Generate Certificate :* Deploy link

Upload the encrypted DEP Token generated by Apple :* EMM3.0.000_Token_2016-11-28T06-29-16Z_sn

EMM domain enrollment successful

SAVE CLOSE

18. If valid data is entered then ‘Domain enrollment successful’ message will be displayed.
19. User has to reset the device by navigating to Settings -> General Settings -> Reset.
20. After the device is reset, it gets listed in the Fusion EMM server -> Discovery view -> register tab.



No SIM 11:36 AM 70%

Settings

This iPad is supervised. Delta Technology Limited can monitor your Internet traffic and locate this device.

21. Select the device and click on register. Device gets listed in the tree view.

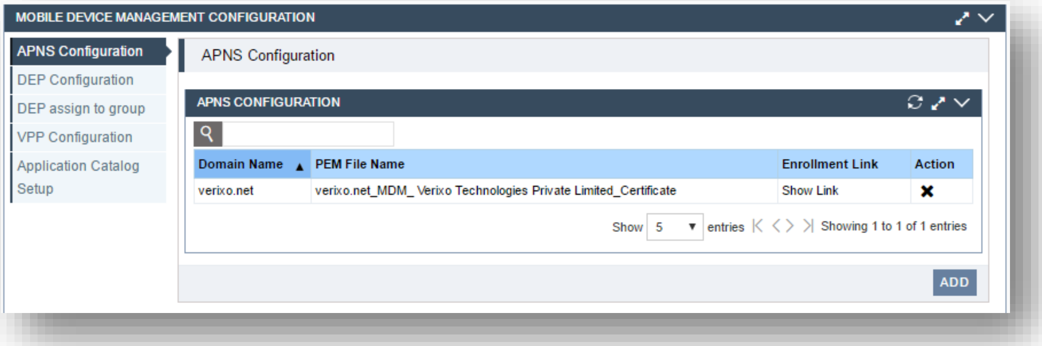
Configuration Setup for Apple MDM

APNS Configuration

User have to configure by APNS for user registration process.

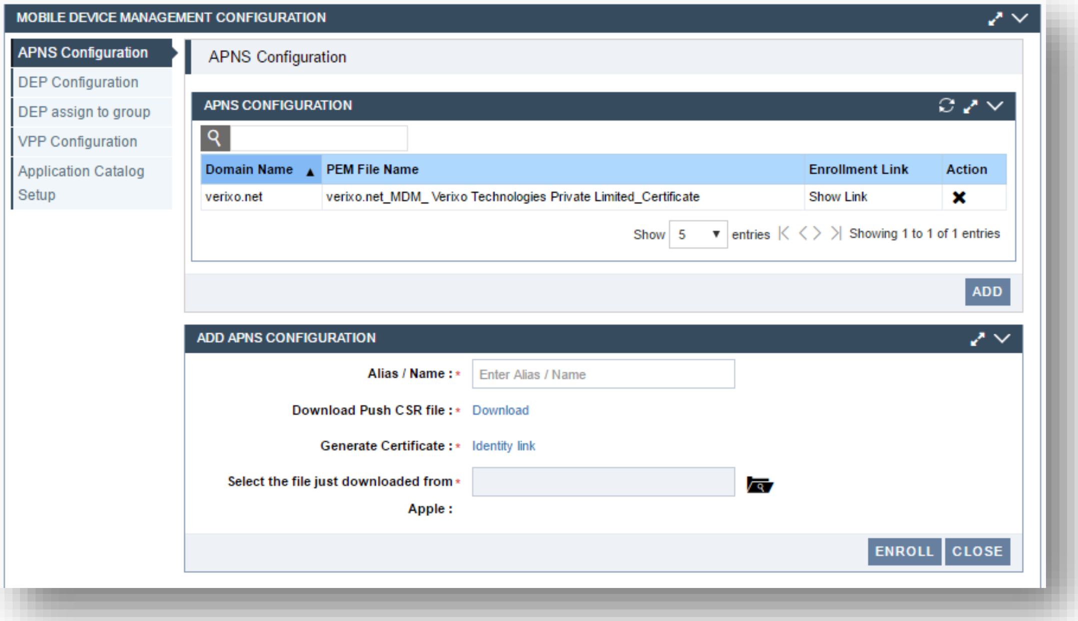
User have to go through enrolment process for Apple push certificate.

24. Fusion EMM Server -> Go to Configuration Setup-> Apple MDM configuration -> APNS Configuration
25. Click on Add button



Domain Name ▲	PEM File Name	Enrollment Link	Action
verixo.net	verixo.net_MDM_ Verixo Technologies Private Limited_Certificate	Show Link	✖

26. Download apple push .csr file.



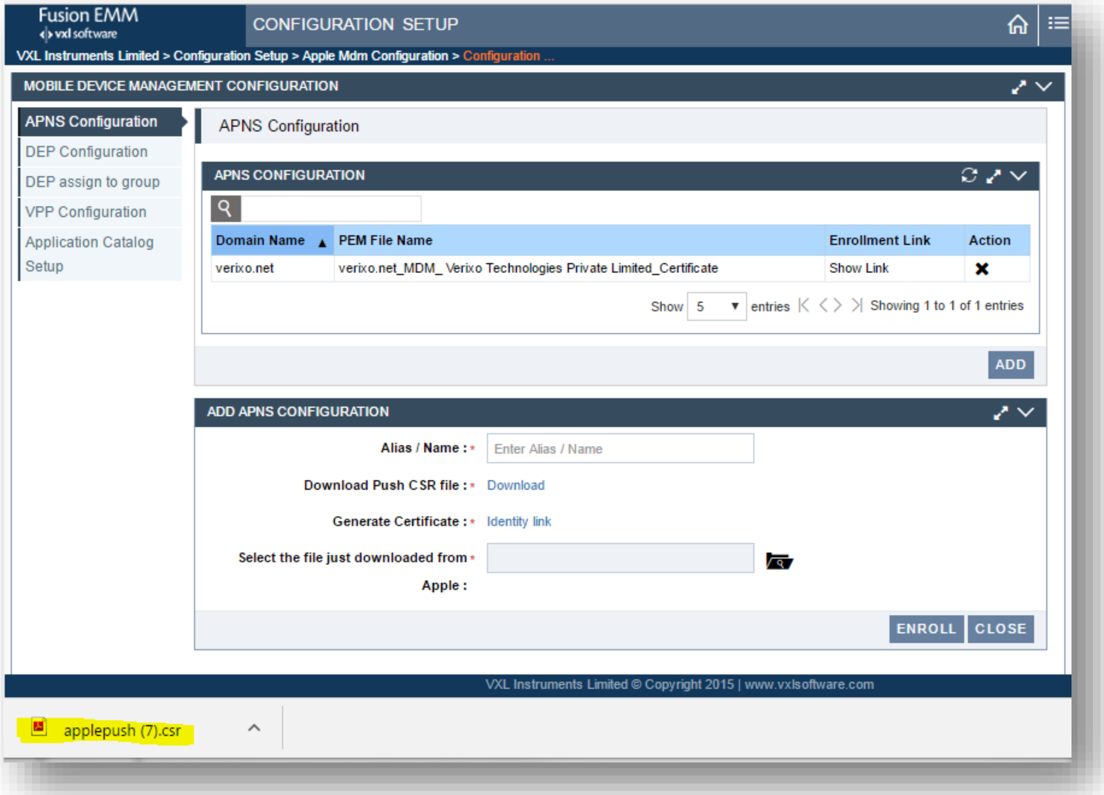
Domain Name ▲	PEM File Name	Enrollment Link	Action
verixo.net	verixo.net_MDM_ Verixo Technologies Private Limited_Certificate	Show Link	✖

Alias / Name : * Enter Alias / Name

Download Push CSR file : * Download

Generate Certificate : * Identity link

Select the file just downloaded from Apple : *



VXL Instruments Limited > Configuration Setup > Apple Mdm Configuration > Configuration ...

MOBILE DEVICE MANAGEMENT CONFIGURATION

APNS Configuration

APNS CONFIGURATION

Domain Name	PEM File Name	Enrollment Link	Action
verixo.net	verixo.net_MDM_ Verixo Technologies Private Limited_Certificate	Show Link	✖

Show 5 entries Showing 1 to 1 of 1 entries

ADD APNS CONFIGURATION

Alias / Name : * Enter Alias / Name

Download Push CSR file : * Download

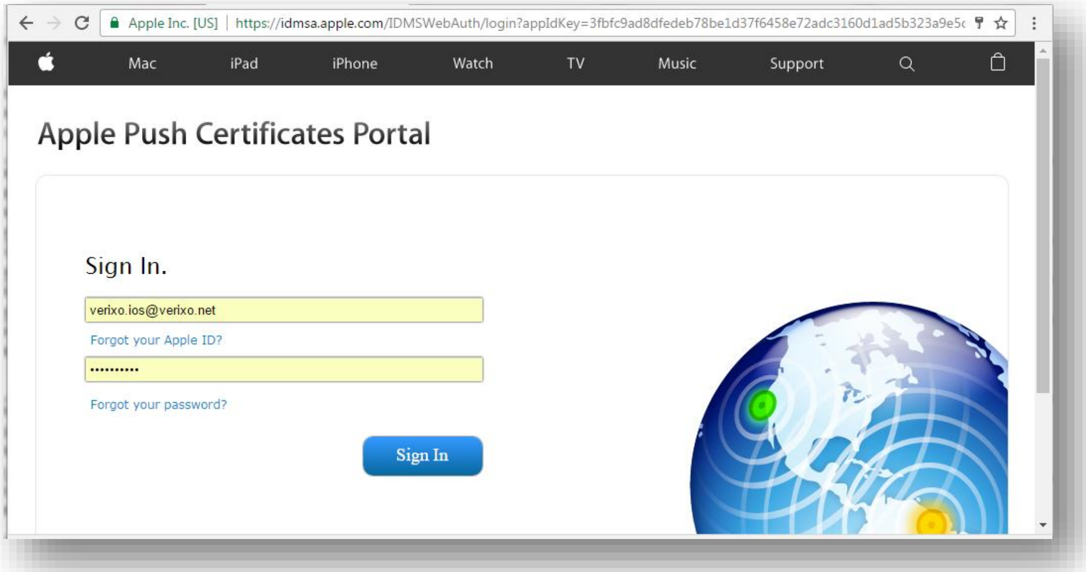
Generate Certificate : * Identity link

Select the file just downloaded from Apple : *

VXL Instruments Limited © Copyright 2015 | www.vxlsoftware.com

applepush (7).csr

27. Go To site https://identity.apple.com/pushcert/
28. Sign in with enterprise account.



Apple Inc. [US] | https://idmsa.apple.com/IDMSWebAuth/login?appIdKey=3fbfc9ad8dfedeb78be1d37f6458e72adc3160d1ad5b323a9e5c

Apple Push Certificates Portal

Sign In.

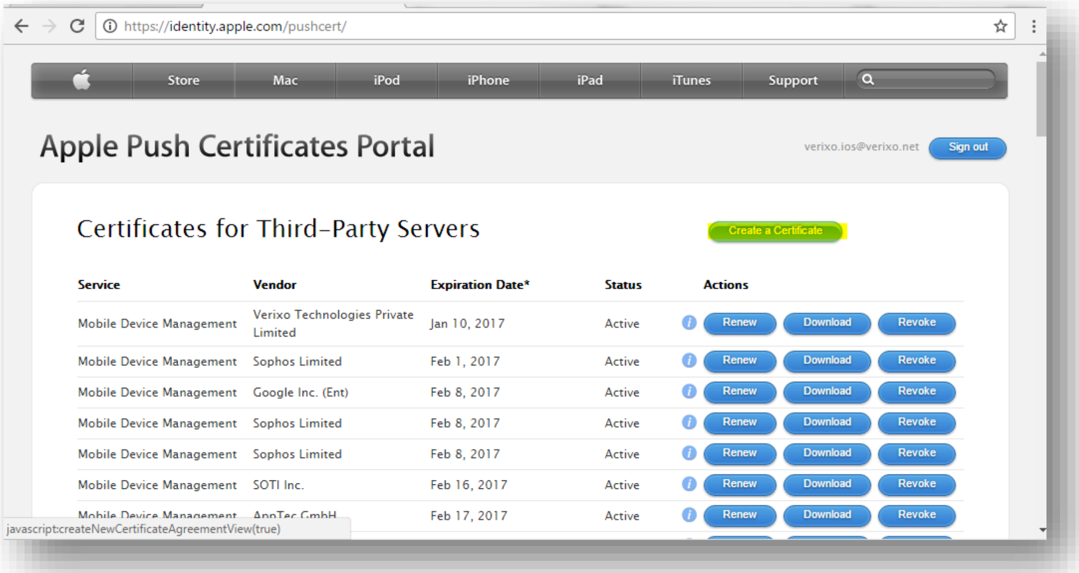
verixo.ios@verixo.net

Forgot your Apple ID?

••••••••••

Forgot your password?

29. Click on Create Certificate.



Apple Push Certificates Portal

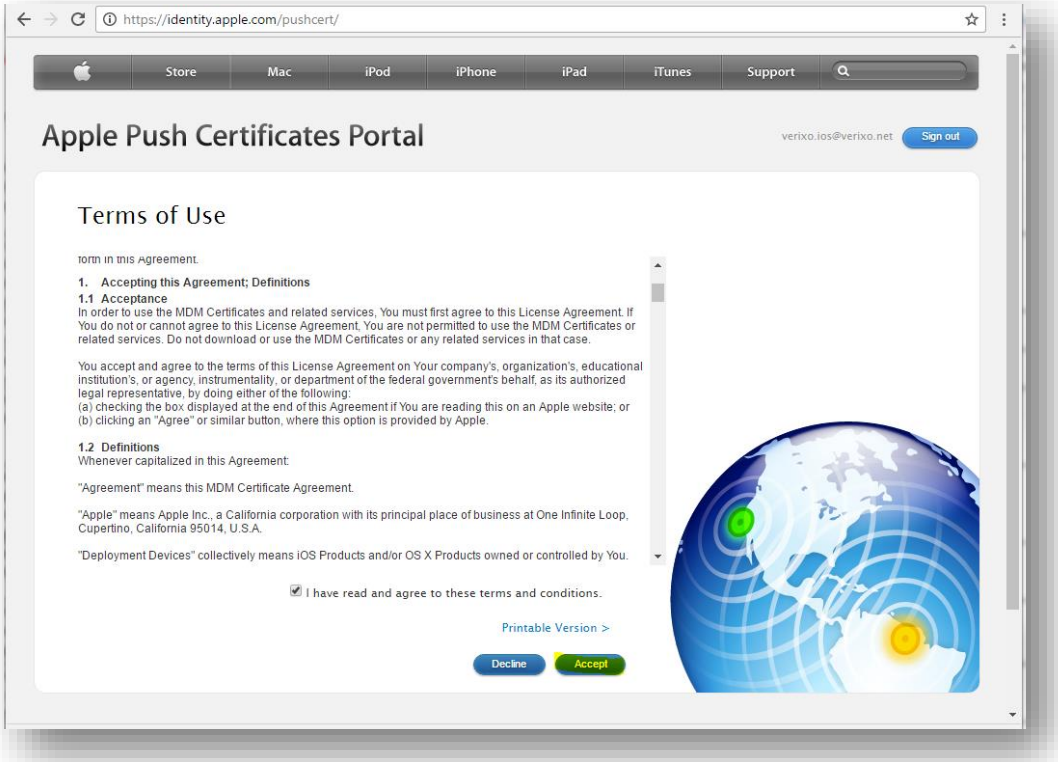
verixo.ios@verixo.net Sign out

Certificates for Third-Party Servers

Create a Certificate

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Verixo Technologies Private Limited	Jan 10, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 1, 2017	Active	Renew Download Revoke
Mobile Device Management	Google Inc. (Ent)	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	Sophos Limited	Feb 8, 2017	Active	Renew Download Revoke
Mobile Device Management	SOTI Inc.	Feb 16, 2017	Active	Renew Download Revoke
Mobile Device Management	AppTec GmbH	Feb 17, 2017	Active	Renew Download Revoke

javascript:createNewCertificateAgreementView(true)



Apple Push Certificates Portal

verixo.ios@verixo.net Sign out

Terms of Use

forth in this Agreement.

1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the MDM Certificates and related services, You must first agree to this License Agreement. If You do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates or related services. Do not download or use the MDM Certificates or any related services in that case.

You accept and agree to the terms of this License Agreement on Your company's, organization's, educational institution's, or agency, instrumentality, or department of the federal government's behalf, as its authorized legal representative, by doing either of the following:
(a) checking the box displayed at the end of this Agreement if You are reading this on an Apple website; or
(b) clicking an "Agree" or similar button, where this option is provided by Apple.

1.2 Definitions

Whenever capitalized in this Agreement:

"Agreement" means this MDM Certificate Agreement.

"Apple" means Apple Inc., a California corporation with its principal place of business at One Infinite Loop, Cupertino, California 95014, U.S.A.

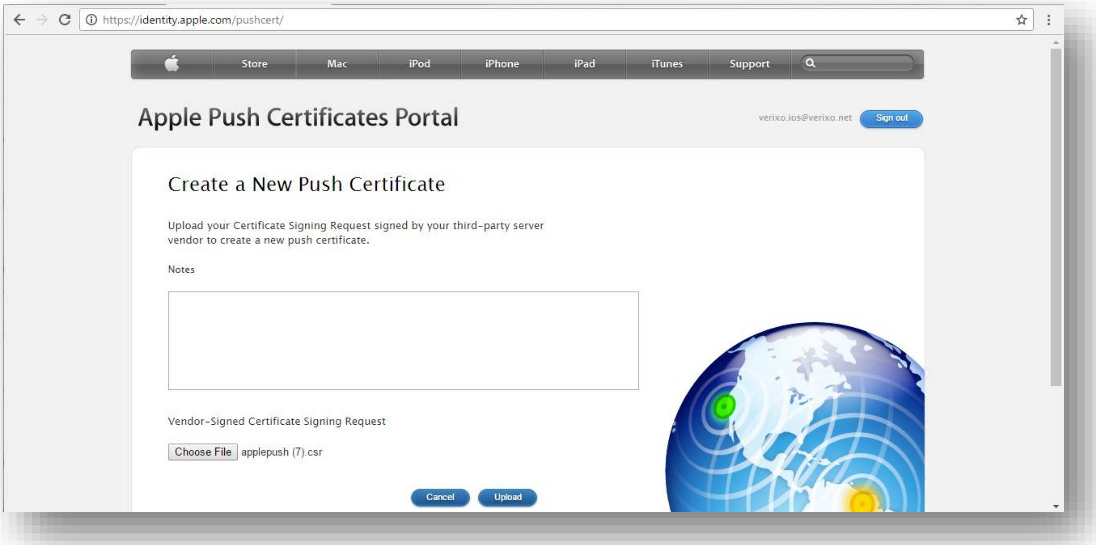
"Deployment Devices" collectively means iOS Products and/or OS X Products owned or controlled by You.

☑ I have read and agree to these terms and conditions.

Printable Version >

Decline Accept

30. Click on Upload & Browse downloaded .csr file.



Apple Push Certificates Portal

Create a New Push Certificate

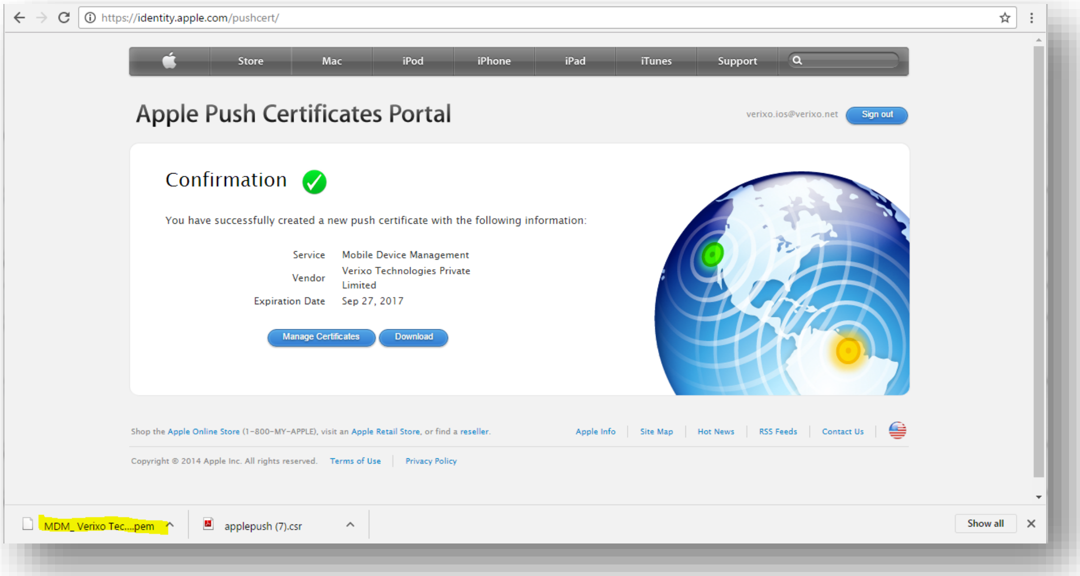
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

Vendor-Signed Certificate Signing Request

applepush (7).csr

31. Click on Download button.
32. .pem file gets download, from Fusion EMM server -> APNS -> click on Add



Apple Push Certificates Portal

Confirmation ✓

You have successfully created a new push certificate with the following information:

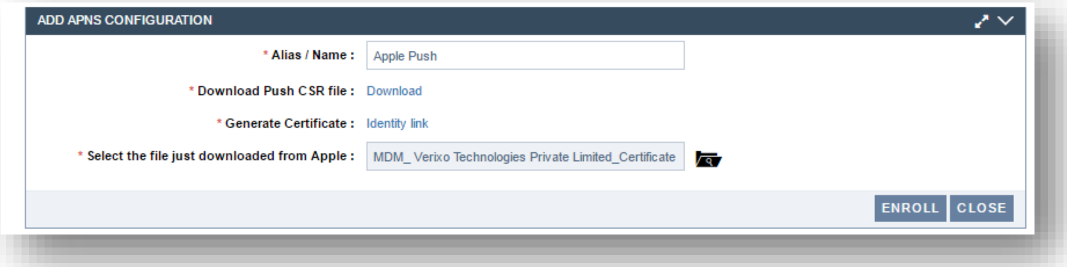
Service	Mobile Device Management
Vendor	Verixo Technologies Private Limited
Expiration Date	Sep 27, 2017

Shop the Apple Online Store (1-800-MY-APPLE), visit an Apple Retail Store, or find a reseller.

Copyright © 2014 Apple Inc. All rights reserved.

33. Browse .pem file which user downloaded from create password process.
34. Click on Enroll.

35. In data table enrolment link get created with PEM name description.



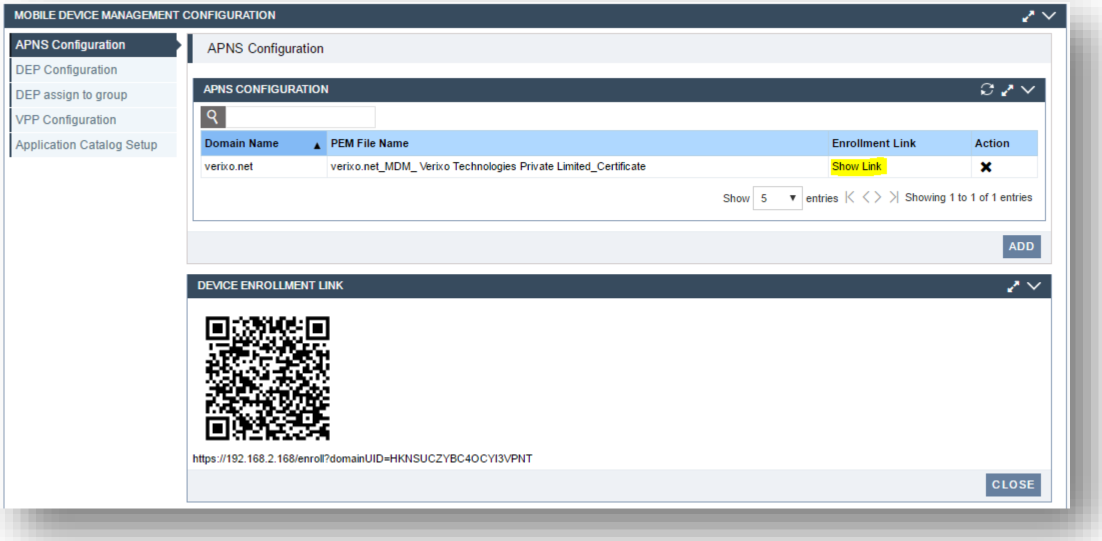
* Alias / Name : Apple Push

* Download Push CSR file : Download

* Generate Certificate : Identity link

* Select the file just downloaded from Apple : MDM_ Verixo Technologies Private Limited_Certificate

36. Click on Show Link.
37. QR code & Enrollment link gets displayed.
38. User able to scan QR code from device by QR scanning app or manually enter url given on device browser.
39. After entering url or scanning code-> User interaction popup displayed.
40. Click on Continue & go for Installation process.
41. After click on Done
42. On Fusion EMM server go to Discovery -> Click on register -> check request initiated tab, client get discover.
43. Select device, Click on register. Client gets register successfully.



Domain Name ▲	PEM File Name	Enrollment Link	Action
verixo.net	verixo.net_MDM_ Verixo Technologies Private Limited_Certificate	Show Link	✖

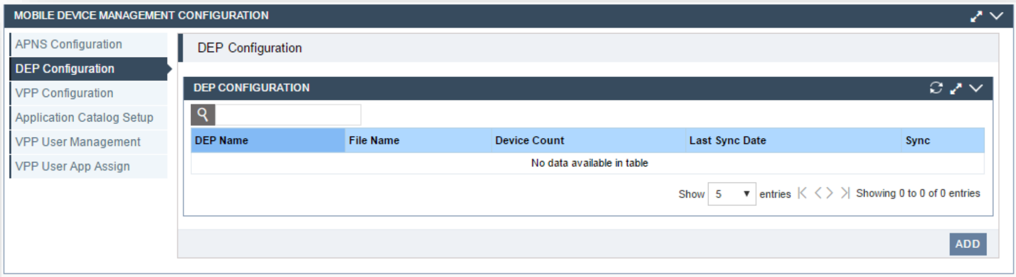
Show 5 ▾ entries Showing 1 to 1 of 1 entries

https://192.168.2.168/enroll?domainUID=HKNSUCZYBC4OCYI3VPNT

DEP Configuration

Apple's Device Enrollment Program is a way to automatically enroll a large number of devices wirelessly. DEP is a feature available only to paid accounts.

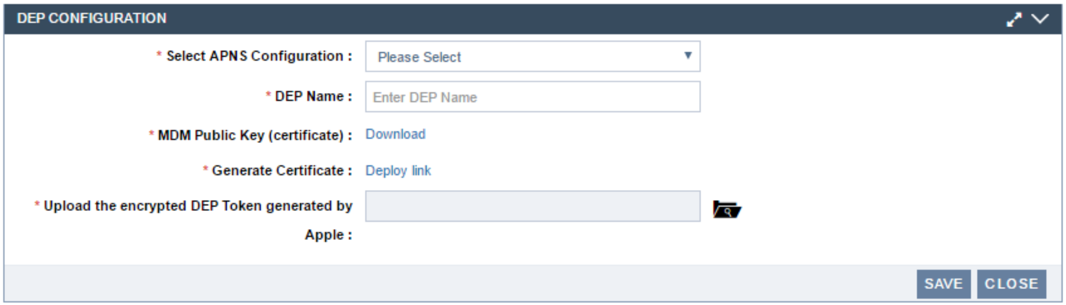
22. Go to configuration setup> Apple MDM configuration.
23. Select DEP configuration.



DEP Name	File Name	Device Count	Last Sync Date	Sync
No data available in table				

Showing 0 to 0 of 0 entries

24. Click on Add.



* Select APNS Configuration : Please Select

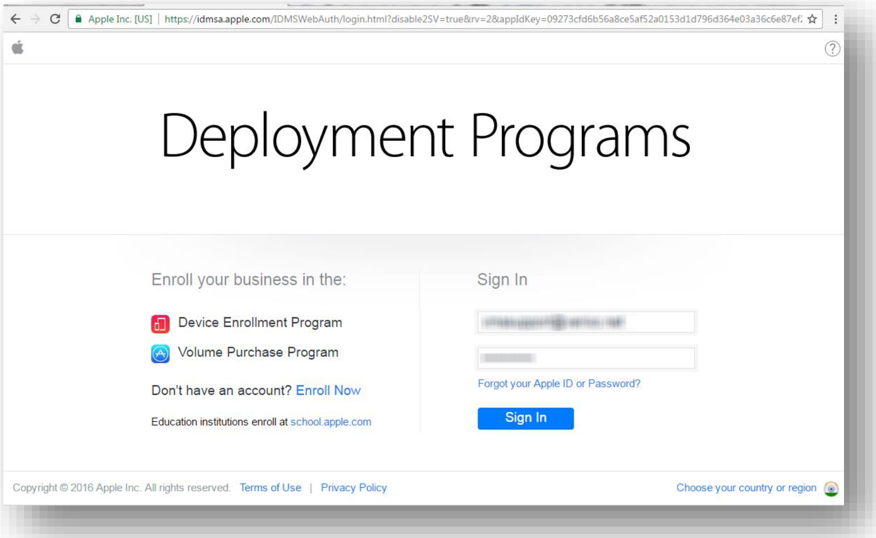
* DEP Name : Enter DEP Name

* MDM Public Key (certificate) : Download

* Generate Certificate : Deploy link

* Upload the encrypted DEP Token generated by Apple :

25. Select APNS configuration from drop down list which user already created in APNS configuration form.
26. Enter DEP name.
27. Download MDM public key certificate.(.crt)
28. To get DEP token click on Generate certificate deploy link.


Apple Inc. [US] | https://idmsa.apple.com/IDMSWebAuth/login.html?disable2SV=true&rv=2&appIdKey=09273cfd6b56a8ce5af52a0153d1d796d364e03a36c6e87ef

Deployment Programs

Enroll your business in the:

Device Enrollment Program

Volume Purchase Program

Don't have an account? Enroll Now

Education institutions enroll at school.apple.com

Sign In

[redacted]

[redacted]

Forgot your Apple ID or Password?

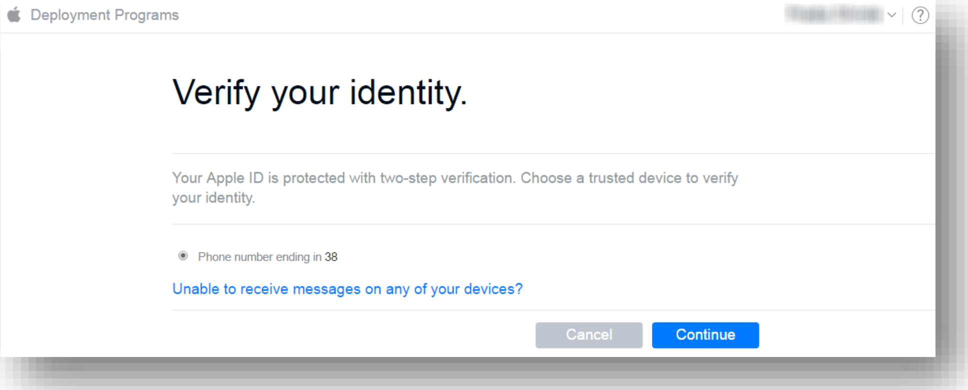
Sign In

Copyright © 2016 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

Choose your country or region

29. Choose country as per user request.(e.g. United kingdom)

30. Sign in with valid authentication & proceed two step verification.


Deployment Programs [redacted]

Verify your identity.

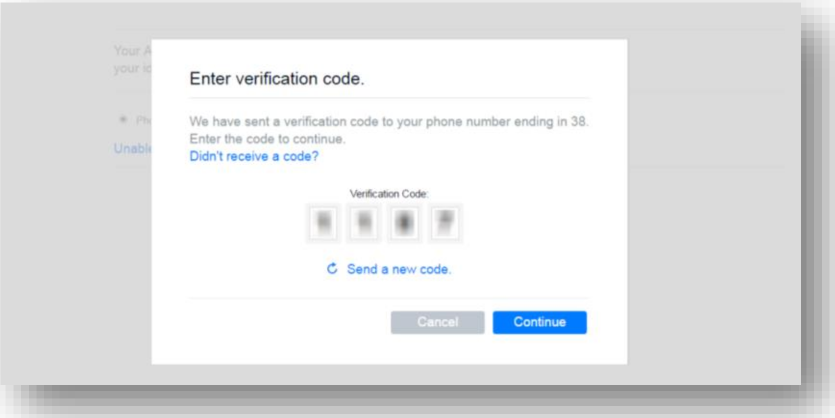
Your Apple ID is protected with two-step verification. Choose a trusted device to verify your identity.

● Phone number ending in 38

Unable to receive messages on any of your devices?

Cancel Continue

31. Enter verification code received on registered mobile number & proceed.



Enter verification code.

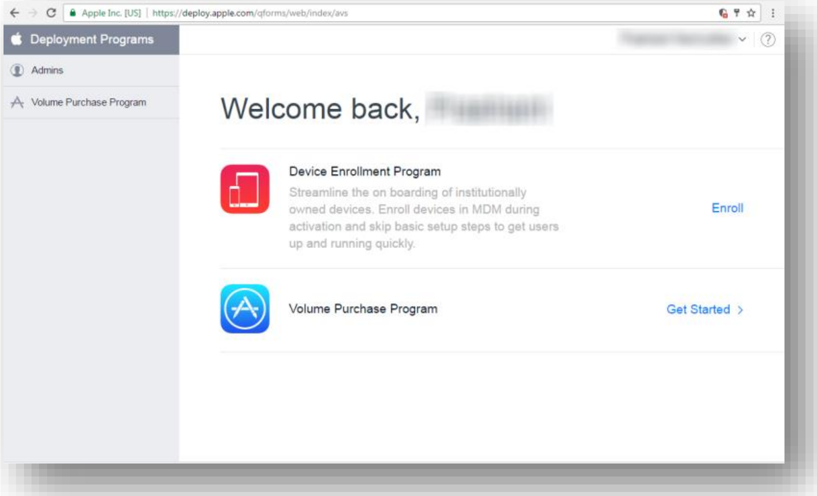
We have sent a verification code to your phone number ending in 38. Enter the code to continue.

Didn't receive a code?

Verification Code:

[redacted]

32. Click on Get started of Device Enrollment program.



https://deploy.apple.com/qforms/web/index/avs

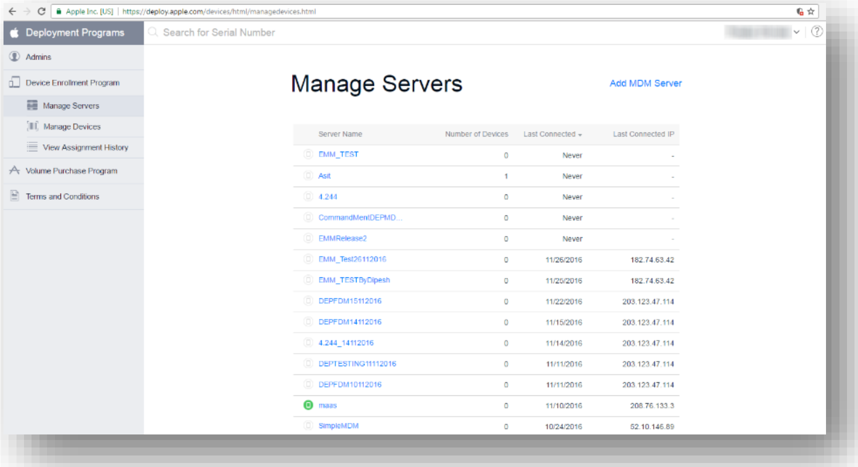
Welcome back, [redacted]

Device Enrollment Program

Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.

Volume Purchase Program

33. User will get all MDM server list.



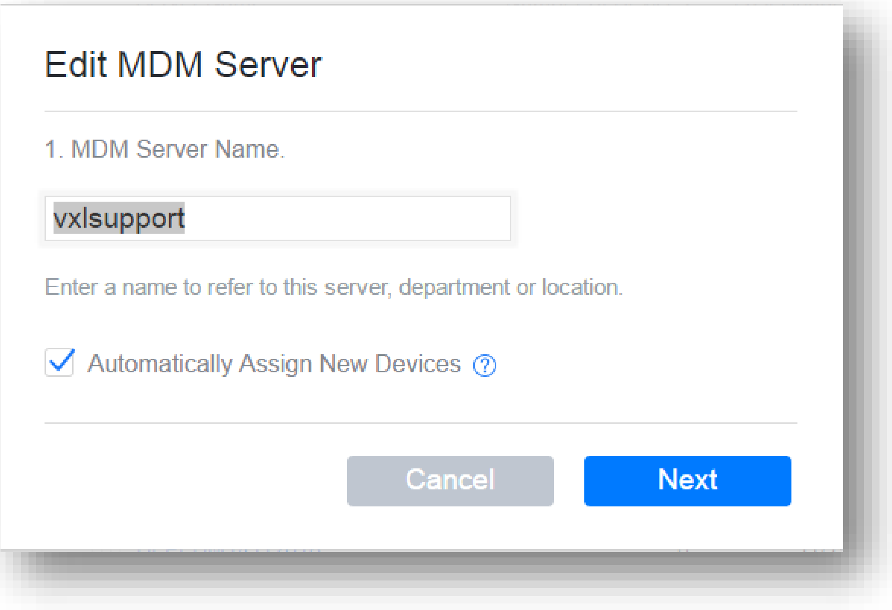
https://deploy.apple.com/devices/html/managedevices.html

Manage Servers

Server Name	Number of Devices	Last Connected	Last Connected IP
EMM_TEST	0	Never	-
Asit	1	Never	-
4.244	0	Never	-
CommandMentDEPMD...	0	Never	-
EMMRelease2	0	Never	-
EMM_Test26112016	0	11/26/2016	182.74.63.42
EMM_TESTByDipesh	0	11/25/2016	182.74.63.42
DEPFDM15112016	0	11/22/2016	203.123.47.114
DEPFDM14112016	0	11/15/2016	203.123.47.114
4.244_14112016	0	11/14/2016	203.123.47.114
DEPTESTING11112016	0	11/11/2016	203.123.47.114
DEPFDM10112016	0	11/11/2016	203.123.47.114
maas	0	11/10/2016	208.76.133.3
SimpleMDM	0	10/24/2016	52.10.146.89

34. Click on Add MDM server.

35. Enter MDM server name & click on Next.



Edit MDM Server

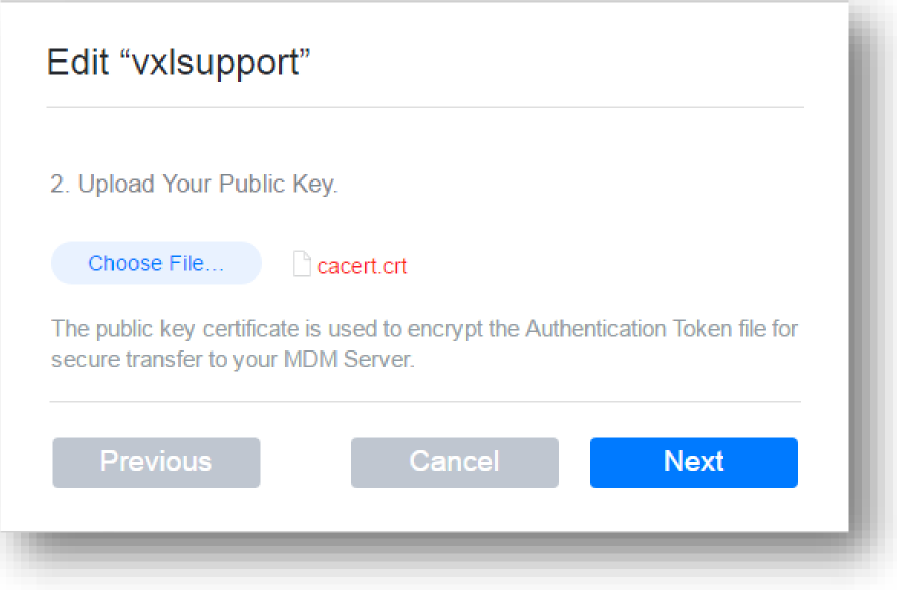
1. MDM Server Name.

vxlsupport

Enter a name to refer to this server, department or location.

☑ Automatically Assign New Devices

36. Upload certificate which user downloaded in Step 6 & click on Next.



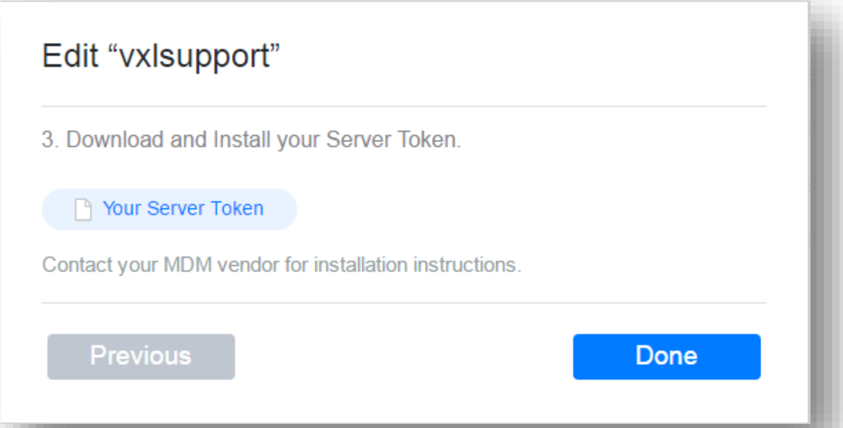
Edit “vxlsupport”

2. Upload Your Public Key.

cacert.crt

The public key certificate is used to encrypt the Authentication Token file for secure transfer to your MDM Server.

37. User have to download DEP server token.(.p7m)



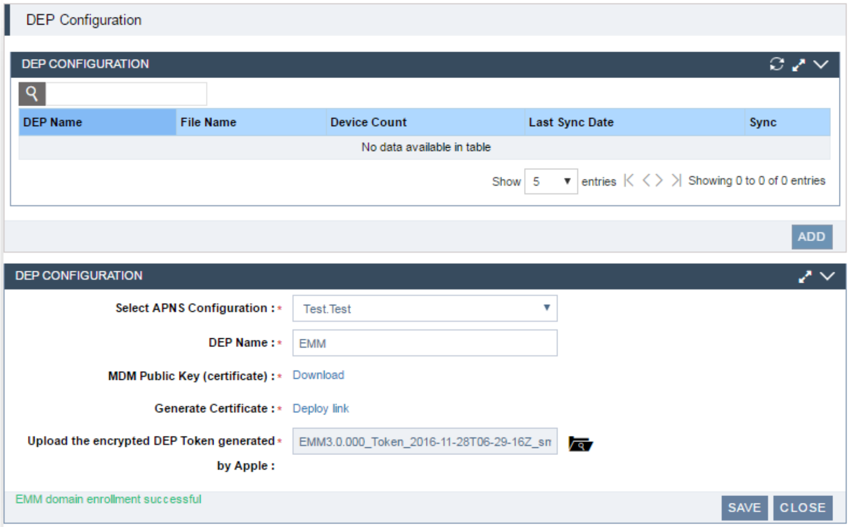
Edit “vxlsupport”

3. Download and Install your Server Token.

Contact your MDM vendor for installation instructions.

38. Upload DEP server token in DEP configuration form which user downloaded in Step 16.

39. Click on save.



DEP Configuration

DEP CONFIGURATION

DEP Name	File Name	Device Count	Last Sync Date	Sync
No data available in table				

Show 5 entries Showing 0 to 0 of 0 entries

DEP CONFIGURATION

Select APNS Configuration : *	Test.Test
DEP Name : *	EMM
MDM Public Key (certificate) : *	Download
Generate Certificate : *	Deploy link
Upload the encrypted DEP Token generated by Apple : *	EMM3.0.000_Token_2016-11-28T06-29-16Z_sn

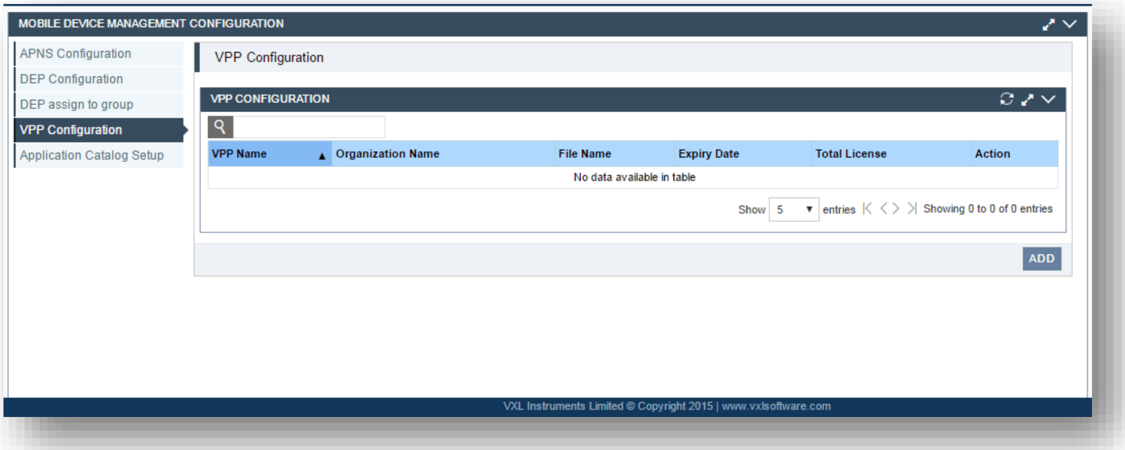
EMM domain enrollment successful

40. If valid data entered then only, “Domain enrollment successfully” message will get displayed.

VPP Configuration

User able to add token for application store.

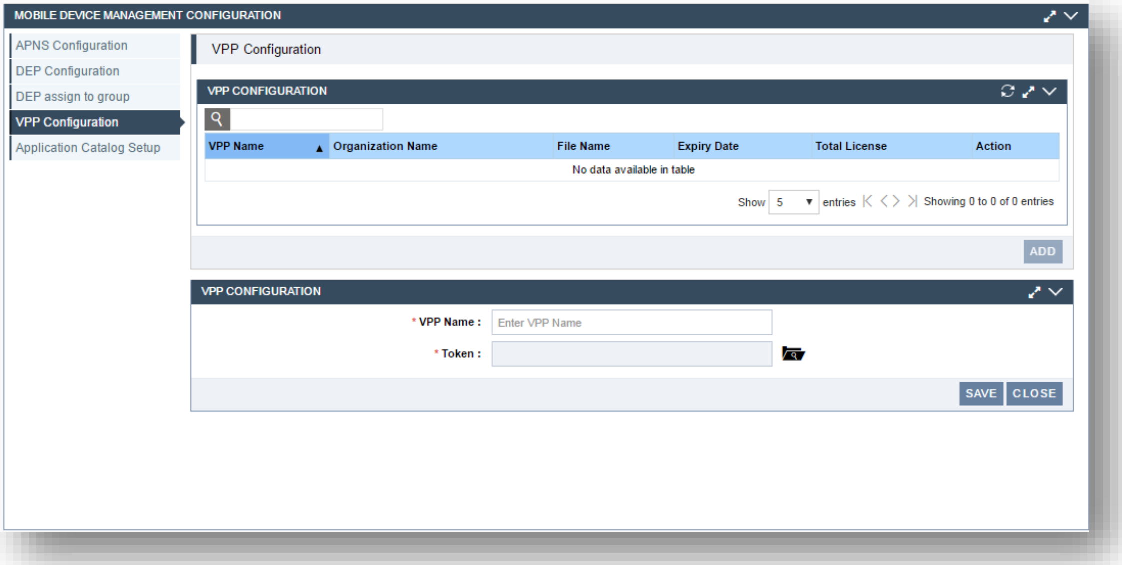
1. Go to Configuration Setup -> click on Apple MDM configuration then click on VPP configuration.
2. Click on ADD.


MOBILE DEVICE MANAGEMENT CONFIGURATION
APNS Configuration
DEP Configuration
DEP assign to group
VPP Configuration
Application Catalog Setup
VPP Configuration
VPP CONFIGURATION
Show 5 entries
ADD
VXL Instruments Limited © Copyright 2015 | www.vxlsoftware.com

VPP Name	Organization Name	File Name	Expiry Date	Total License	Action
No data available in table					

Showing 0 to 0 of 0 entries

3. User have to enter VPP name & browse token.



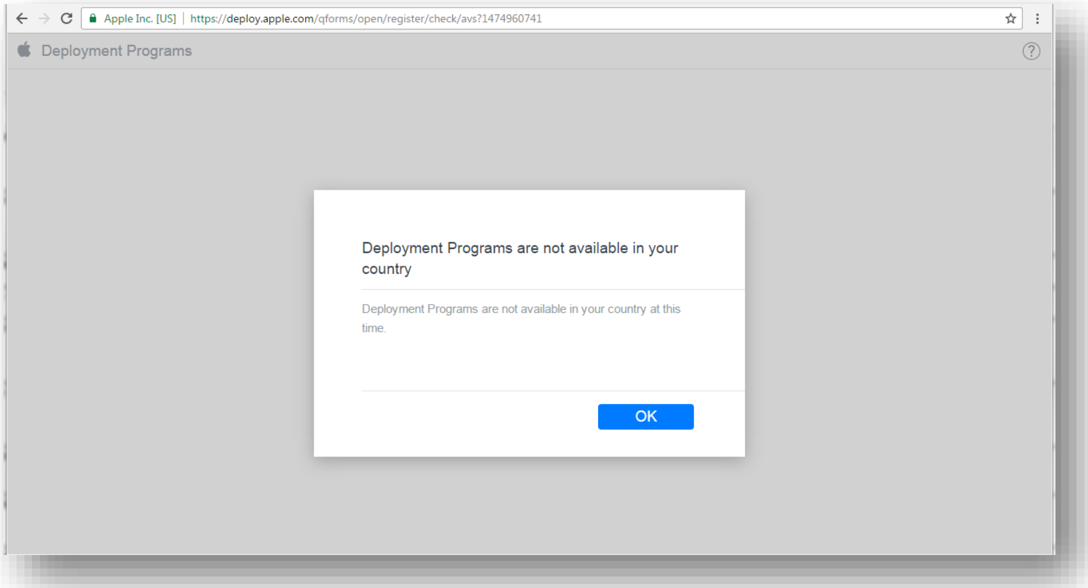
VPP Name	Organization Name	File Name	Expiry Date	Total License	Action
No data available in table					

Showing 0 to 0 of 0 entries

* VPP Name : Enter VPP Name

* Token :

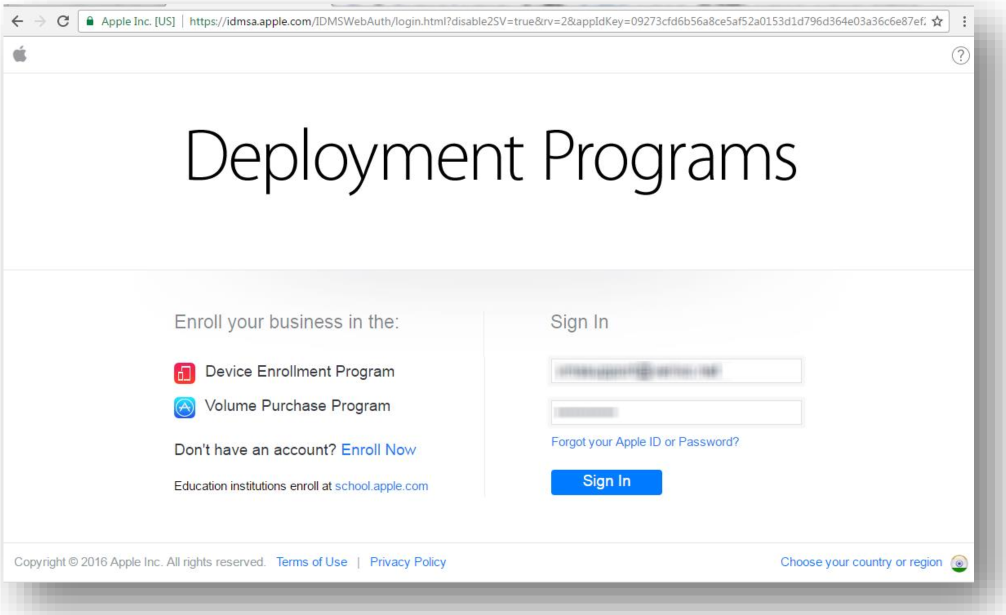
4. To get Token user have to login on site https://deploy.apple.com/
5. If deployment programme are not available in your country? Then user able to change country from right side drop down.


Apple Inc. [US]
https://deploy.apple.com/qforms/open/register/check/avs?1474960741
Deployment Programs
?

Deployment Programs are not available in your country

Deployment Programs are not available in your country at this time.

6. Sign in with VPP ID


Apple Inc. [US]
https://idmsa.apple.com/IDMSWebAuth/login.html?disable2SV=true&rv=2&appIdKey=09273cfd6b56a8ce5af52a0153d1d796d364e03a36c6e87ef.
?

Deployment Programs

Enroll your business in the:

- Device Enrollment Program
- Volume Purchase Program

Don't have an account? Enroll Now

Education institutions enroll at school.apple.com

Sign In

[redacted]

[redacted]

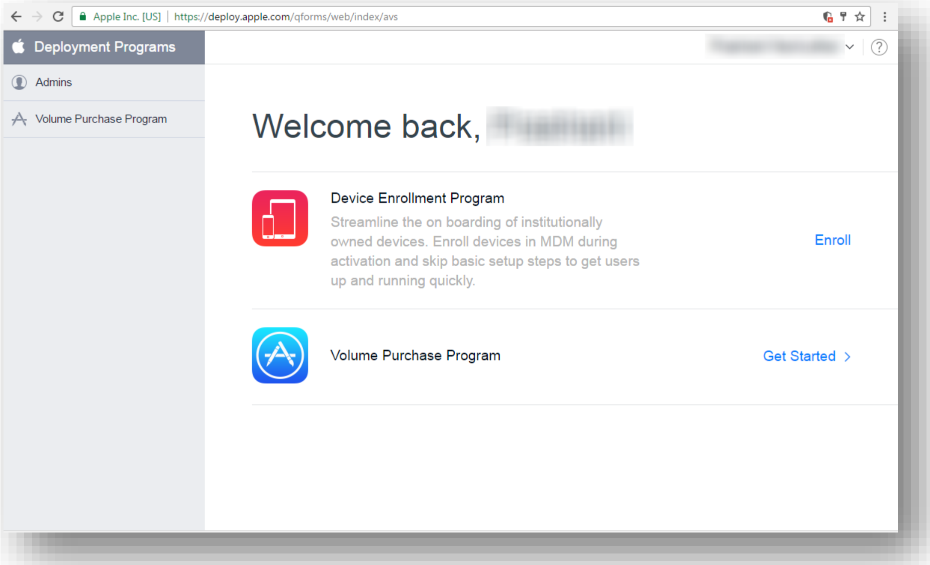
Forgot your Apple ID or Password?
Sign In

Copyright © 2016 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

Choose your country or region

7. Click on Volume Purchase programme.

8. Sign in with Apple ID Click on Sign in.

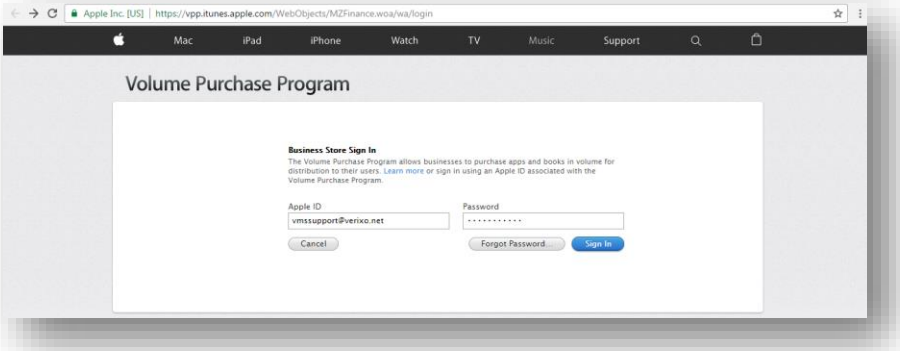


Welcome back, [redacted]

Device Enrollment Program

Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.

Volume Purchase Program


Apple Inc. [US] | https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/login
Mac
iPad
iPhone
Watch
TV
Music
Support
Cancel
Forgot Password...
Sign In

Volume Purchase Program

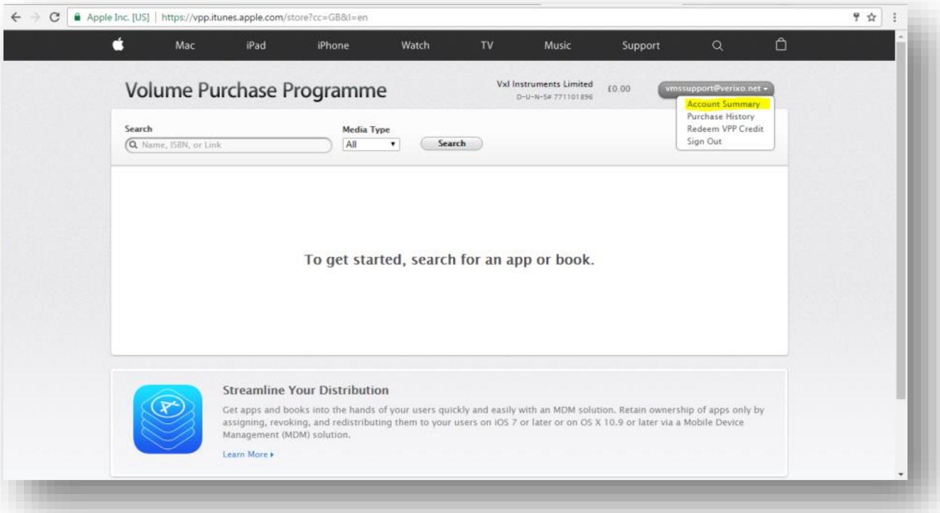
Business Store Sign In

The Volume Purchase Program allows businesses to purchase apps and books in volume for distribution to their users. Learn more or sign in using an Apple ID associated with the Volume Purchase Program.

Apple ID: vmssupport@verixo.net

Password: ···········

9. Click on login id username -> Select Account Summary.



Volume Purchase Programme

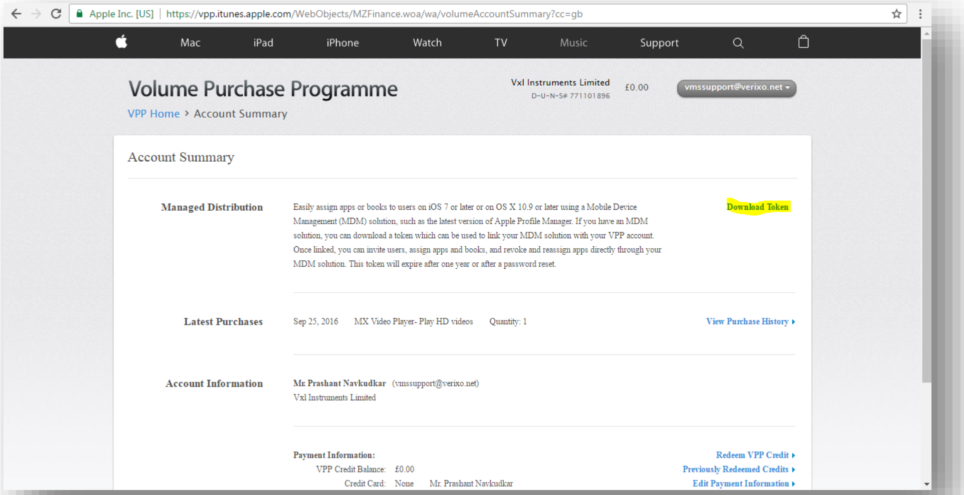
Vxl Instruments Limited
D-U-N-S# 771101896
£0.00

To get started, search for an app or book.

Streamline Your Distribution

Get apps and books into the hands of your users quickly and easily with an MDM solution. Retain ownership of apps only by assigning, revoking, and redistributing them to your users on iOS 7 or later or on OS X 10.9 or later via a Mobile Device Management (MDM) solution.

10. Click on Download Token
11. Go to VPP form on server -> browse download token.


Apple Inc. [US] | https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/volumeAccountSummary?cc=gb
Mac
iPad
iPhone
Watch
TV
Music
Support
vmssupport@verixo.net
VPP Home › Account Summary
Download Token
View Purchase History
Redeem VPP Credit
Previously Redeemed Credits
Edit Payment Information

Volume Purchase Programme

Vxl Instruments Limited
D-U-N-S# 771101896
£0.00

Account Summary

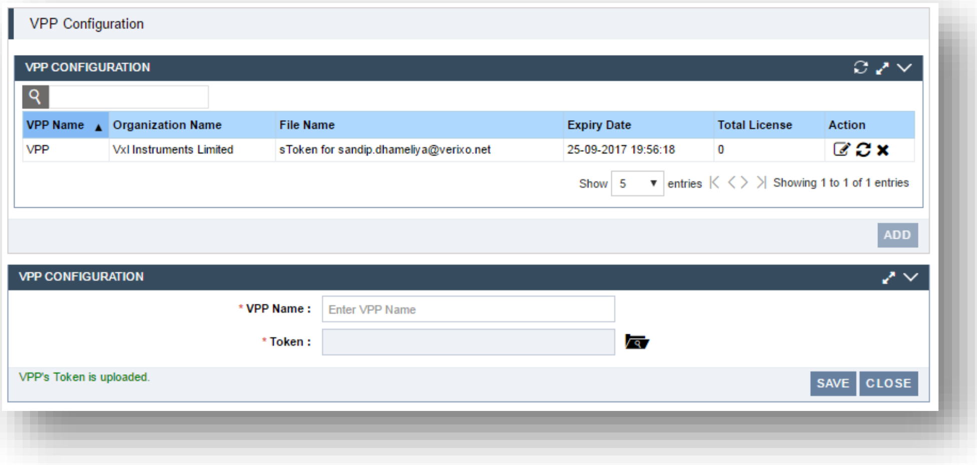
Managed Distribution Easily assign apps or books to users on iOS 7 or later or on OS X 10.9 or later using a Mobile Device Management (MDM) solution, such as the latest version of Apple Profile Manager. If you have an MDM solution, you can download a token which can be used to link your MDM solution with your VPP account. Once linked, you can invite users, assign apps and books, and revoke and reassign apps directly through your MDM solution. This token will expire after one year or after a password reset.

Latest Purchases Sep 25, 2016 MX Video Player- Play HD videos Quantity: 1

Account Information Mr. Prashant Navkudkar (vmssupport@verixo.net)
Vxl Instruments Limited

Payment Information:
VPP Credit Balance: £0.00
Credit Card: None Mr. Prashant Navkudkar

12. Click on Save, VPP name with details gets listed out with Edit , Sync, Delete functionality.
13. Click on Sync to get all app data from respective token.
14. After sync go to Application catalogue setup -> app gets listed out in app catalogue.



VPP Configuration

VPP CONFIGURATION

VPP Name ▲	Organization Name	File Name	Expiry Date	Total License	Action
VPP	Vxl Instruments Limited	sToken for sandip.dhameliya@verixo.net	25-09-2017 19:56:18	0	✎ ⟳ ✖

Show 5 entries Showing 1 to 1 of 1 entries

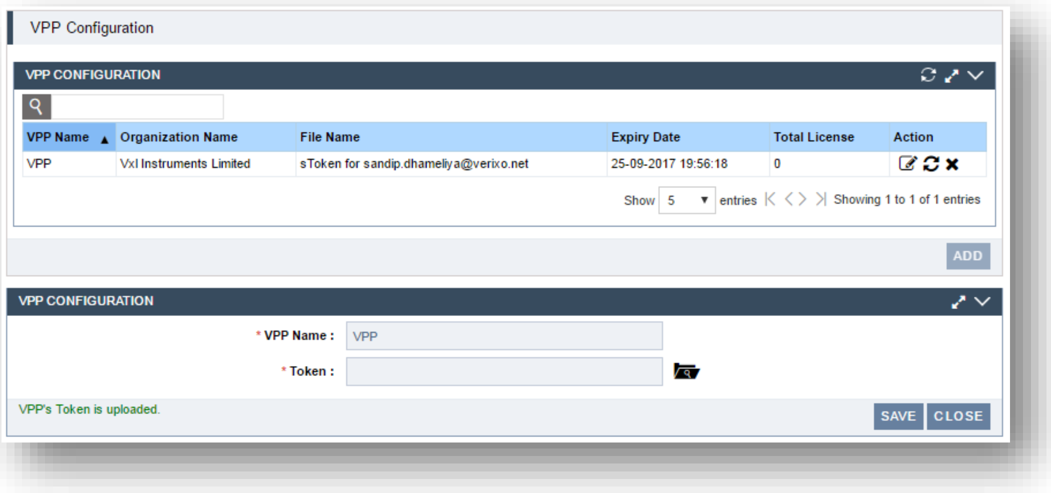
VPP CONFIGURATION

* VPP Name : Enter VPP Name

* Token :

VPP's Token is uploaded.

15. Click on Edit to update VPP app. ✎



VPP Configuration

VPP CONFIGURATION

VPP Name ▲	Organization Name	File Name	Expiry Date	Total License	Action
VPP	Vxl Instruments Limited	sToken for sandip.dhameliya@verixo.net	25-09-2017 19:56:18	0	✎ ⟳ ✖

Show 5 entries Showing 1 to 1 of 1 entries

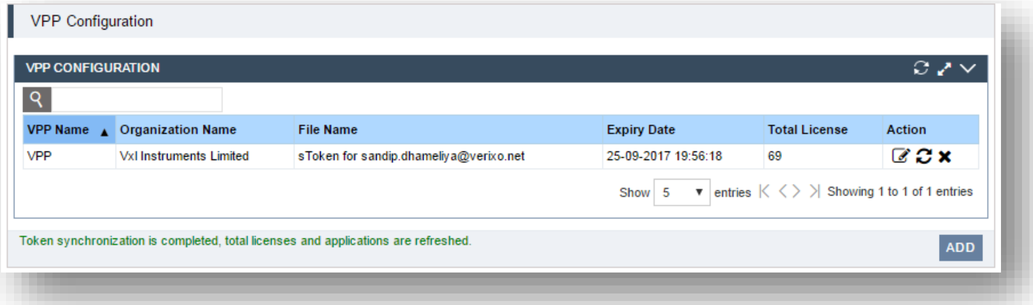
VPP CONFIGURATION

* VPP Name : VPP

* Token :

VPP's Token is uploaded.

16. Click on delete to delete selected App. ✖



VPP Configuration

VPP CONFIGURATION

VPP Name ▲	Organization Name	File Name	Expiry Date	Total License	Action
VPP	Vxl Instruments Limited	sToken for sandip.dhameliya@verixo.net	25-09-2017 19:56:18	69	

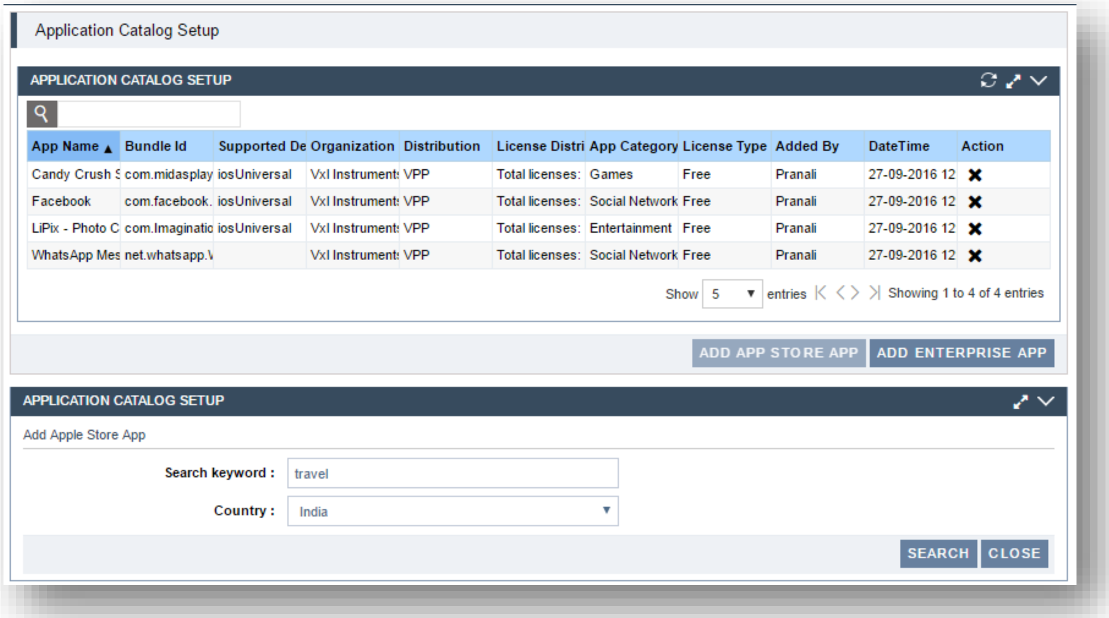
Token synchronization is completed, total licenses and applications are refreshed.

Application Catalogue Setup

Add App Store App

User able to View, Add Store App , Enterprise App from Application catalogue setup.

1. Go to Configuration setup-> click on Apple MDM configuration then click on Application catalogue setup.
2. Click on **Add Store App.**



Application Catalog Setup

APPLICATION CATALOG SETUP

App Name ▲	Bundle Id	Supported De	Organization	Distribution	License Distri	App Category	License Type	Added By	DateTime	Action
Candy Crush S	com.midasplay	iosUniversal	Vxl Instrument	VPP	Total licenses:	Games	Free	Pranali	27-09-2016 12	✖
Facebook	com.facebook.	iosUniversal	Vxl Instrument	VPP	Total licenses:	Social Network	Free	Pranali	27-09-2016 12	✖
LiPix - Photo C	com.Imaginatic	iosUniversal	Vxl Instrument	VPP	Total licenses:	Entertainment	Free	Pranali	27-09-2016 12	✖
WhatsApp Mes	net.whatsapp.\		Vxl Instrument	VPP	Total licenses:	Social Network	Free	Pranali	27-09-2016 12	✖

Show 5 entries Showing 1 to 4 of 4 entries

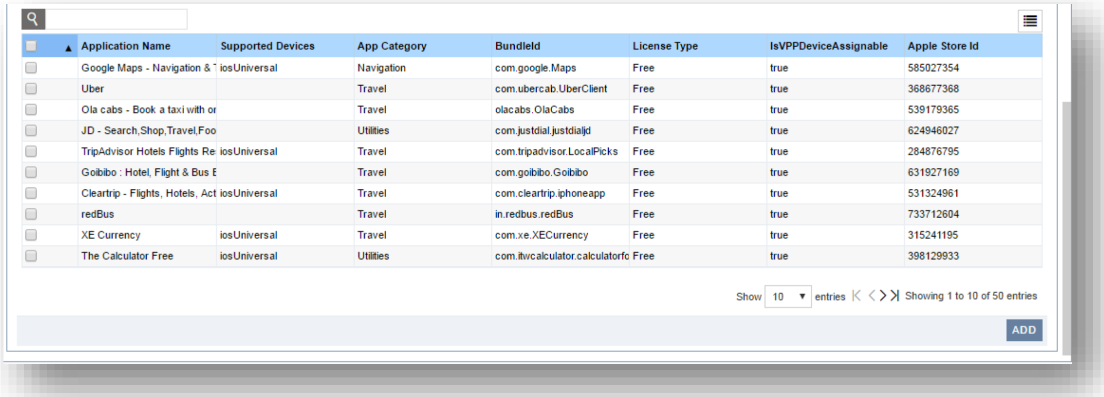
APPLICATION CATALOG SETUP

Add Apple Store App

Search keyword : travel

Country : India

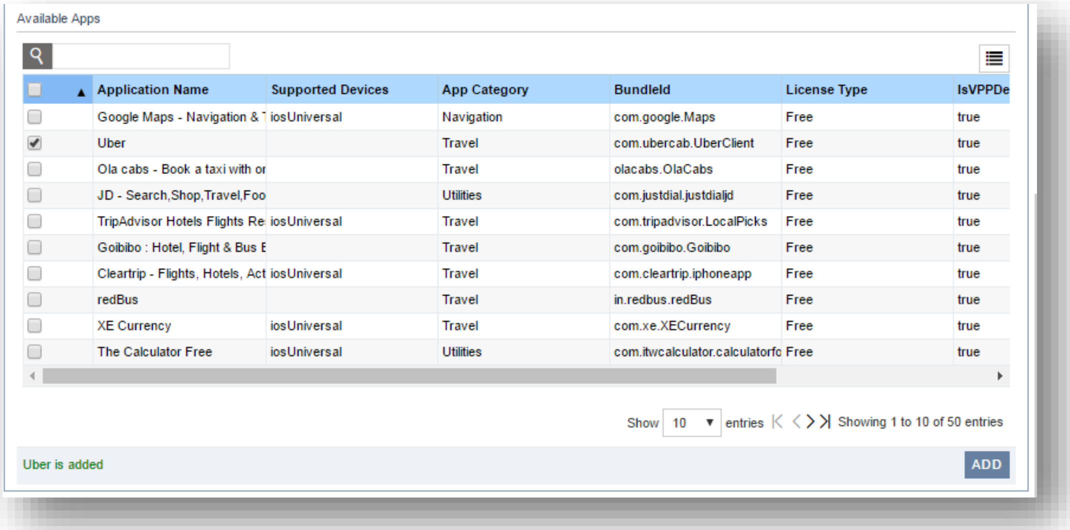
3. User able to search any keyword of application, also able to select country from dropdown list.
4. Click on Search.



□ ▲	Application Name	Supported Devices	App Category	BundleId	License Type	IsVPPDeviceAssignable	Apple Store Id
□	Google Maps - Navigation & T	iosUniversal	Navigation	com.google.Maps	Free	true	585027354
□	Uber		Travel	com.ubercab.UberClient	Free	true	368677368
□	Ola cabs - Book a taxi with or		Travel	olacabs.OlaCabs	Free	true	539179365
□	JD - Search,Shop,Travel,Foo		Utilities	com.justdial.justdialjd	Free	true	624946027
□	TripAdvisor Hotels Flights Re	iosUniversal	Travel	com.tripadvisor.LocalPicks	Free	true	284876795
□	Goibibo : Hotel, Flight & Bus E		Travel	com.goibibo.Goibibo	Free	true	631927169
□	Cleartrip - Flights, Hotels, Act	iosUniversal	Travel	com.cleartrip.iphoneapp	Free	true	531324961
□	redBus		Travel	in.redbus.redBus	Free	true	733712604
□	XE Currency	iosUniversal	Travel	com.xe.XECurrency	Free	true	315241195
□	The Calculator Free	iosUniversal	Utilities	com.itwcalculator.calculatorfo	Free	true	398129933

Show 10 entries Showing 1 to 10 of 50 entries

5. Application related to search keyword gets listed out.
6. Already VPP configured app also gets listed out in Application catalogue table.
7. Select any App from list, click on Add., Application is applied message displayed.
8. User able to delete by clicking ✖ .



Available Apps

□ ▲	Application Name	Supported Devices	App Category	BundleId	License Type	IsVPPDe
□	Google Maps - Navigation & T	iosUniversal	Navigation	com.google.Maps	Free	true
☑	Uber		Travel	com.ubercab.UberClient	Free	true
□	Ola cabs - Book a taxi with or		Travel	olacabs.OlaCabs	Free	true
□	JD - Search,Shop,Travel,Foo		Utilities	com.justdial.justdialjd	Free	true
□	TripAdvisor Hotels Flights Re	iosUniversal	Travel	com.tripadvisor.LocalPicks	Free	true
□	Goibibo : Hotel, Flight & Bus E		Travel	com.goibibo.Goibibo	Free	true
□	Cleartrip - Flights, Hotels, Act	iosUniversal	Travel	com.cleartrip.iphoneapp	Free	true
□	redBus		Travel	in.redbus.redBus	Free	true
□	XE Currency	iosUniversal	Travel	com.xe.XECurrency	Free	true
□	The Calculator Free	iosUniversal	Utilities	com.itwcalculator.calculatorfo	Free	true

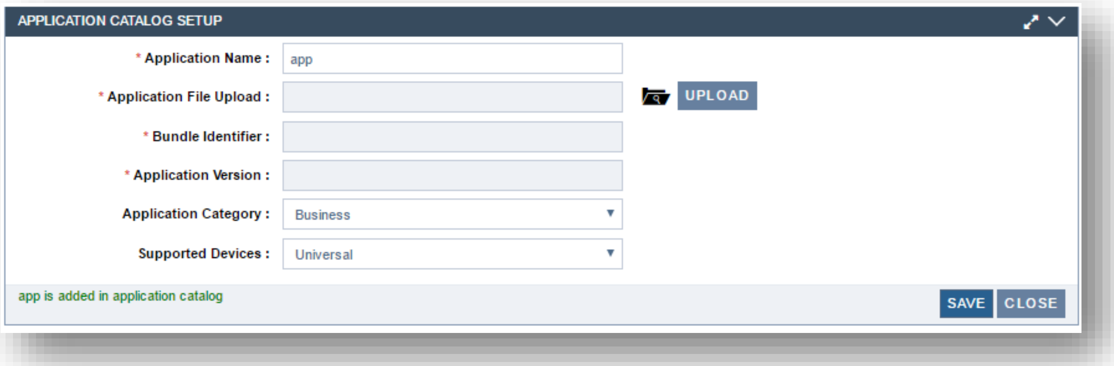
Show 10 ▾ entries Showing 1 to 10 of 50 entries

Uber is added

Add Enterprise App

User able to add enterprise application by uploading valid .ipa file.

1. Go to Configuration setup-> click on Apple MDM configuration then click on Application catalogue setup.
2. Click on **Add Enterprise App.**
3. Enter all mandatory fields.
4. Browse .ipa app & click on Upload.
5. If .ipa file is valid then it will displayed Bundle identifier, Application version.
6. Select Application Category & Supported devices.
7. Click on Save
8. App is added in application catalog message displayed.
9. App gets listed out on data table.



APPLICATION CATALOG SETUP

* Application Name : app

* Application File Upload :

* Bundle Identifier :

* Application Version :

Application Category : Business

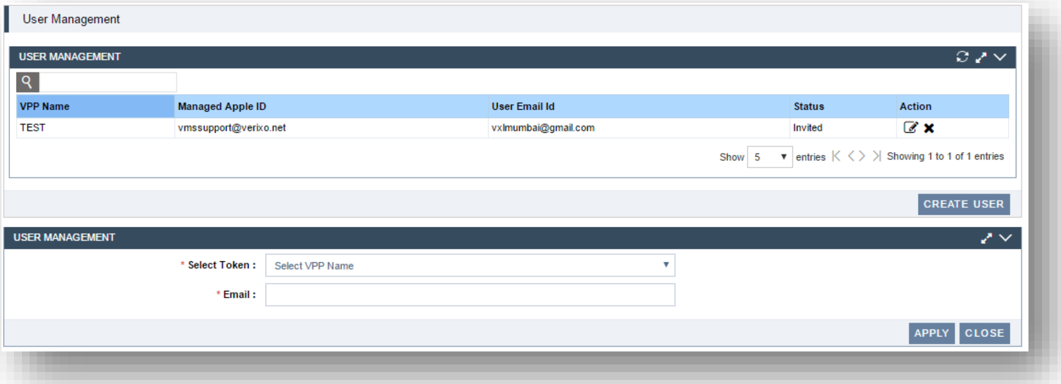
Supported Devices : Universal

app is added in application catalog

VPP USER Management

VPP user management able to managed Apple ID to get account from respective User email id’s.

1. Go to Configuration Setup > Apple MDM Configuration.
2. Select VPP user Management.
3. Click on Create User.



User Management

USER MANAGEMENT

VPP Name	Managed Apple ID	User Email Id	Status	Action
TEST	vmssupport@verixo.net	vxlmumbai@gmail.com	Invited	

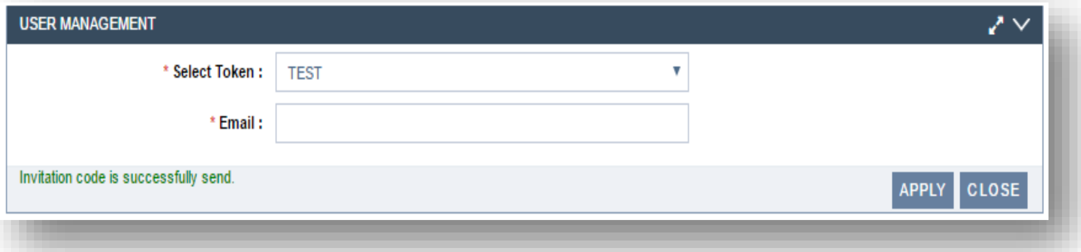
Show 5 entries Showing 1 to 1 of 1 entries

USER MANAGEMENT

* Select Token : Select VPP Name

* Email :

4. Select Token from dropdown list on which user wants to create VPP user.
5. List of Token comes after adding token in VPP configuration.



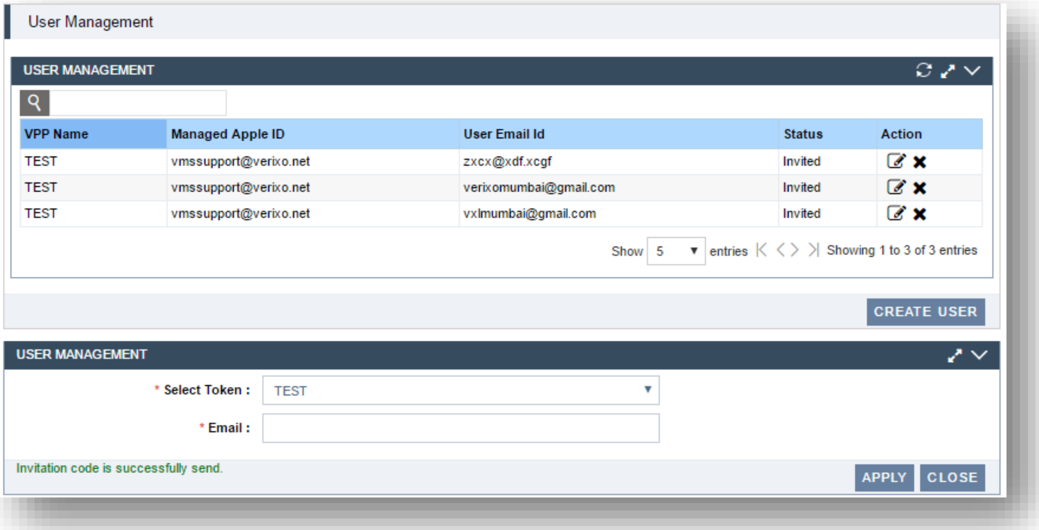
USER MANAGEMENT

* Select Token : TEST

* Email :

Invitation code is successfully send.

6. Enter valid Email id to receive invite user url link.



User Management

USER MANAGEMENT

VPP Name	Managed Apple ID	User Email Id	Status	Action
TEST	vmssupport@verixo.net	zxcx@xdf.xcgf	Invited	
TEST	vmssupport@verixo.net	verixomumbai@gmail.com	Invited	
TEST	vmssupport@verixo.net	vxlmumbai@gmail.com	Invited	

Show 5 entries Showing 1 to 3 of 3 entries

USER MANAGEMENT

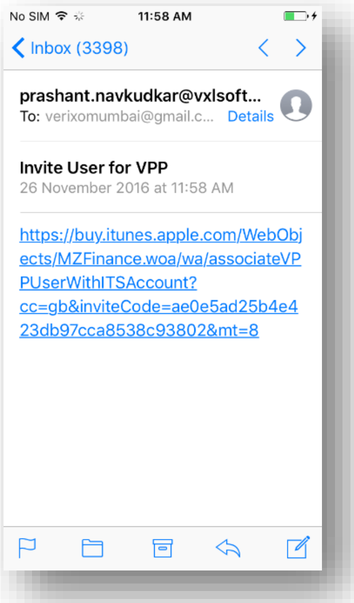
* Select Token : TEST

* Email :

Invitation code is successfully send.

7. Click on Apply

8. User will get url on entered Email id on device.



prashant.navkudkar@vxlsoft...

To: verixomumbai@gmail.c... Details

Invite User for VPP

26 November 2016 at 11:58 AM

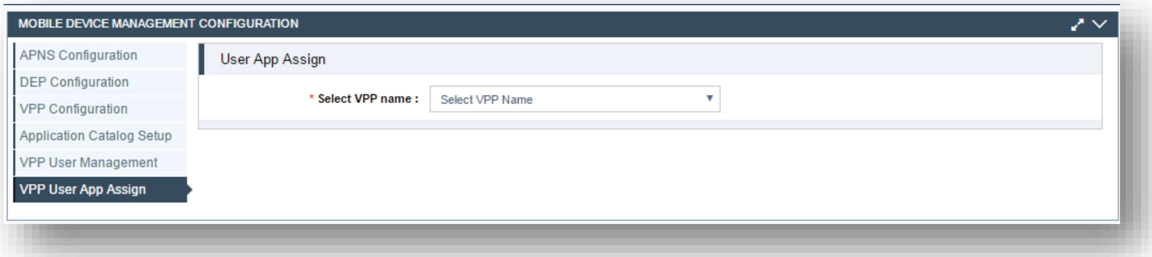
https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/associateVPPUserWithITSAccount?cc=gb&inviteCode=ae0e5ad25b4e423db97cca8538c93802&mt=8

9. Click on invited url & follow process accordingly.
10. After Token sync from VPP configuration, User management status will get updated from invited to Associated.
11. After creation of user " Organisation can now Assign App to created user".
12. User also able Edit or Delete User management data by click on Action 📝 ✖ button respectively.

VPP User App Assign

VPP user App design helps organisation to assign app to created VPP user.

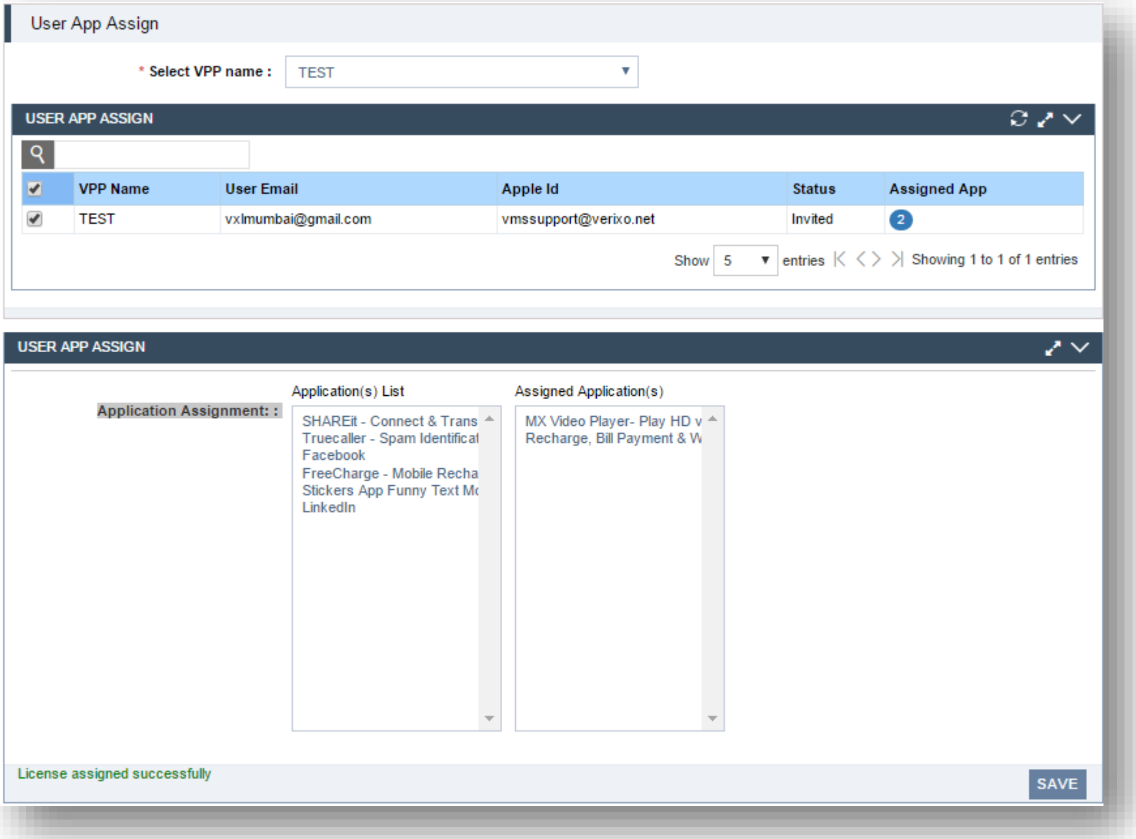
1. Go to Configuration Setup> Apple MDM configuration.
2. Select VPP User APP Assign



User App Assign

* Select VPP name : Select VPP Name

3. Select VPP name from dropdown list, User App Design form will get open.
4. In data table list of VPP Users , VPP name & assigned app count will be displayed



User App Assign

* Select VPP name : TEST

USER APP ASSIGN

☑	VPP Name	User Email	Apple Id	Status	Assigned App
☑	TEST	vxlmumbai@gmail.com	vmssupport@verixo.net	Invited	2

Show 5 entries Showing 1 to 1 of 1 entries

USER APP ASSIGN

Application Assignment: :

Application(s) List
SHAREit - Connect & Trans
Truecaller - Spam Identificat
Facebook
FreeCharge - Mobile Recha
Stickers App Funny Text Mc
LinkedIn

Assigned Application(s)
MX Video Player- Play HD v
Recharge, Bill Payment & W

License assigned successfully

5. In Application assignment user able to assign app to selected VPP name.

6. Click on Save “License assigned successfully.”
7. To disassociate app, click on assigned app count click on assigned app which user want to disassociate & click on save.
8. After assign particular app, count will get decrease in application catalogue setup License distribution column.

Working with the Device Manager for Android

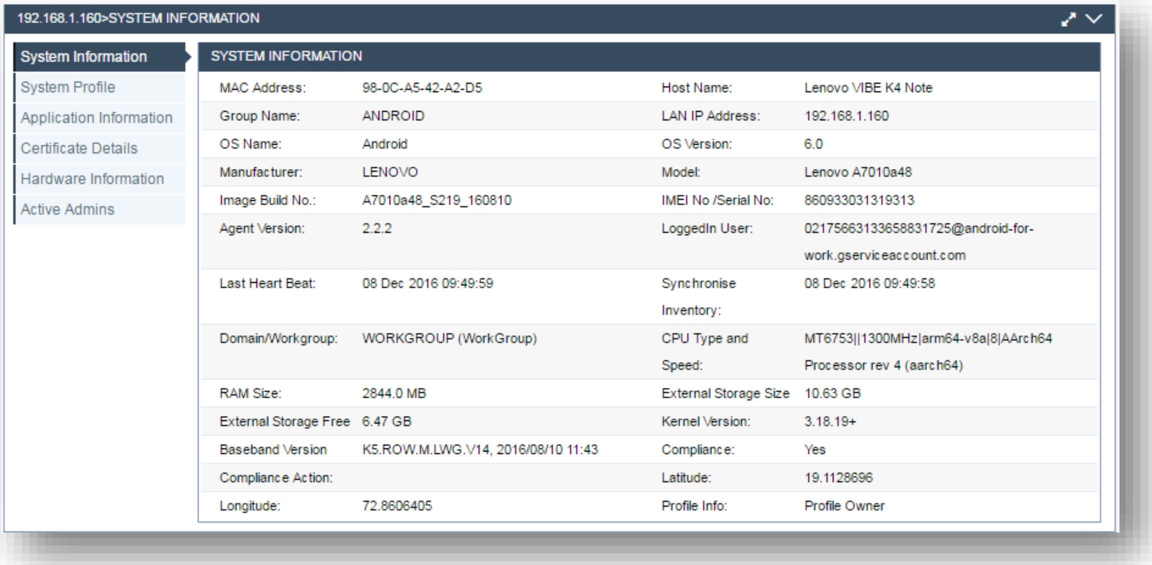
Viewing System Information

System Information provides an overview of system-related information for a network-connected device.

The information displayed is specific to the operating device. For example, the information displayed for an Android based device will be different from the information displayed for a iOS based device.

To view system information

1. In the devices tree, click the required device.
2. The **System Information** pane is display.



192.168.1.160>SYSTEM INFORMATION

SYSTEM INFORMATION

MAC Address:	98-0C-A5-42-A2-D5	Host Name:	Lenovo VIBE K4 Note
Group Name:	ANDROID	LAN IP Address:	192.168.1.160
OS Name:	Android	OS Version:	6.0
Manufacturer:	LENOVO	Model:	Lenovo A7010a48
Image Build No.:	A7010a48_S219_160810	IMEI No /Serial No:	860933031319313
Agent Version:	2.2.2	LoggedIn User:	02175663133658831725@android-for-work.gserviceaccount.com
Last Heart Beat:	08 Dec 2016 09:49:59	Synchronise Inventory:	08 Dec 2016 09:49:58
Domain/Workgroup:	WORKGROUP (WorkGroup)	CPU Type and Speed:	MT6753||1300MHz|arm64-v8a|8|AArch64 Processor rev 4 (aarch64)
RAM Size:	2844.0 MB	External Storage Size	10.63 GB
External Storage Free	6.47 GB	Kernel Version:	3.18.19+
Baseband Version	K5.ROW.M.LWG.V14, 2016/08/10 11:43	Compliance:	Yes
Compliance Action:		Latitude:	19.1128696
Longitude:	72.8606405	Profile Info:	Profile Owner

Viewing General Information

Under **System Information**, you can also view the following general information:

- System Profile
- Application Information
- Certificate Details
- Hardware Information
- Active Admins

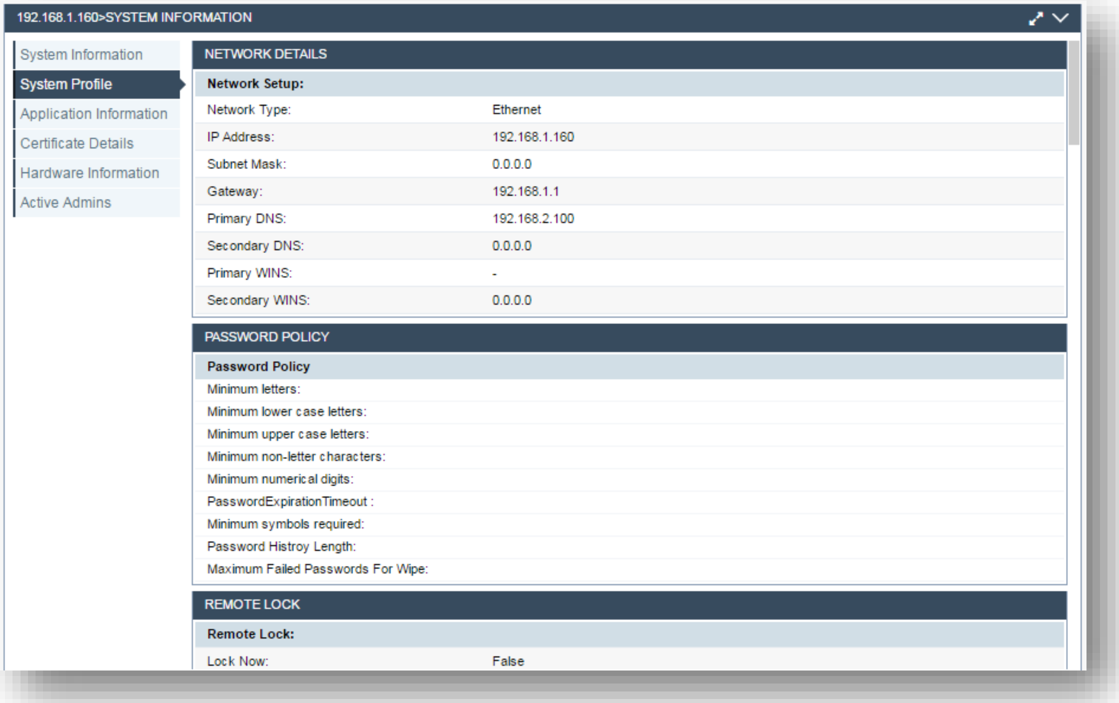
Viewing System Profile

The following details are displayed under **System Profile**:

- Network Details
- Password Policy
- Remote Lock
- Wipe Data
- Peripheral Settings
- Data Security Policy
- User Restriction Policy
- Camera & Screen Capture
- Keyguard Features
- Agent Settings
- Set Input Methods
- Accessibility
- Install from Unknown Sources
- Runtime Permission
- Application Permission
- Application Restriction
- Profile Policy
- Cross-profile Widget Providers
- Cross-profile Intents

To view the system profile

1. In the devices tree, click the required device.
2. Under **System Information**, click **System Profile**.



NETWORK DETAILS

Network Setup:	
Network Type:	Ethernet
IP Address:	192.168.1.160
Subnet Mask:	0.0.0.0
Gateway:	192.168.1.1
Primary DNS:	192.168.2.100
Secondary DNS:	0.0.0.0
Primary WINS:	-
Secondary WINS:	0.0.0.0

PASSWORD POLICY

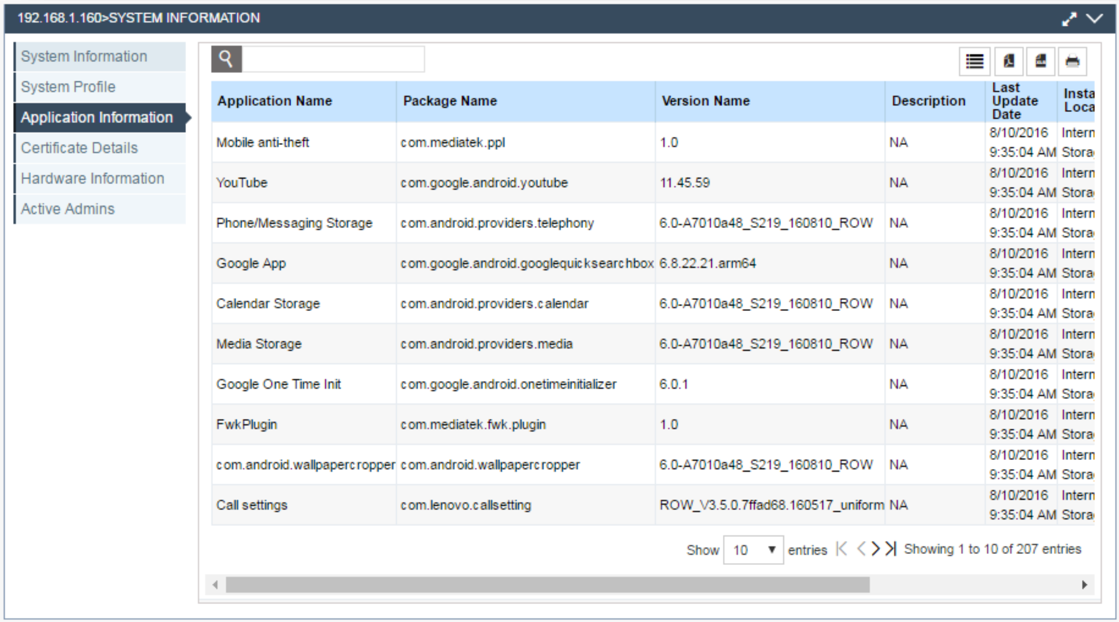
Password Policy	
Minimum letters:	
Minimum lower case letters:	
Minimum upper case letters:	
Minimum non-letter characters:	
Minimum numerical digits:	
PasswordExpirationTimeout :	
Minimum symbols required:	
Password Histroy Length:	
Maximum Failed Passwords For Wipe:	

REMOTE LOCK

Remote Lock:	
Lock Now:	False

Viewing Application Information

All detailed information about each of the applications installed in the selected device are listed out. The information includes the following: Software Name, Package Name, Version Name, Description, Last Update Date, Install Location, Install Size, Data Size, Total Size, App Type.

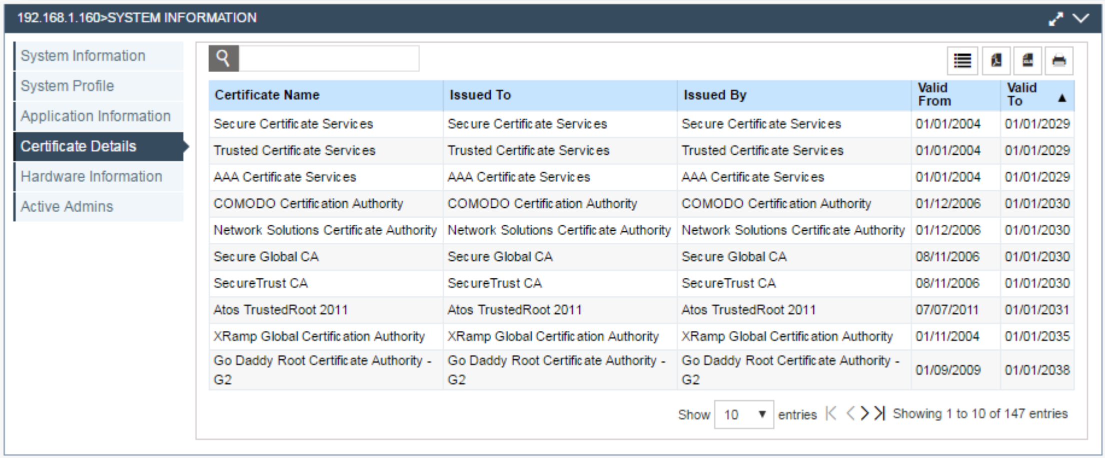


Application Name	Package Name	Version Name	Description	Last Update Date	Insta Loca
Mobile anti-theft	com.mediatek.ppl	1.0	NA	8/10/2016 9:35:04 AM	Intern Stora
YouTube	com.google.android.youtube	11.45.59	NA	8/10/2016 9:35:04 AM	Intern Stora
Phone/Messaging Storage	com.android.providers.telephony	6.0-A7010a48_S219_160810_ROW	NA	8/10/2016 9:35:04 AM	Intern Stora
Google App	com.google.android.googlequicksearchbox	6.8.22.21.arm64	NA	8/10/2016 9:35:04 AM	Intern Stora
Calendar Storage	com.android.providers.calendar	6.0-A7010a48_S219_160810_ROW	NA	8/10/2016 9:35:04 AM	Intern Stora
Media Storage	com.android.providers.media	6.0-A7010a48_S219_160810_ROW	NA	8/10/2016 9:35:04 AM	Intern Stora
Google One Time Init	com.google.android.onetimeinitializer	6.0.1	NA	8/10/2016 9:35:04 AM	Intern Stora
FwkPlugin	com.mediatek.fwk.plugin	1.0	NA	8/10/2016 9:35:04 AM	Intern Stora
com.android.wallpapercropper	com.android.wallpapercropper	6.0-A7010a48_S219_160810_ROW	NA	8/10/2016 9:35:04 AM	Intern Stora
Call settings	com.lenovo.callsetting	ROW_V3.5.0.7ffad68.160517_uniform	NA	8/10/2016 9:35:04 AM	Intern Stora

Show 10 entries Showing 1 to 10 of 207 entries

Viewing Certificate Details

All system and manually added certificates are listed out in certificate details where all information about all certificates present in device such as Certificate name, issued to, Issue by, Valid from date and Valid to date is display.



Certificate Name	Issued To	Issued By	Valid From	Valid To ▲
Secure Certificate Services	Secure Certificate Services	Secure Certificate Services	01/01/2004	01/01/2029
Trusted Certificate Services	Trusted Certificate Services	Trusted Certificate Services	01/01/2004	01/01/2029
AAA Certificate Services	AAA Certificate Services	AAA Certificate Services	01/01/2004	01/01/2029
COMODO Certification Authority	COMODO Certification Authority	COMODO Certification Authority	01/12/2006	01/01/2030
Network Solutions Certificate Authority	Network Solutions Certificate Authority	Network Solutions Certificate Authority	01/12/2006	01/01/2030
Secure Global CA	Secure Global CA	Secure Global CA	08/11/2006	01/01/2030
SecureTrust CA	SecureTrust CA	SecureTrust CA	08/11/2006	01/01/2030
Atos TrustedRoot 2011	Atos TrustedRoot 2011	Atos TrustedRoot 2011	07/07/2011	01/01/2031
XRamp Global Certification Authority	XRamp Global Certification Authority	XRamp Global Certification Authority	01/11/2004	01/01/2035
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	01/09/2009	01/01/2038

Show 10 ▼ entries Showing 1 to 10 of 147 entries

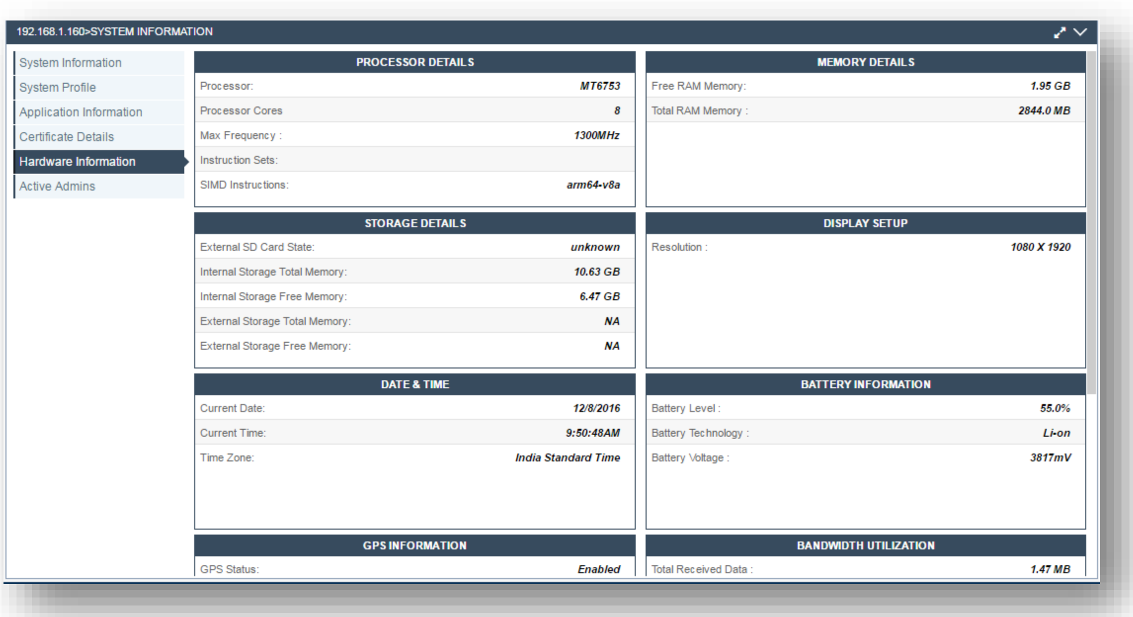
Viewing Hardware Information

The following information is display under **Hardware Information**:

- Processor details
- Memory details
- Storage details
- Display setup
- Date and time
- Battery information
- GPS information
- Bandwidth utilization
- Telephony details
- Network setup

To view hardware information

1. In the devices tree, click the required device.
2. Under **System Information**, click **Hardware Information**.



PROCESSOR DETAILS

Processor:	MT6753
Processor Cores	8
Max Frequency :	1300MHz
Instruction Sets:	
SIMD Instructions:	arm64-v8a

MEMORY DETAILS

Free RAM Memory:	1.95 GB
Total RAM Memory :	2844.0 MB

STORAGE DETAILS

External SD Card State:	unknown
Internal Storage Total Memory:	10.63 GB
Internal Storage Free Memory:	6.47 GB
External Storage Total Memory:	NA
External Storage Free Memory:	NA

DISPLAY SETUP

Resolution :	1080 X 1920

DATE & TIME

Current Date:	12/8/2016
Current Time:	9:50:48AM
Time Zone:	India Standard Time

BATTERY INFORMATION

Battery Level :	55.0%
Battery Technology :	Li-on
Battery Voltage :	3817mV

GPS INFORMATION

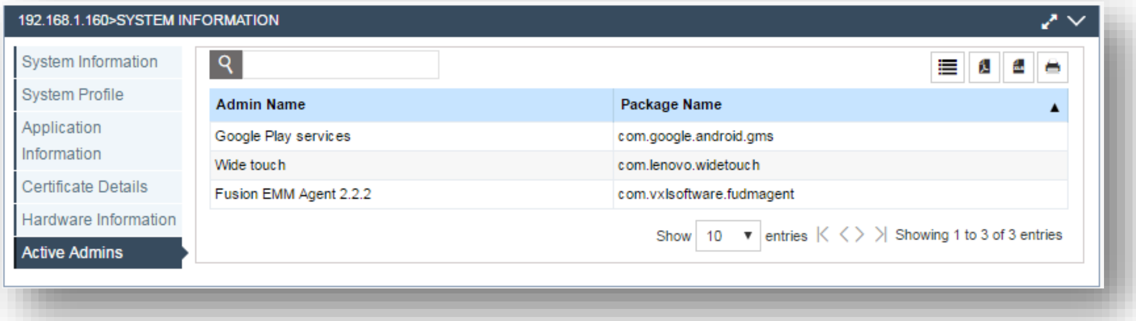
GPS Status:	Enabled

BANDWIDTH UTILIZATION

Total Received Data :	1.47 MB

Viewing Active Admins

1. All software with administrator rights will displayed here. On device, Security ->Device Administrator -> software listed out here are going to displayed on Agent Admin list.
2. Active Admins software user not able to delete from server or agent until and unless in Security-> Device administrator -> checkbox is unchecked.



Admin Name	Package Name
Google Play services	com.google.android.gms
Wide touch	com.lenovo.widetouch
Fusion EMM Agent 2.2.2	com.vxlsoftware.fudmagent

Show 10 entries Showing 1 to 3 of 3 entries

Configuring System Settings

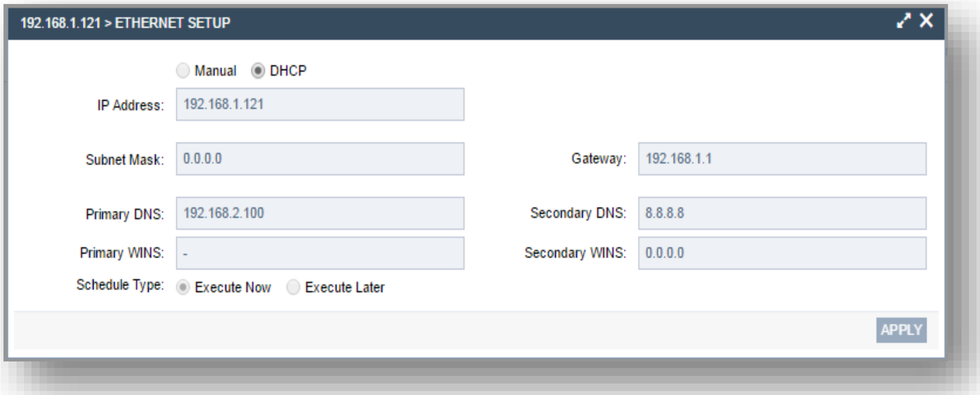
Configuring Ethernet Settings

You can configure Ethernet settings for a network-connected device in two ways; manually, or using the DHCP and obtaining a DNS server address automatically.

In the first method, all details, such as IP Address, Subnet Mask, Gateway, Primary and Secondary DNS Server Address must be provided. However, these details can be automatically configured in the network using a DHCP and a DNS server.

Using DHCP Mode:

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **System Settings**, then click **Network Settings**, and then click **Ethernet Setup**.



192.168.1.121 > ETHERNET SETUP

○ Manual ● DHCP

IP Address: 192.168.1.121

Subnet Mask: 0.0.0.0

Gateway: 192.168.1.1

Primary DNS: 192.168.2.100

Secondary DNS: 8.8.8.8

Primary WINS: -

Secondary WINS: 0.0.0.0

Schedule Type: ● Execute Now ○ Execute Later

4. The **DHCP** option get selected by default.
   The following information displayed:
   - IP Address
   - Subnet Mask
   - Gateway
   - Primary WINS
   - Secondary WINS
   - Primary DNS
   - Secondary DNS

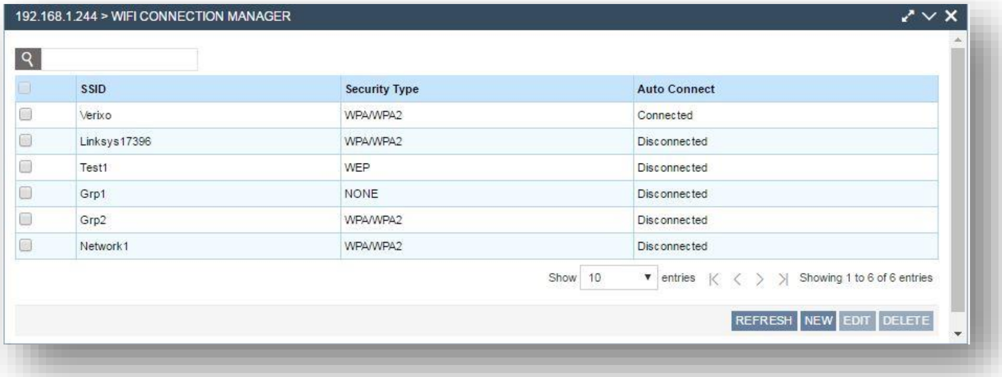
Configuring Wifi Connection Manager Settings

In Wifi Connection Manager, you can view the list of network connections present on a connected device. You can also add new connections, update the security for an existing connection, and delete an existing connection from the device.

Viewing the List of network connections

1. In the devices tree, click the required device.
2. Expand the right menu.

3. Click **System Settings**, then click **Network Settings**, and then click **Wifi Connection Manager**.
4. The list of network connections currently present in the device is display.
5. To view the updated list of network connections, click **Refresh** button.



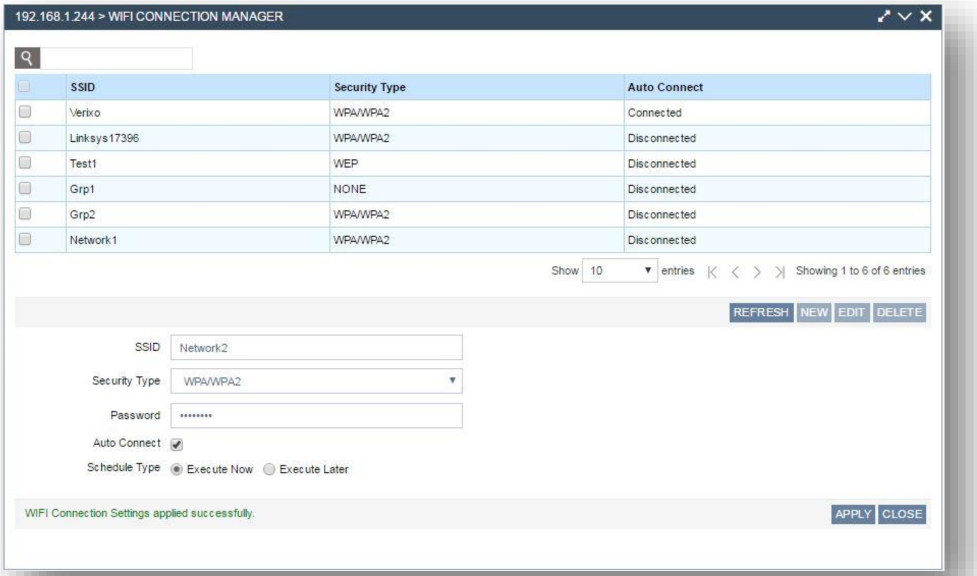
□	SSID	Security Type	Auto Connect
□	Verixo	WPA/WPA2	Connected
□	Linksys17396	WPA/WPA2	Disconnected
□	Test1	WEP	Disconnected
□	Grp1	NONE	Disconnected
□	Grp2	WPA/WPA2	Disconnected
□	Network1	WPA/WPA2	Disconnected

Show 10 entries Showing 1 to 6 of 6 entries

Adding a network connection

1. To create a new connection, click the **New** button.
2. In the **SSID** textbox, enter the network connection name.
3. Select the required **Security Type** for the network.
4. If security type selected is WEP or WPA/WPA2, then **Password** textbox is enabled.
5. In the **Password** textbox, enter the password for the network.
6. You can select the auto-connect checkbox if you want to automatically connect your device to the network.

7. Select the required **Schedule Type**.
8. Click **Apply**.
9. The **Wifi Connection Settings applied successfully** message is display.



□	SSID	Security Type	Auto Connect
□	Verixo	WPA/WPA2	Connected
□	Linksys17396	WPA/WPA2	Disconnected
□	Test1	WEP	Disconnected
□	Grp1	NONE	Disconnected
□	Grp2	WPA/WPA2	Disconnected
□	Network1	WPA/WPA2	Disconnected

Show 10 entries — Showing 1 to 6 of 6 entries

SSID: Network2

Security Type: WPA/WPA2

Password: ••••••••

Auto Connect: ☑

Schedule Type: ● Execute Now ○ Execute Later

WIFI Connection Settings applied successfully.

Editing a network connection

You can edit a connection which was previously made from the server.

1. To edit a connection, select the check box against the required connection.
   The **Edit** and **Delete** buttons are enabled. Click **Edit.**
2. The **SSID** textbox will be disabled.
3. Select the required **Security Type** for the network.

If the connection is from scanned list, then the password type dropdown will be disabled.

4. If security type selected is WEP or WPA/WPA2, then **Password** textbox is enabled.
5. In the **Password** textbox, enter the password for the network.
6. You can select the **auto-connect** checkbox if you want to automatically connect to the network.

7. Select the required **Schedule Type**.
8. Click **Apply**.
9. The **Wifi Connection Settings applied successfully** message is display.

Deleting a network connection

You can only delete a connection which was previously made from the server or manually added on the device.

1. To delete a connection, select the connection name and click the **Delete** button.
2. A prompt to delete the connection is display. Click **OK**.
3. Select the required **Schedule Type**.
4. Click **Apply**.
5. The **Wifi Connection Settings applied successfully** message is display.

Working with Security Settings

You can change security settings for a group of devices or a single device.

Configuring Password Policy Settings

You can configure the password policy for a remotely connected device.

The following password type can be set from the server:

- **Numeric**: PIN/ Password

  The user must have entered a password containing at least numeric characters.
- **Alphabetic**: Password

  The user must have entered a password containing at least alphabetic characters.
- **Alphanumeric**: Password

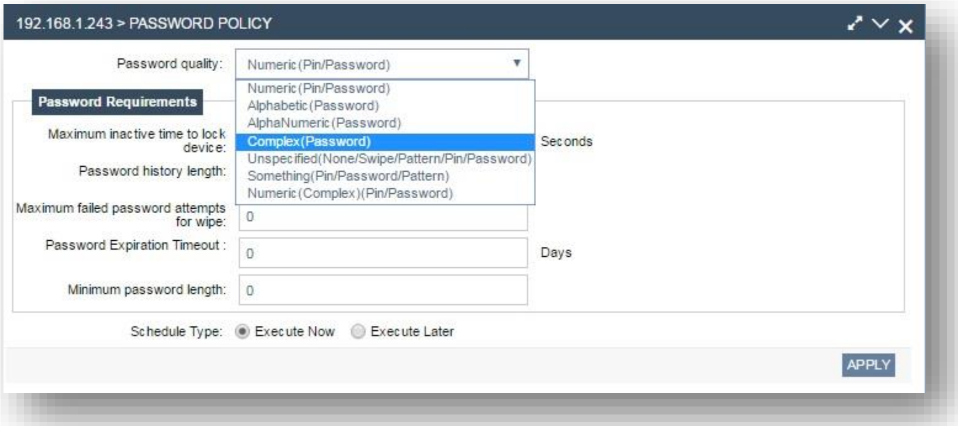
  The user must have entered a password containing at least both numeric and alphabetic characters.
- **Complex**: Password

  The user must have entered a password containing at least a letter, a numerical digit and a special symbol.
- **Unspecified**: None/Swipe/Pin/Pattern/Password

  The policy has no requirements for the password.
- **Something:** Pin/Password/Pattern

  The policy requires some kind of password or pattern, but doesn't care what it is.
- **Numeric (Complex)**: Pin/Password

The user must enter a password containing at least numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.



192.168.1.243 > PASSWORD POLICY

Password quality: Numeric (Pin/Password)

- Numeric (Pin/Password)
- Alphabetic (Password)
- AlphaNumeric (Password)
- Complex(Password)
- Unspecified(None/Swipe/Pattern/Pin/Password)
- Something(Pin/Password/Pattern)
- Numeric (Complex)(Pin/Password)

Password Requirements

Maximum inactive time to lock device: Seconds

Password history length:

Maximum failed password attempts for wipe: 0

Password Expiration Timeout : 0 Days

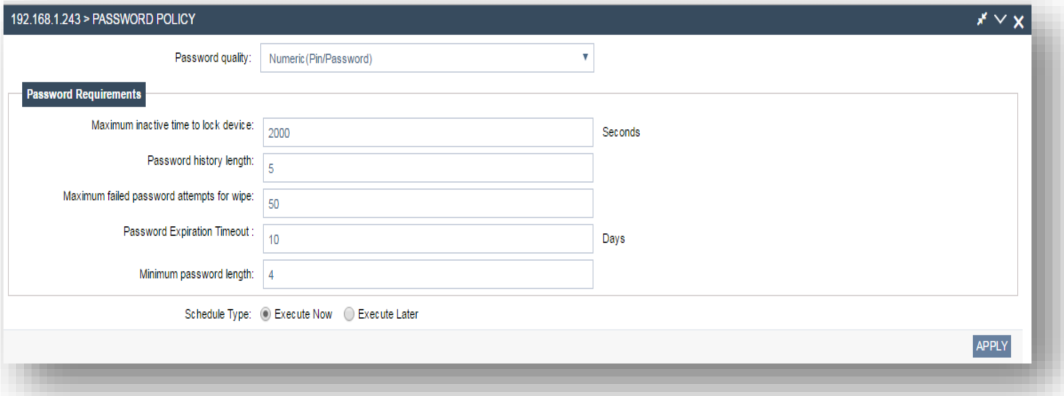
Minimum password length: 0

Schedule Type: ● Execute Now ○ Execute Later

APPLY

To configure Password settings

1. In the devices tree, click the required device.
2. Expand the right menu. Click **Security Settings**, and then click **Password Policy**.
3. Select the required **Password quality**.



192.168.1.243 > PASSWORD POLICY

Password quality: Numeric (Pin/Password)

Password Requirements

Maximum inactive time to lock device: 2000 Seconds

Password history length: 5

Maximum failed password attempts for wipe: 50

Password Expiration Timeout : 10 Days

Minimum password length: 4

Schedule Type: ● Execute Now ○ Execute Later

APPLY

4. The following fields are displayed for each password type:

- Maximum inactive time to lock device
- Password history length
- Maximum failed password attempts for wipe
- Password expiration timeout
- Minimum password length

For Alphabetic password type, following extra fields are displayed:

- Minimum lower case letters
- Minimum upper case letter

For Alphanumeric password type, following extra fields are displayed:

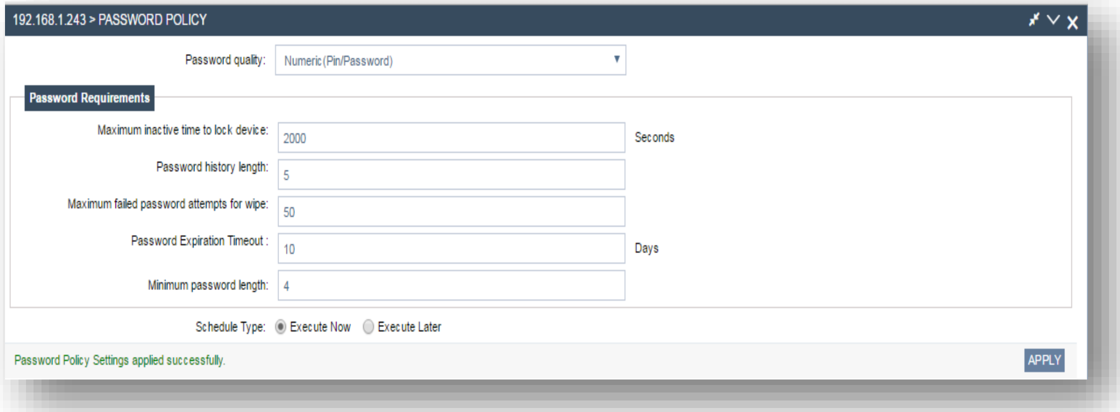
- Minimum letters
- Minimum lower case letters
- Minimum upper case letter
- Minimum non-letters characters
- Minimum numeric digits

For Complex, Unspecified, Something, Numeric (Complex) password type, following extra fields are displayed:

- Minimum letters
- Minimum lower case letters
- Minimum upper case letter
- Minimum non-letters characters
- Minimum numeric digits
- Minimum symbols required

5. In **Password Minimum Letter**, enter the minimum number of letters a password must contain.
6. In **Password Minimum Lower Case**, enter the minimum number of lower case letters a password must contain.
7. In **Password Minimum Upper Case**, enter the minimum number of upper case letters a password must contain.
8. In **Password Minimum Non Letter,** enter the minimum number of non-letters password must contain.
9. In **Password Minimum Numeric**, enter the minimum number of digits a password must contain.
10. In **Password Expiration Timeout,** enter the number of days to expire the user's password.
11. In **Password Minimum Symbols,** enter the minimum number of symbols a password must contain.
12. In **Password History Length,** enter the number of new passwords the user needs to use before using an old password.
13. In **Maximum Failed Password for Wipe** enter the maximum number of times an incorrect password can be entered before the device is locked or its data is wiped out.
14. Select the required **Schedule Type**.
15. Click **Apply**.

The **Password Policy Settings applied successfully** message is display.



Password quality: Numeric (Pin/Password)

Password Requirements

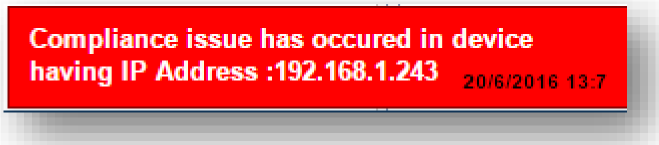
Maximum inactive time to lock device:	2000	Seconds
Password history length:	5	
Maximum failed password attempts for wipe:	50	
Password Expiration Timeout :	10	Days
Minimum password length:	4	

Schedule Type: ● Execute Now ○ Execute Later

Password Policy Settings applied successfully.

Compliance Status:

After applying Password Policy settings, a popup is display on Device Manager page as follows:



Compliance issue has occured in device having IP Address :192.168.1.243 20/6/2016 13:7

At this time, on device all the work profile applications (except Fusion EMM Agent) are hidden from list and work profile is disabled.

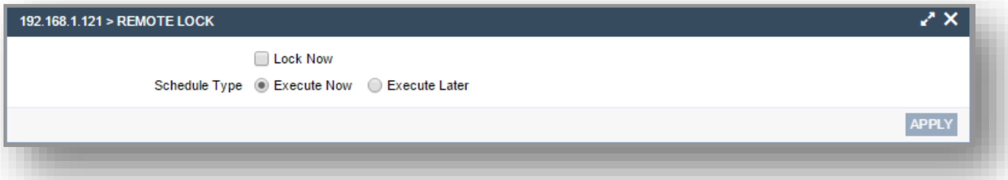
When user changes the password, the status of compliance is updated and work profile applications are enabled again.

Configuring Remote Lock Settings

You can remotely lock a device on the network.

To lock a device

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Remote Lock**.



192.168.1.121 > REMOTE LOCK

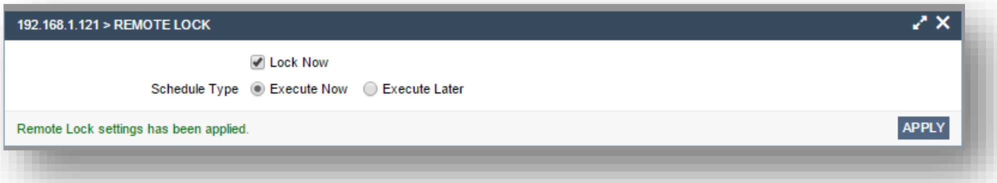
□ Lock Now

Schedule Type ● Execute Now ○ Execute Later

APPLY

4. To lock the device immediately, select the **Lock Now** check box.
5. Select the required **Schedule Type**.
6. Click **Apply**.

   The **Remote Lock settings applied successfully** message is display.



192.168.1.121 > REMOTE LOCK

☑ Lock Now

Schedule Type ● Execute Now ○ Execute Later

Remote Lock settings has been applied.

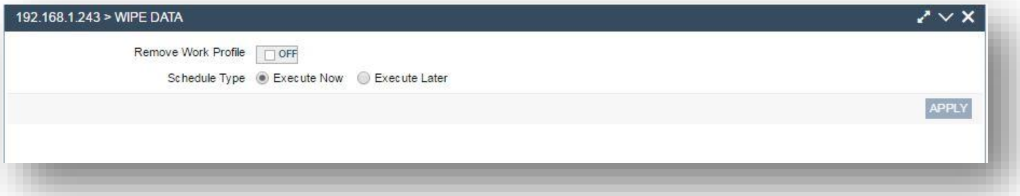
APPLY

Configuring Wipe Data Settings

You can configure the settings to remove a work profile from a device.

To remotely remove the work profile from a device

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Wipe Data**.



192.168.1.243 > WIPE DATA

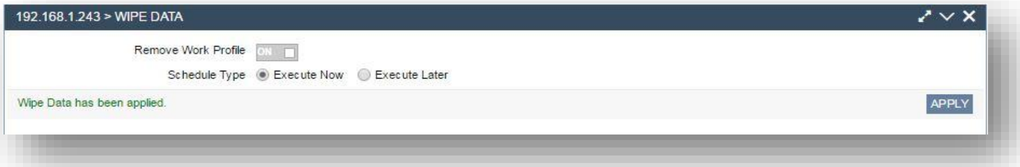
Remove Work Profile □ OFF

Schedule Type ● Execute Now ○ Execute Later

APPLY

4. To remove a work profile, set the **Remove Work Profile** button to ON.
5. Select the required **Schedule Type**.
6. Click **Apply**.

   The **Wipe Data has been applied** message is display.



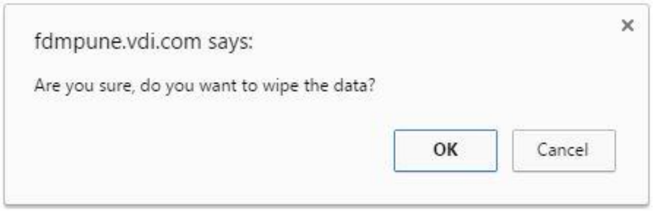
192.168.1.243 > WIPE DATA

Remove Work Profile ON

Schedule Type ● Execute Now ○ Execute Later

Wipe Data has been applied.

When we toggle the button to ON & Apply or Save the setting, server shows confirmation popup “Are you sure, do you want to wipe the data?”



fdmpune.vdi.com says:

Are you sure, do you want to wipe the data?

On the device, Go to Settings -> Accounts -> The previously created work profile should be deleted.

Configuring Peripheral Settings

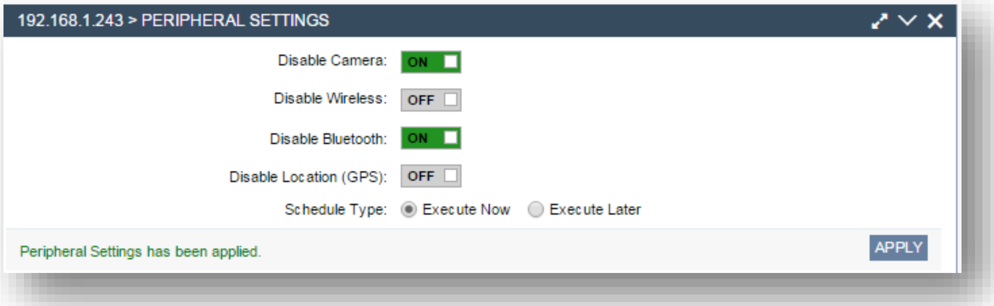
You can disable a Camera, Wi-Fi, Bluetooth, GPS attached to a remote device on the network.

To enable or disable a required option.

In the devices tree, click the required device.

1. Expand the right menu.
2. Click **Security Settings**, and then click **Peripheral Settings.**
3. Select the any peripheral setting to On/Off for Disable/Enable purpose respectively.
4. Select the required **Schedule Type**.
5. Click **Apply.**

   The **Peripheral Settings applied successfully** message is display.



192.168.1.243 > PERIPHERAL SETTINGS

Disable Camera: ON

Disable Wireless: OFF

Disable Bluetooth: ON

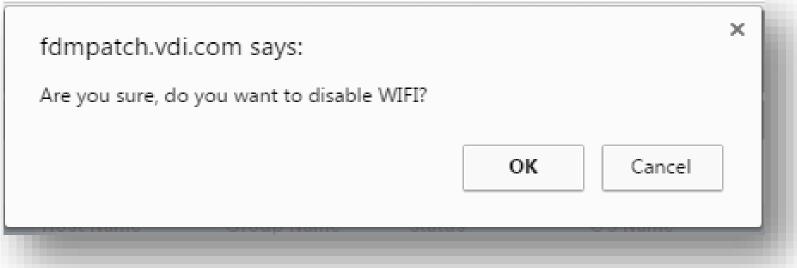
Disable Location (GPS): OFF

Schedule Type: ● Execute Now ○ Execute Later

Peripheral Settings has been applied.

When we disable Wi-Fi settings, server shows confirmation popup “Are you sure, do you want to disable Wi-Fi?”

If Ok is clicked, after task completion, the client will get off due no network connection.



fdmpatch.vdi.com says:

Are you sure, do you want to disable WIFI?

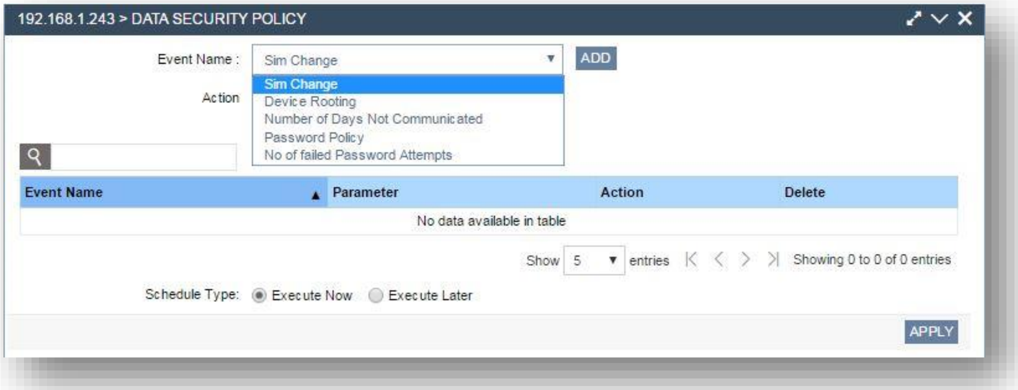
Configuring Data Security Policy Settings

You can configure data security policies to the connected Android device. On occurrence of any of the mentioned event, the selected security action will be applied on the device.

Events and Actions explained in short as follows:

- **Event Name:**
  - **Sim Change**: Change of SIM card on the device.
  - **Device Rooting**: Rooting of an Android device.
  - **Number of days not communicated:** Number of days not communicated with the server.

    - **Password Policy:** Changing the password type on the device.
    - **No of failed password attempts:** Number of failed password attempts on the device.



192.168.1.243 > DATA SECURITY POLICY

Event Name : Sim Change

Action

Sim Change
Device Rooting
Number of Days Not Communicated
Password Policy
No of failed Password Attempts
ADD

Event Name	Parameter	Action	Delete
No data available in table			

Show 5 entries Showing 0 to 0 of 0 entries

Schedule Type: ● Execute Now ○ Execute Later

- **Action:**
    - **Data Wipe:** Removing the work profile on the device.
    - **Disable Work Profile:** Removing the account registered with the work profile.

To set a data security policy on the device

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Data Security Policy**.
4. Select the required **Event** from the list.
5. Select the required **Action** from the list.
6. Click the **Add** button to add the selected choices into the table.
7. You can delete a policy from the table by clicking on **Delete** button next to the respective entry.
8. Select the required Schedule Type.
9. Click **Apply**.

The Data Security Policy Settings applied successfully message is display.

If all entries from the table will be deleted and settings are applied, then previously applied policies must be reset.

Configuring Security Policy Settings

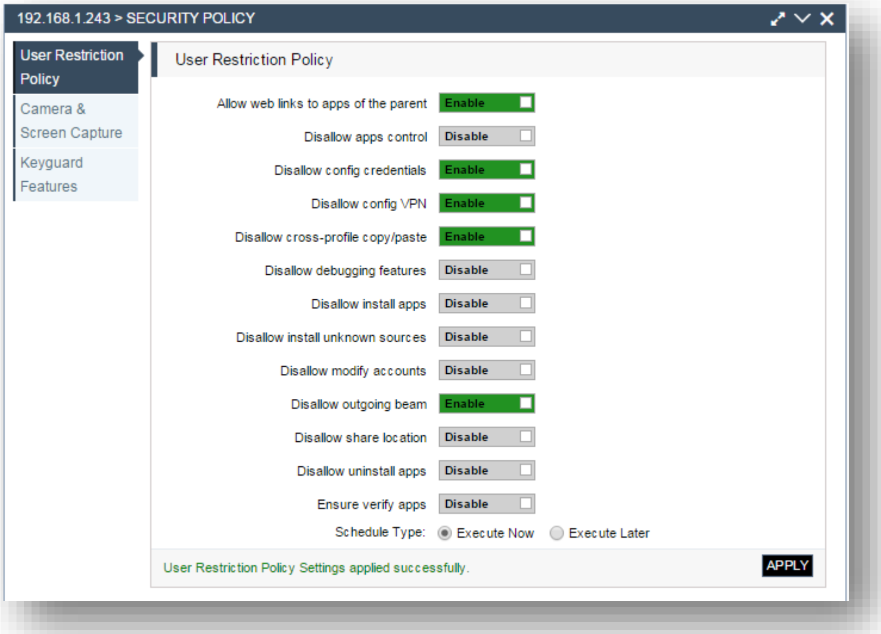
You can set various security policies to a remote device on the network.

Configuring User Restriction Policy

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Security Policy**.
4. Select the **User Restriction Policy** sub-menu.
5. Select the required policy setting to ON/OFF for Disable/Enable purpose.
6. Select the required Schedule Type.
7. Click **Apply**.

The User Restriction Policy Settings applied successfully message is display.

On the device, you can check if the applied settings are being reflected. For example, if you disallow share location from the server, then location sharing option for the work profile are gets disabled on the device.



Allow web links to apps of the parent: Enable ☑
Disallow apps control: Disable □
Disallow config credentials: Enable ☑
Disallow config VPN: Enable ☑
Disallow cross-profile copy/paste: Enable ☑
Disallow debugging features: Disable □
Disallow install apps: Disable □
Disallow install unknown sources: Disable □
Disallow modify accounts: Disable □
Disallow outgoing beam: Enable ☑
Disallow share location: Disable □
Disallow uninstall apps: Disable □
Ensure verify apps: Disable □
Schedule Type: ● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Camera & Screen Capture

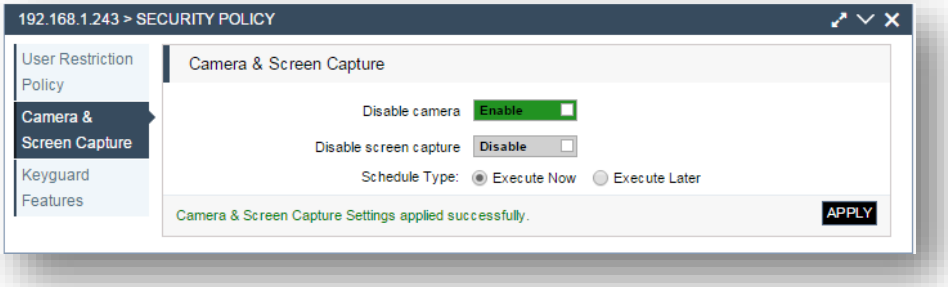
Disable camera will disable the camera in the work-profile of the device.

Disable screen-capture will disable the screenshot feature of the device when working in a work-profile app.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Security Policy**.
4. Select the **Camera & Screen Capture** sub-menu.
5. Select the required policy setting to ON/OFF for Disable/Enable purpose.

6. Select the required **Schedule Type**.
7. Click **Apply**.

The Camera & Screen Capture Settings applied successfully message is display.



Disable camera: Enable
Disable screen capture: Disable
Schedule Type: ● Execute Now ○ Execute Later

Camera & Screen Capture Settings applied successfully.

On devices running with Android version 5, disable camera feature will also disable the camera of device owner.

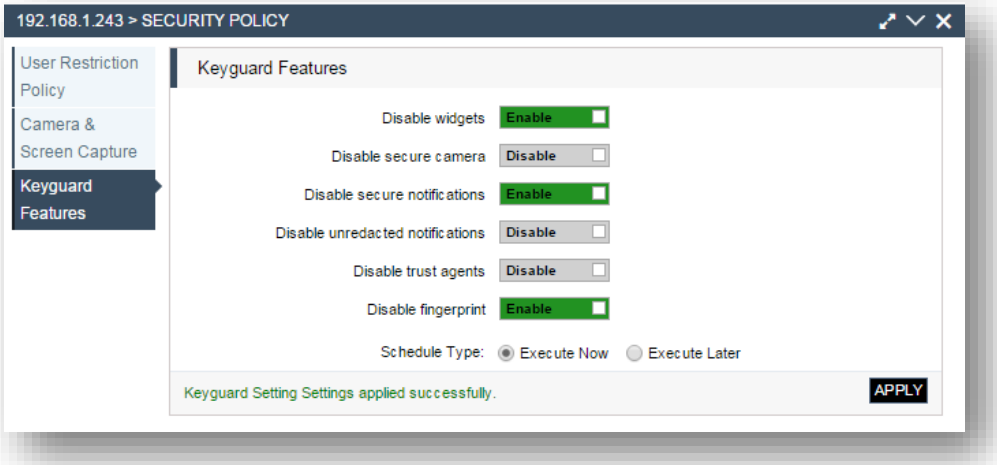
Configuring Keyguard Features

You can configure various key guard features on the connected Android device.

The settings will only be applied to the devices running on Android version 6 and above.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Security Settings**, and then click **Security Policy**.
4. Select the **Key Guard Features** sub-menu.
5. Select the required policy setting to ON/OFF for Disable/Enable purpose.
6. Select the required **Schedule Type**.
7. Click **Apply**.

The Key guard Features Settings applied successfully message is displayed.



Keyguard Features

Disable widgets: Enable ☑
Disable secure camera: Disable □
Disable secure notifications: Enable ☑
Disable unredacted notifications: Disable □
Disable trust agents: Disable □
Disable fingerprint: Enable ☑
Schedule Type: ● Execute Now ○ Execute Later

Keyguard Setting Settings applied successfully.

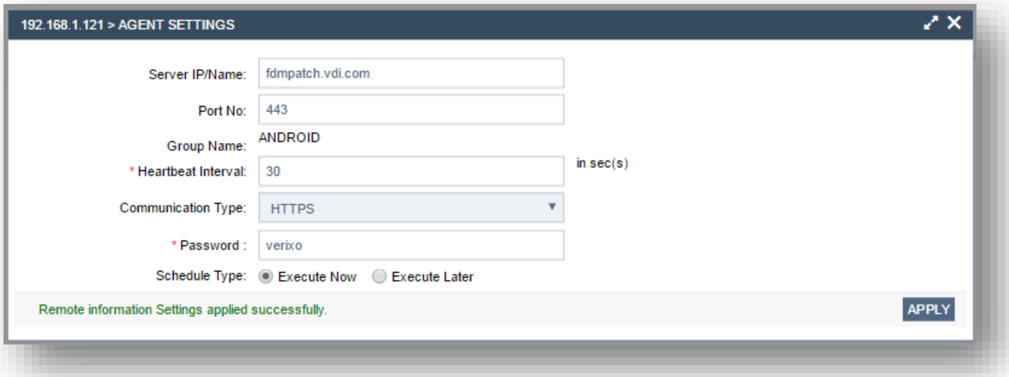
On the device, you can check if the applied settings are being reflected. For example, if you disable the fingerprint option from the server, then unlocking the device with fingerprint will be disabled on the device.

Working with Administration Settings

You can configure the settings to remotely administer an Android device.

Configuring Agent Settings

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Agent settings**.



Server IP/Name: fdmpatch.vdi.com
Port No: 443
Group Name: ANDROID
* Heartbeat Interval: 30 in sec(s)
Communication Type: HTTPS
* Password : verixo
Schedule Type: ● Execute Now ○ Execute Later

Remote information Settings applied successfully.

4. In **Server IP/Name**, enter any one of the following:
   - Server IP Address
   - Server Name

5. In **Port No**, enter the port number.
6. In **Heartbeat Interval**, enter the required value.
7. From the **Communication Type** list, select the required option.
8. In **Password**, enter the required password.
9. Select the required **Schedule Type**.
10. Click **Apply**.

    The **Remote Information Settings applied successfully** message is display.

Configuring Certificate Manager Settings

All certificates which user has added manually on the Android device will be displayed here. After the task gets successful, the certificates will be silently installed on the device.

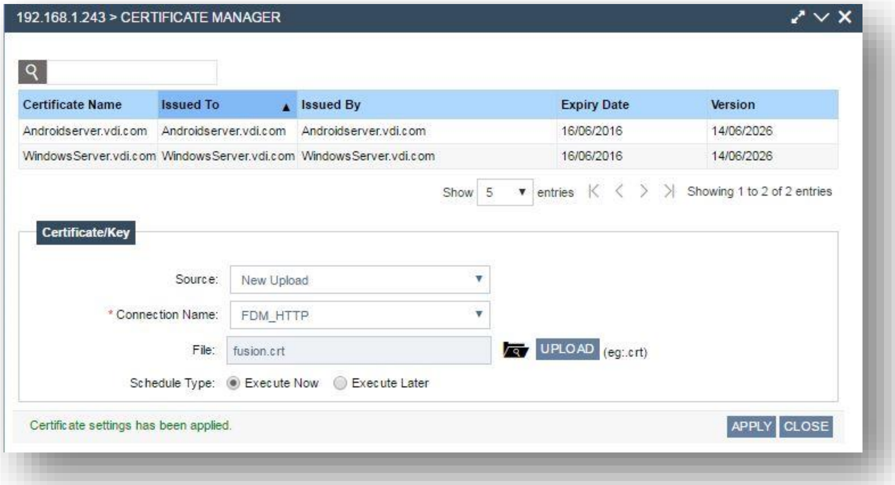
On Agent side to check installed certificate, go to Settings-> Security -> Trusted credentials-> Users -> Work.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Certificate Manager**.
4. To upload a new certificate, from **Source** dropdown select New Upload.
5. Select the required **Connection Name**.
6. Click the file browser icon to browse the file & click **Upload** button to upload the file.

Certificates of '.crt' extension file format are valid for the Android devices.

7. To use a previously uploaded certificate, select **Repository** from Source dropdown.
8. Select the required **Connection Name**.
9. Select the certificate **File**.
10. Select the required **Schedule Type**.
11. Click **Apply**.

    The **Certificate settings applied successfully** message is display.



192.168.1.243 > CERTIFICATE MANAGER

Certificate Name	Issued To	Issued By	Expiry Date	Version
Androidserver.vdi.com	Androidserver.vdi.com	Androidserver.vdi.com	16/06/2016	14/06/2026
WindowsServer.vdi.com	WindowsServer.vdi.com	WindowsServer.vdi.com	16/06/2016	14/06/2026

Show 5 entries Showing 1 to 2 of 2 entries

Certificate/Key

Source: New Upload

* Connection Name: FDM_HTTP

File: fusion.crt UPLOAD (eg:.crt)

Schedule Type: ● Execute Now ○ Execute Later

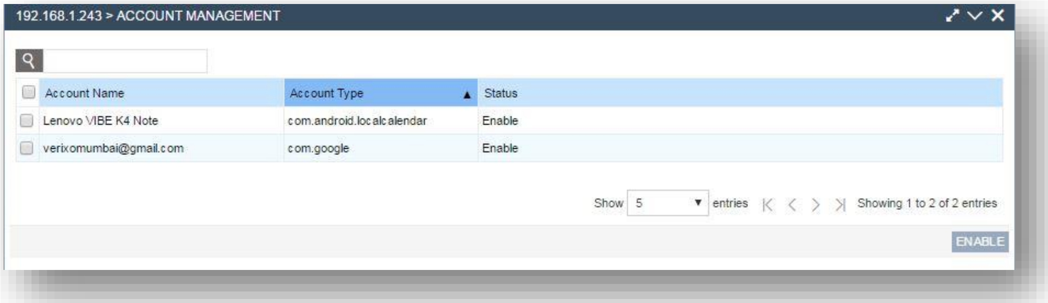
Certificate settings has been applied.

Configuring Account Management Settings

You can enable or disable the new account addition of a particular account type in the work-profile section.

Viewing Account Management

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, then click **Account Management**.



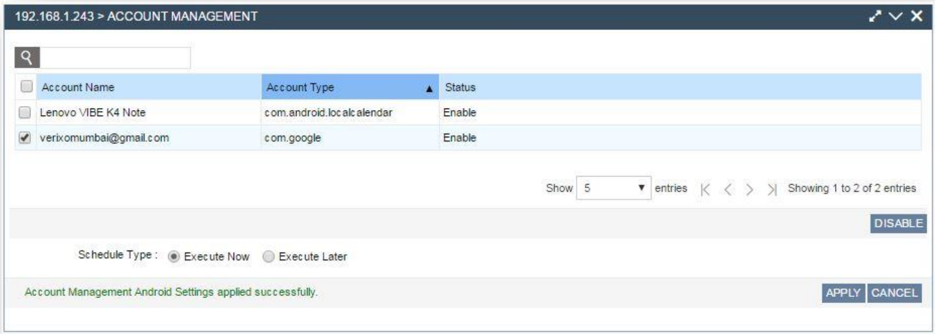
192.168.1.243 > ACCOUNT MANAGEMENT

□ Account Name	Account Type	Status
□ Lenovo VIBE K4 Note	com.android.localcalendar	Enable
□ verixomumbai@gmail.com	com.google	Enable

Show 5 entries Showing 1 to 2 of 2 entries

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Account Management**.
4. Select the check box against the required account name.
5. If the status of the selected account is Enable, then button will be changed to **Disable** and vice-versa.
6. Select the required **Schedule Type**.
7. Click **Apply**.

The Account Management Android Settings applied successfully message is display.



192.168.1.243 > ACCOUNT MANAGEMENT

☐	Account Name	Account Type ▲	Status
☐	Lenovo VIBE K4 Note	com.android.localcalendar	Enable
☑	verixomumbai@gmail.com	com.google	Enable

Show 5 ▾ entries   Showing 1 to 2 of 2 entries

Schedule Type : ● Execute Now ○ Execute Later

Account Management Android Settings applied successfully.

Configuring Global Application Policy Settings

You can configure various application policies on the connected Android device.

Viewing the Global Application Policy

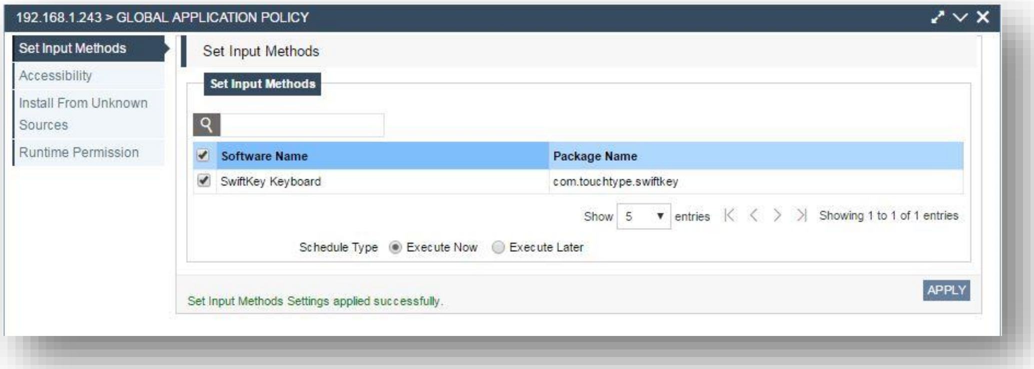
1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Global Application Policy**.

Configuring Set Input Methods

Set Input Methods allows to define what input methods are permitted to use on the device. System input methods are always available to the user. Input methods apply to both profiles; there are no work profile-specific methods.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Global Application Policy**.
4. Select the **Set Input Methods** sub-menu.
5. Select / unselect the required input method to enable/disable purpose respectively.
6. Select the required Schedule Type.
7. Click **Apply**.

The Set Input Methods Settings applied successfully message is display.



☑ Software Name	Package Name
☑ SwiftKey Keyboard	com.touchtype.swiftkey

Show 5 entries Showing 1 to 1 of 1 entries

Schedule Type ● Execute Now ○ Execute Later

Set Input Methods Settings applied successfully.

On device, go to Settings -> Language & Input -> Current Keyboard -> Choose Keyboards.

The applications listed will be allowed or disallowed with the respective applied settings.

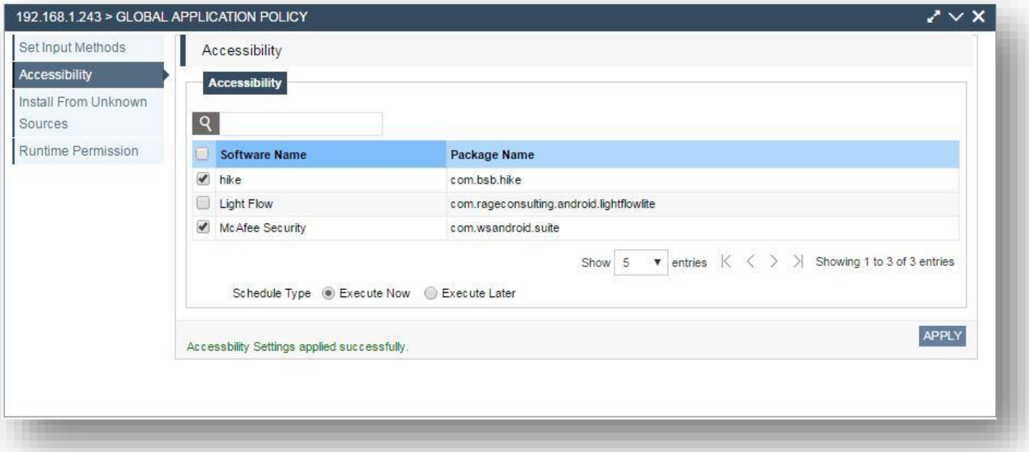
Configuring Accessibility

Accessibility allows to define what services are permitted to use on the device.

System accessibility services are always available to the user. Accessibility services apply to both profiles; there are no work profile-specific accessibility services.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Global Application Policy**.
4. Select the **Accessibility** sub-menu.
5. Select / unselect the required accessibility service to enable/disable purpose respectively.
6. Select the required Schedule Type.
7. Click **Apply**.

   The **Accessibility Settings applied successfully** message is display.


192.168.1.243 > GLOBAL APPLICATION POLICY
Set Input Methods
Accessibility
Install From Unknown Sources
Runtime Permission
Accessibility
Accessibility

☐	Software Name	Package Name
☑	hike	com.bsb.hike
☐	Light Flow	com.rageconsulting.android.lightflowlite
☑	McAfee Security	com.wsandroid.suite

Show 5 entries
Showing 1 to 3 of 3 entries

Schedule Type ● Execute Now ○ Execute Later

Accessbility Settings applied successfully.

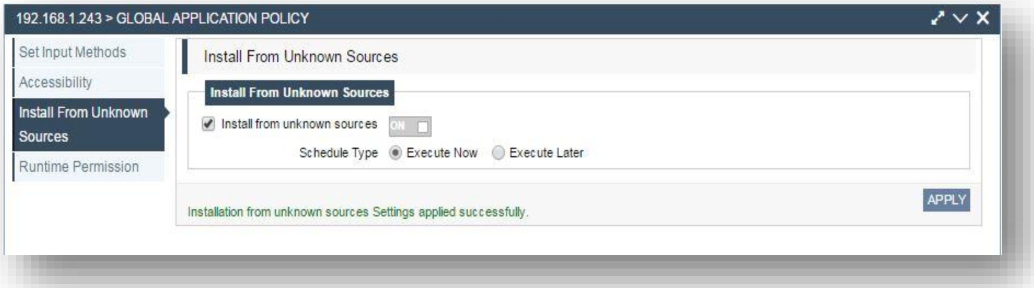
On device, go to Settings -> Accessibility. The applications listed will be enabled or disabled with the respective applied settings.

Configuring Install from Unknown Sources

Install from unknown sources allows the user to install applications manually from external sources like memory cards, shared files, etc.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Global Application Policy**.
4. Select the **Install from Unknown Sources** sub-menu.
5. Select the checkbox against the Install from unknown sources to enable the toggle button.
6. Select the required setting to ON/OFF for enable/ disable purpose respectively.
7. Select the required Schedule Type.
8. Click **Apply**.

   The **Accessibility Settings applied successfully** message is display.


192.168.1.243 > GLOBAL APPLICATION POLICY
Set Input Methods
Accessibility
Install From Unknown Sources
Runtime Permission
Install From Unknown Sources
Install From Unknown Sources

☑ Install from unknown sources ON

Schedule Type ● Execute Now ○ Execute Later

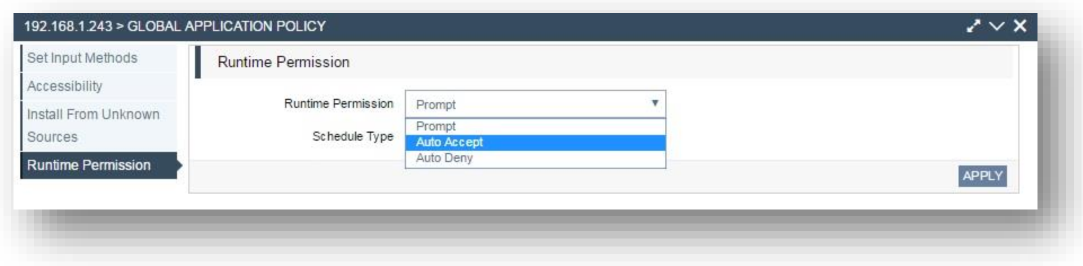
Installation from unknown sources Settings applied successfully.

Configuring Runtime Permissions

You can configure runtime permissions for the work applications on the remotely connected device.

The settings will only be applied to the devices running on Android version 6 and above.

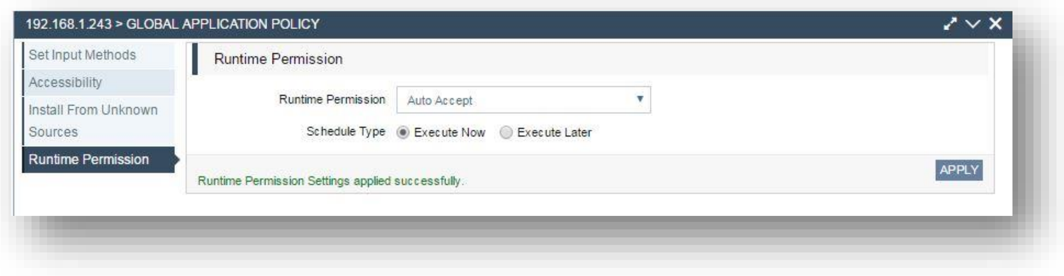
1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Administration**, and then click **Global Application Policy**.
4. Select the **Runtime Permissions** sub-menu.
5. Select the required **Permission** setting.



Runtime Permission: Prompt

6. Select the required **Schedule Type**.
7. Click **Apply**.

   The **Runtime Permission Settings applied successfully** message is display.



Runtime Permission: Auto Accept

Schedule Type ● Execute Now ○ Execute Later

Runtime Permission Settings applied successfully.

Managing Software Deployment

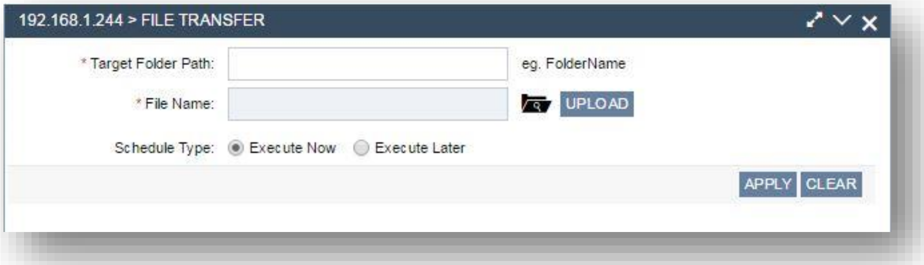
You can remotely check and update software installed on a client device.

Configuring with File Transfer

You can transfer a file on SD card by providing the folder name in which file can be transfer.

1. In the devices tree, click the required machine.
2. Expand the right menu.
3. Click **Software Deployment,** and then click **File Transfer**.

In **Target Folder Path**, enter the folder name where you want to upload the file.

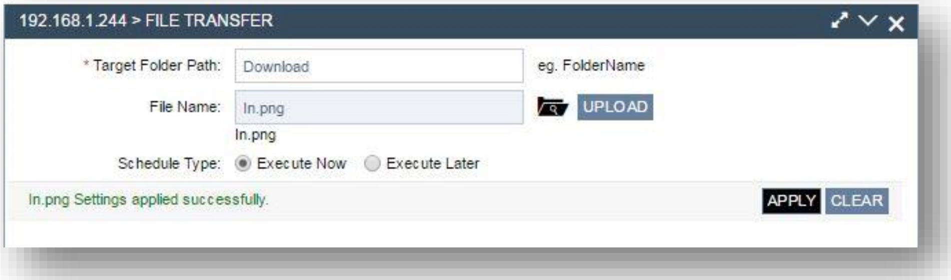


* Target Folder Path:

* File Name:

Schedule Type: ● Execute Now ○ Execute Later

4. Click the **file browser** icon to browse the file to be transferred.
5. Click **Upload** button to upload the selected file.
6. In **File Name**, the uploaded filename will be displayed.
7. Select the required **Schedule Type**.



* Target Folder Path: Download

File Name: In.png

In.png

Schedule Type: ● Execute Now ○ Execute Later

In.png Settings applied successfully.

8. Click **Apply**.

   The **Settings applied successfully** message is display

You need to have a file manager application installed in work-profile to access the transferred file in that particular folder.

Managing Software & Patch Install/Uninstall

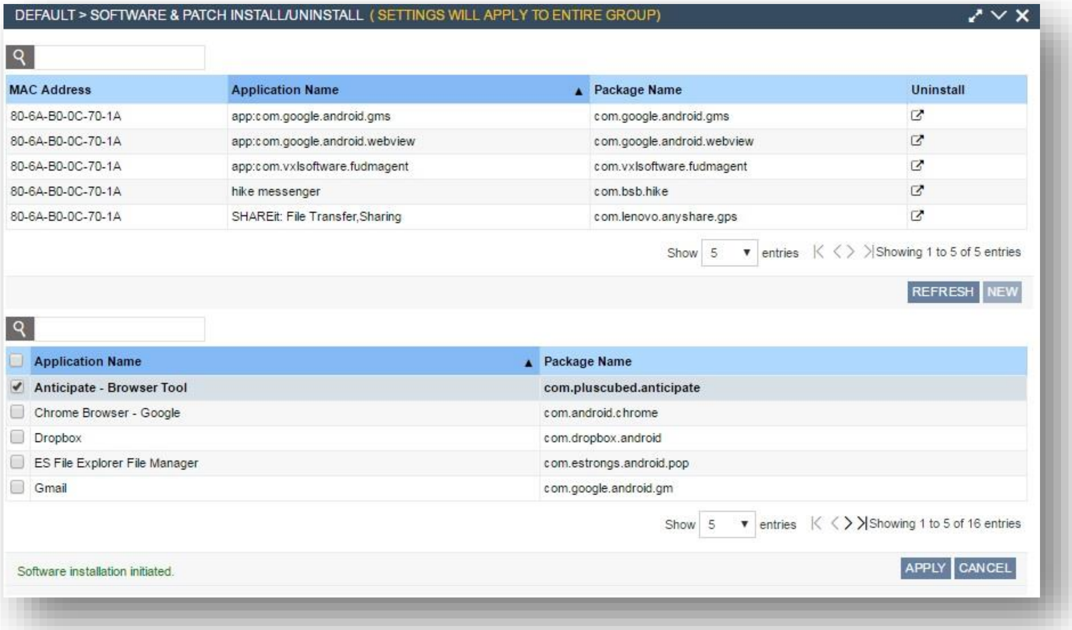
You can view, install and uninstall software from a client device.

Installing Software:

To install software

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click Software Deployment, then click **Software& Patch Install/Uninstall.**
4. Click **New** to install a new application. List of all company approved applications will be displayed.
5. Select the applications to be installed.
6. Click **Apply**.

   The **Software installation initiated** message is displayed.



DEFAULT > SOFTWARE & PATCH INSTALL/UNINSTALL (SETTINGS WILL APPLY TO ENTIRE GROUP)

MAC Address	Application Name	Package Name	Uninstall
80-6A-B0-0C-70-1A	app:com.google.android.gms	com.google.android.gms	↗
80-6A-B0-0C-70-1A	app:com.google.android.webview	com.google.android.webview	↗
80-6A-B0-0C-70-1A	app:com.vxlsoftware.fudmagent	com.vxlsoftware.fudmagent	↗
80-6A-B0-0C-70-1A	hike messenger	com.bsb.hike	↗
80-6A-B0-0C-70-1A	SHAREit: File Transfer,Sharing	com.lenovo.anyshare.gps	↗

Show 5 entries Showing 1 to 5 of 5 entries

☐	Application Name	Package Name
☑	Anticipate - Browser Tool	com.pluscubed.anticipate
☐	Chrome Browser - Google	com.android.chrome
☐	Dropbox	com.dropbox.android
☐	ES File Explorer File Manager	com.estrongs.android.pop
☐	Gmail	com.google.android.gm

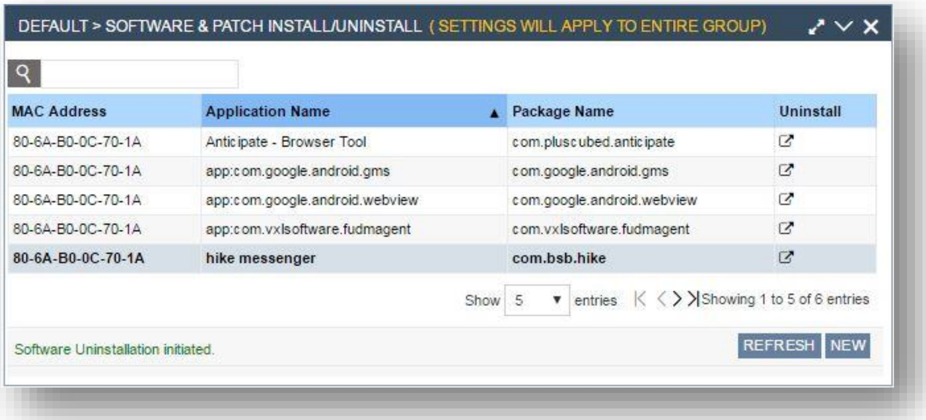
Show 5 entries Showing 1 to 5 of 16 entries

Software installation initiated.

Uninstalling Software:

You can remotely uninstall software from an Android based device.

1. To uninstall software
2. In the devices tree, click the required device.
3. Expand the right menu.
4. Click Software **Deployment, then** click **Software &Patch Install/Uninstall.**


DEFAULT > SOFTWARE & PATCH INSTALL/UNINSTALL (SETTINGS WILL APPLY TO ENTIRE GROUP)
Show 5 entries
Showing 1 to 5 of 6 entries
REFRESH
NEW

MAC Address	Application Name ▲	Package Name	Uninstall
80-6A-B0-0C-70-1A	Anticipate - Browser Tool	com.pluscubed.anticipate	↗
80-6A-B0-0C-70-1A	app:com.google.android.gms	com.google.android.gms	↗
80-6A-B0-0C-70-1A	app:com.google.android.webview	com.google.android.webview	↗
80-6A-B0-0C-70-1A	app:com.vxlsoftware.fudmagent	com.vxlsoftware.fudmagent	↗
80-6A-B0-0C-70-1A	**hike messenger**	**com.bsb.hike**	↗

Software Uninstallation initiated.

5. In the table, select the software to uninstall.
6. Click the **Uninstall icon**.

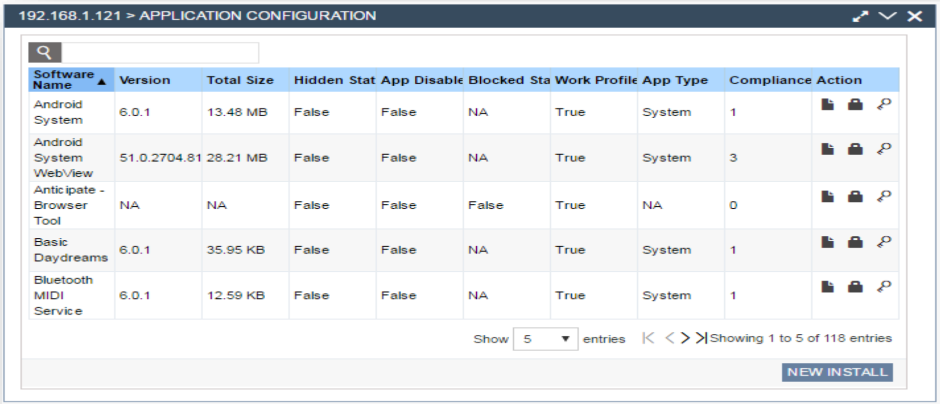
   The **Software uninstallation initiated** message is display.

Configuring Application Configuration Settings

You can view, install applications, also manage the policy, permissions and provide the restrictions for specific android application on device.

Viewing Application Configuration

1. In the devices tree, click the required android device.
2. Expand the right menu.
3. Click **Software Deployment,** and then click **Application Configuration**.


192.168.1.121 > APPLICATION CONFIGURATION
Show 5 entries
Showing 1 to 5 of 118 entries
NEW INSTALL

Software Name ▲	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action
Android System	6.0.1	13.48 MB	False	False	NA	True	System	1	📄 🔒 🔍
Android System WebView	51.0.2704.81	28.21 MB	False	False	NA	True	System	3	📄 🔒 🔍
Anticipate - Browser Tool	NA	NA	False	False	False	True	NA	0	📄 🔒 🔍
Basic Daydreams	6.0.1	35.95 KB	False	False	NA	True	System	1	📄 🔒 🔍
Bluetooth MIDI Service	6.0.1	12.59 KB	False	False	NA	True	System	1	📄 🔒 🔍

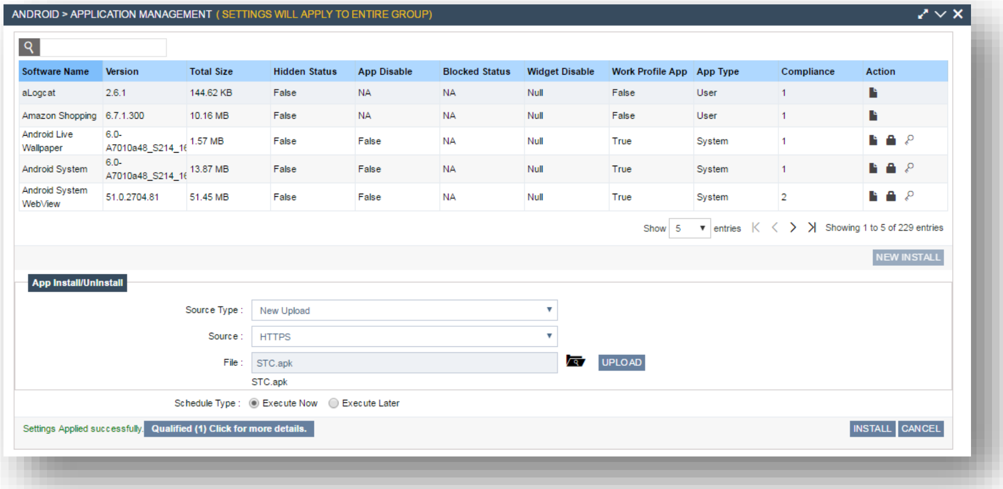
Group: On group, organization approved applications list are displayed.

Node: On node after synchronize the applications which present on the agent device get listed out along with their permissions and policy.

Installing applications

1. In the devices tree, click the required Android device.
2. Click **New Install**.
3. In the **Source Type** list, select the required source.
4. In the **Source** list, select the required source.
5. In the **File** list, select the required apk for application installation.
6. Select the required **Schedule Type**.
7. Click **Apply**.

   The Installation schedule message is display.



ANDROID > APPLICATION MANAGEMENT (SETTINGS WILL APPLY TO ENTIRE GROUP)

Software Name	Version	Total Size	Hidden Status	App Disable	Blocked Status	Widget Disable	Work Profile App	App Type	Compliance	Action
aLogcat	2.6.1	144.62 KB	False	NA	NA	Null	False	User	1	
Amazon Shopping	6.7.1.300	10.16 MB	False	NA	NA	Null	False	User	1	
Android Live Wallpaper	6.0-A7010a48_S214_16	1.57 MB	False	False	NA	Null	True	System	1	
Android System	6.0-A7010a48_S214_16	13.87 MB	False	False	NA	Null	True	System	1	
Android System WebView	51.0.2704.81	51.45 MB	False	False	NA	Null	True	System	2	

Show 5 entries Showing 1 to 5 of 229 entries

App Install/Uninstall

Source Type : New Upload

Source : HTTPS

File : STC.apk

STC.apk

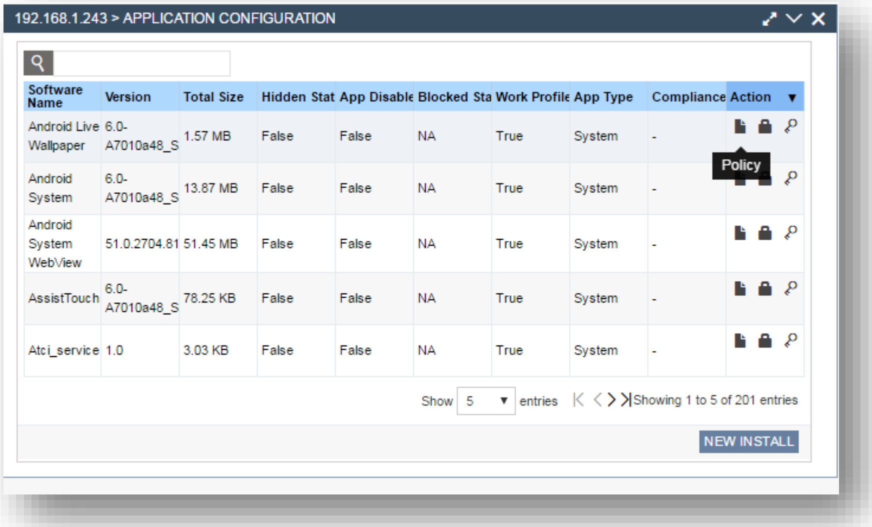
Schedule Type : ● Execute Now ○ Execute Later

Settings Applied successfully. Qualified (1) Click for more details.

Configuring Applications Policy:

You can able to enable /disable (i.e. ON/OFF) three type of policies from server:

- **Disable**-This type of policy disables the application. (i.e. Options present on that application not getting worked).
- **Block**-This type of policy blocks the uninstallation of the applications. (i.e. Application doesn't get uninstalled).
- **Hide**-Under this type of policy, application icon gets hide on Android device.



192.168.1.243 > APPLICATION CONFIGURATION

Software Name	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action
Android Live Wallpaper	6.0-A7010a48_S	1.57 MB	False	False	NA	True	System	-	
Android System	6.0-A7010a48_S	13.87 MB	False	False	NA	True	System	-	
Android System WebView	51.0.2704.81	51.45 MB	False	False	NA	True	System	-	
AssistTouch	6.0-A7010a48_S	78.25 KB	False	False	NA	True	System	-	
Atci_service	1.0	3.03 KB	False	False	NA	True	System	-	

While applying these policies, the following conditions must get present.

1.For Disable Policy: **App Disable** column value must be True and **App Type** must be System.

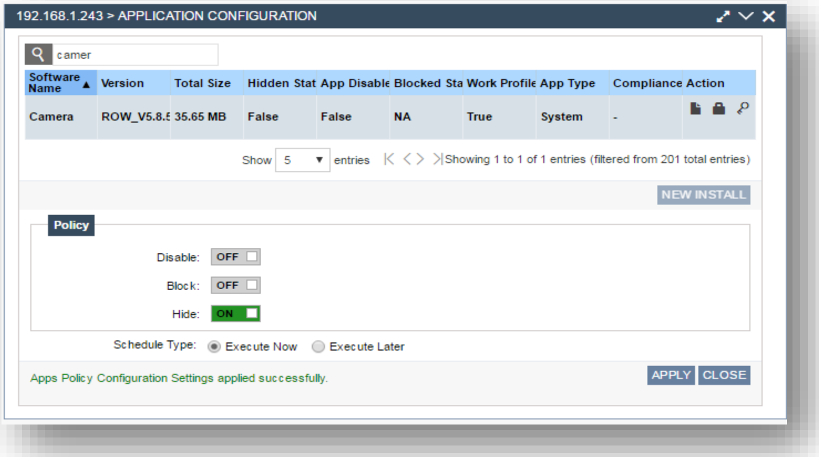
2.For Block policy: **Work Profile** column value must be True and **App Type** must be User.

3.For Hide policy: **Work Profile** column value must be True.

Applying policy:

1. In the devices tree, click the required android device.
2. Click **Policy** icon against the application listed of which you wish to change the policy**.**
3. Apply policy as per conditions mentioned in note.
4. Select the required **Schedule Type**.
5. Click **Apply**.

   The **Policy settings applied** schedule message is display.



192.168.1.243 > APPLICATION CONFIGURATION

camer

Software Name ▲	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action
Camera	ROW_V5.8.5	35.65 MB	False	False	NA	True	System	-	

Show 5 ▾ entries |< < > >| Showing 1 to 1 of 1 entries (filtered from 201 total entries)

Policy

Disable: OFF

Block: OFF

Hide: ON

Schedule Type: ● Execute Now ○ Execute Later

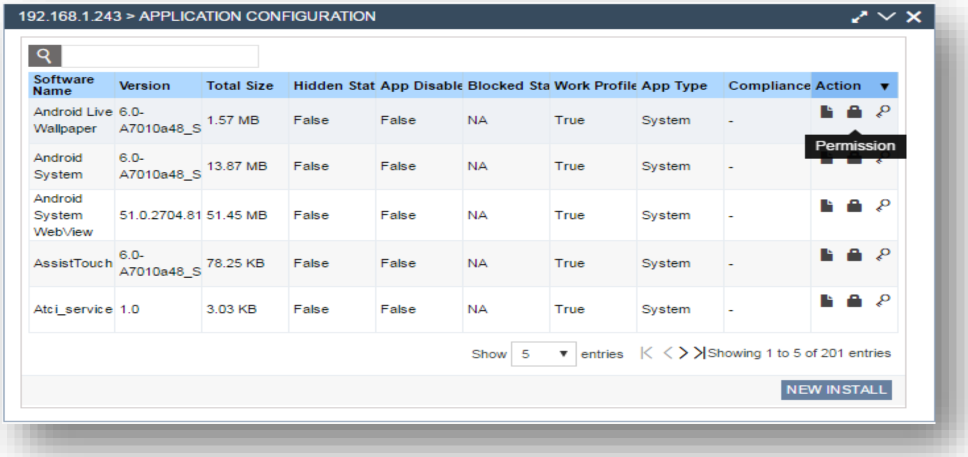
Apps Policy Configuration Settings applied successfully.

Configuring Applications Permission:

You can able set three type of permission from server:

1. **Allow**- Corresponding permission will be forcefully allowed to access for that application.
2. **Deny**-Corresponding permission will be forcefully denied to access for that application.

3. **User Select**-Correspond permission will be select as per user choice whether to allow / deny access for that application.



192.168.1.243 > APPLICATION CONFIGURATION

Software Name	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action ▼
Android Live Wallpaper	6.0-A7010a48_S	1.57 MB	False	False	NA	True	System	-	
Android System	6.0-A7010a48_S	13.87 MB	False	False	NA	True	System	-	
Android System WebView	51.0.2704.81	51.45 MB	False	False	NA	True	System	-	
AssistTouch	6.0-A7010a48_S	78.25 KB	False	False	NA	True	System	-	
Atci_service	1.0	3.03 KB	False	False	NA	True	System	-	

Show 5 ▾ entries |< < > >| Showing 1 to 5 of 201 entries

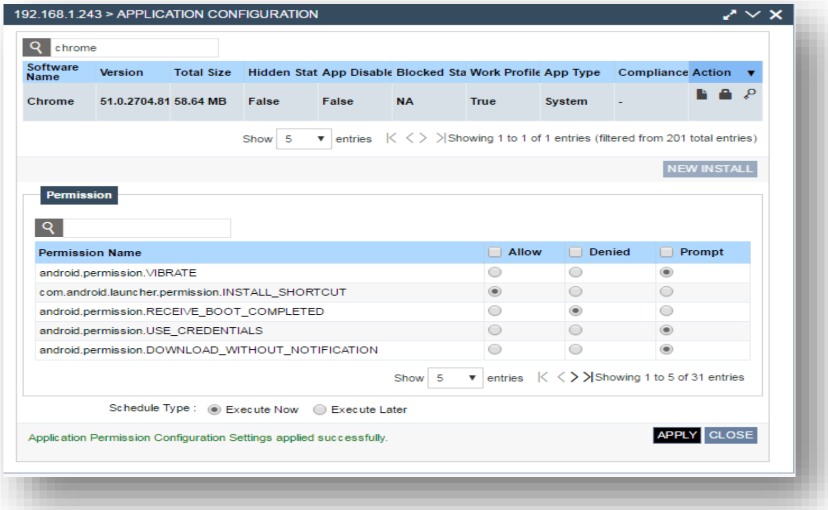
The settings will only be applied to the devices running on Android version 6 and above.

Applying Permission on software:

1. In the devices tree, click the required android device.

2. Click **Permission** icon against the application of which you wish to change the permission.
3. Select the permissions to be set for that application against its respective Permission Name.
4. Select the required **Schedule Type**.
5. Click **Apply**.

   The Permission settings applied schedule message is displayed.



chrome

Software Name	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action
Chrome	51.0.2704.81	58.64 MB	False	False	NA	True	System	-	

Show 5 entries Showing 1 to 1 of 1 entries (filtered from 201 total entries)

Permission Name	□ Allow	□ Denied	□ Prompt
android.permission.VIBRATE	○	○	●
com.android.launcher.permission.INSTALL_SHORTCUT	●	○	○
android.permission.RECEIVE_BOOT_COMPLETED	○	●	○
android.permission.USE_CREDENTIALS	○	○	●
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	○	○	●

Show 5 entries Showing 1 to 5 of 31 entries

Schedule Type : ● Execute Now ○ Execute Later

Application Permission Configuration Settings applied successfully.

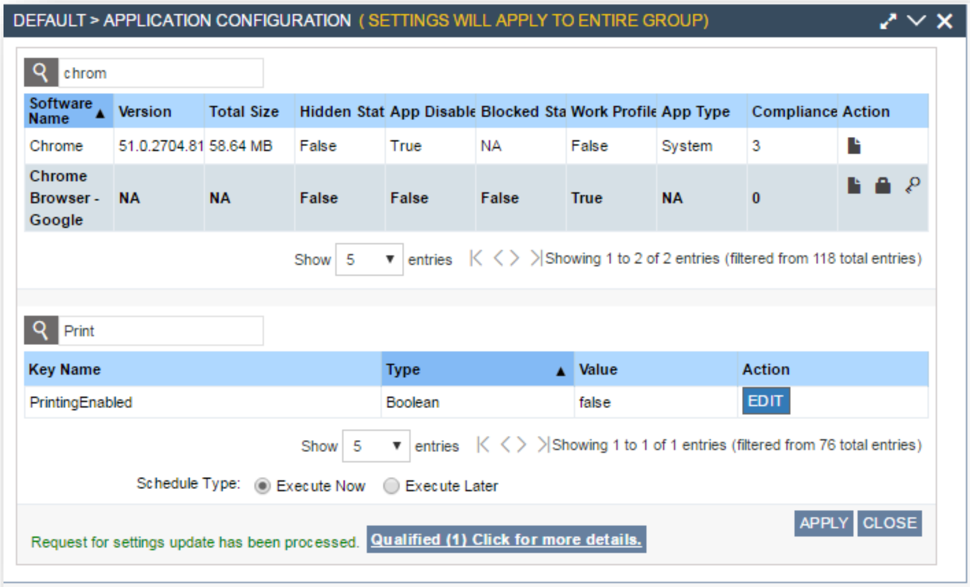
Configuring Applications Restriction:

You can able to restrict the application by providing key and value from server (i.e.-key indicates the which restriction is present on application and value indicated whether On/Off that restriction)

Applying Restriction on software:

1. In the devices tree, click the required android device.
2. Click **Restriction** icon present in data table.
3. Different key with their values are listed. Click on **EDIT** button
4. In **Value**, enter the required value as per data type.
5. Click **Save** to save the restriction.
6. Select the required **Schedule Type**.
7. Click **Apply.**

   The applying Restriction schedule message is displayed.



DEFAULT > APPLICATION CONFIGURATION (SETTINGS WILL APPLY TO ENTIRE GROUP)

chrom

Software Name ▲	Version	Total Size	Hidden Stat	App Disable	Blocked Sta	Work Profile	App Type	Compliance	Action
Chrome	51.0.2704.81	58.64 MB	False	True	NA	False	System	3	
Chrome Browser - Google	**NA**	**NA**	**False**	**False**	**False**	**True**	**NA**	**0**	

Show 5 ▾ entries |< < > >| Showing 1 to 2 of 2 entries (filtered from 118 total entries)

Print

Key Name	Type ▲	Value	Action
PrintingEnabled	Boolean	false	EDIT

Show 5 ▾ entries |< < > >| Showing 1 to 1 of 1 entries (filtered from 76 total entries)

Schedule Type: ● Execute Now ○ Execute Later

Request for settings update has been processed. Qualified (1) Click for more details.

Working with Manage Profile Policy Settings

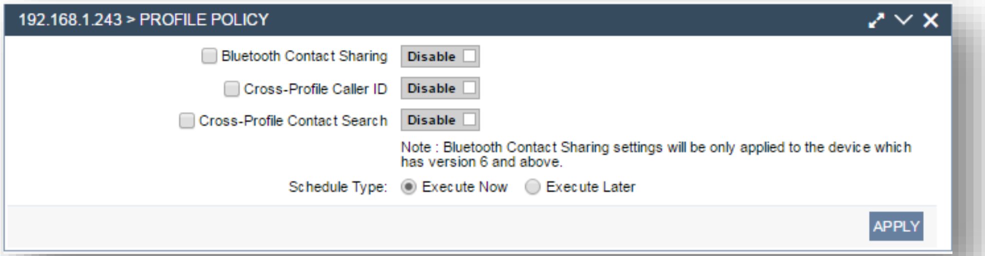
You can configure various Profile Policy settings on the connected Android device.

Configuring Profile Policy Settings

You can configure various policies such as Bluetooth contact sharing, Cross-profile caller ID, Cross-profile contact search on the connected Android device.

Viewing Profile Policy

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Profile Policy**.



192.168.1.243 > PROFILE POLICY

□ Bluetooth Contact Sharing Disable □

□ Cross-Profile Caller ID Disable □

□ Cross-Profile Contact Search Disable □

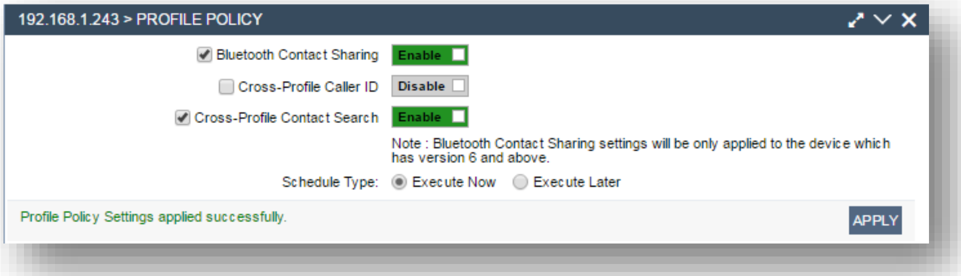
Note : Bluetooth Contact Sharing settings will be only applied to the device which has version 6 and above.

Schedule Type: ● Execute Now ○ Execute Later

Configuring Profile Policy

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Profile Policy.**
4. On selecting the checkbox against the policy, its respective Enable/Disable toggle button will be enabled.
5. **Enable** or **Disable** the required policy.
6. Select the required **Schedule Type**.
7. Click **Apply**.

   The **Profile Policy Settings applied successfully** message is displayed.



192.168.1.243 > PROFILE POLICY

☑ Bluetooth Contact Sharing — Enable

☐ Cross-Profile Caller ID — Disable

☑ Cross-Profile Contact Search — Enable

Note : Bluetooth Contact Sharing settings will be only applied to the device which has version 6 and above.

Schedule Type: ● Execute Now ○ Execute Later

Profile Policy Settings applied successfully.

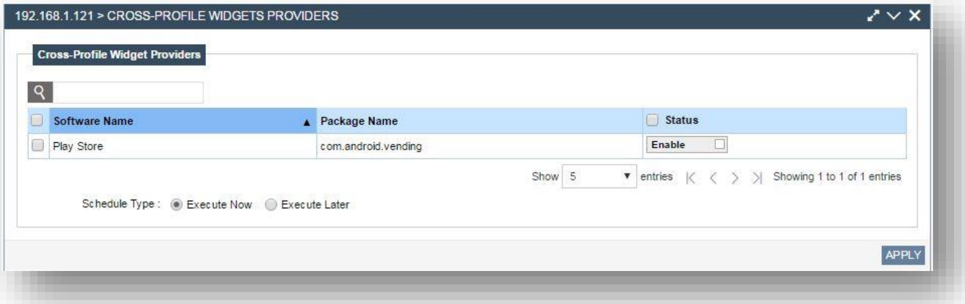
APPLY

Configuring Cross-Profile Widgets Providers Settings

You can allow a managed profile administrator to whitelist some apps to publish widgets on the home-screen on the connected Android device.

Viewing Cross-Profile Widgets Providers

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Cross-Profile Widgets Providers**.



192.168.1.121 > CROSS-PROFILE WIDGETS PROVIDERS

Cross-Profile Widget Providers

☐	Software Name ▲	Package Name	☐ Status
☐	Play Store	com.android.vending	Enable

Show 5 entries — Showing 1 to 1 of 1 entries

Schedule Type : ● Execute Now ○ Execute Later

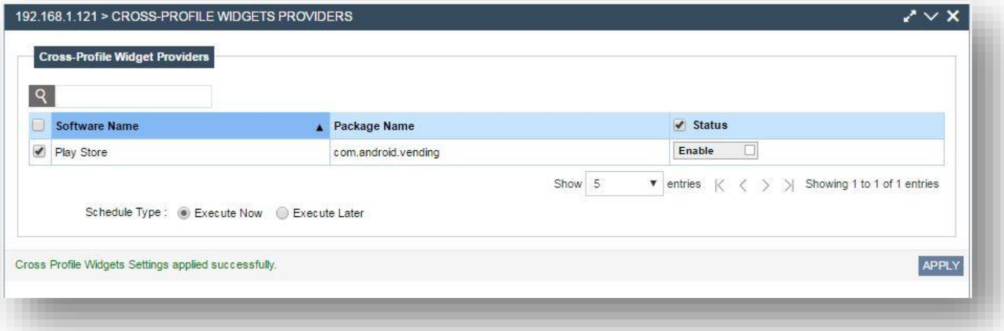
APPLY

Configuring Cross-Profile Widgets Providers

1. In the devices tree, click the required device.

2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Cross-Profile Widgets Providers**.
4. On selecting the checkbox against the widget, its respective Enable/Disable toggle button will be enabled.
5. **Enable** or **Disable** the required widget.
6. Select the required **Schedule Type**.
7. Click **Apply**.

The Cross Profile Widgets Settings applied successfully message is displayed.


192.168.1.121 > CROSS-PROFILE WIDGETS PROVIDERS
Cross-Profile Widget Providers
Show 5 entries
Showing 1 to 1 of 1 entries
APPLY

□	Software Name	Package Name	☑ Status
☑	Play Store	com.android.vending	Enable □

Schedule Type : ● Execute Now ○ Execute Later

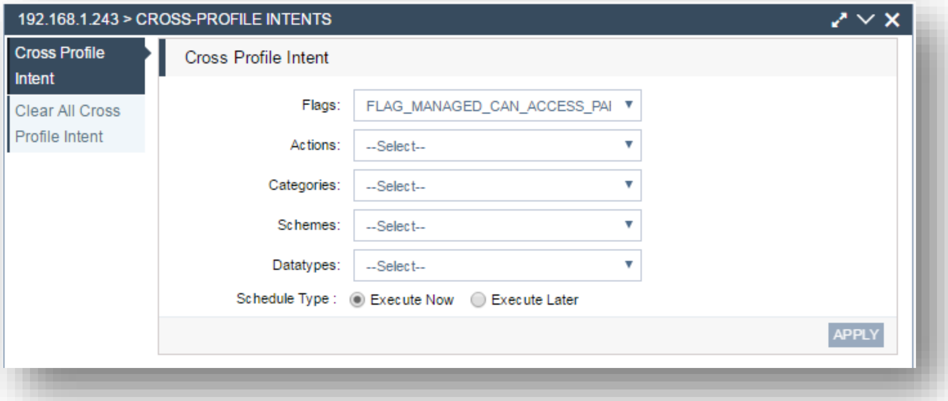
Cross Profile Widgets Settings applied successfully.

Configuring Cross-Profile Intent Settings

The Cross-Profile Intents can whitelist sharing of particular content from apps within the personal profile to the managed profile and vice-versa.

Configuring Cross-Profile Intents

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Cross-Profile Intents**.


192.168.1.243 > CROSS-PROFILE INTENTS
Cross Profile Intent
Clear All Cross Profile Intent
Cross Profile Intent
APPLY

Flags: FLAG_MANAGED_CAN_ACCESS_PAI

Actions: --Select--

Categories: --Select--

Schemes: --Select--

Datatypes: --Select--

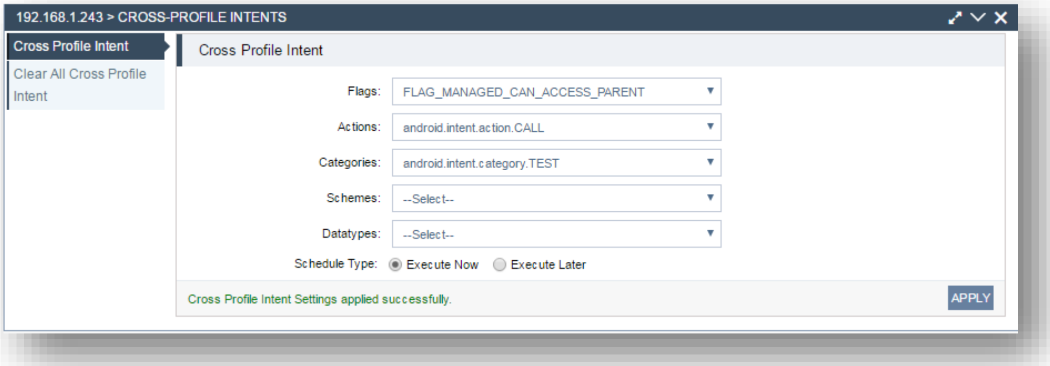
Schedule Type : ● Execute Now ○ Execute Later

4. In **Flags**, select the required value.

If you want the intent to forward from the work profile to the personal profile, select FLAG_MANAGED_CAN_ACCESS_PARENT.

If you want the intent to forward the other way, select FLAG_PARENT_CAN_ACCESS_MANAGED.

5. In **Actions**, select the required value.
6. In **Categories**, select the required value.
7. In **Schemes**, select the required value.
8. In **Data type**, select the required value.
9. You can also add a custom value by selecting **Custom** option from the dropdown and enter the required value in the textbox appearing next to the corresponding field.
10. Select the required **Schedule Type**.
11. Click **Apply**.
12. The **Cross Profile Intents Settings applied successfully** message is displayed.



192.168.1.243 > CROSS-PROFILE INTENTS

Cross Profile Intent

Flags: FLAG_MANAGED_CAN_ACCESS_PARENT

Actions: android.intent.action.CALL

Categories: android.intent.category.TEST

Schemes: --Select--

Datatypes: --Select--

Schedule Type: ● Execute Now ○ Execute Later

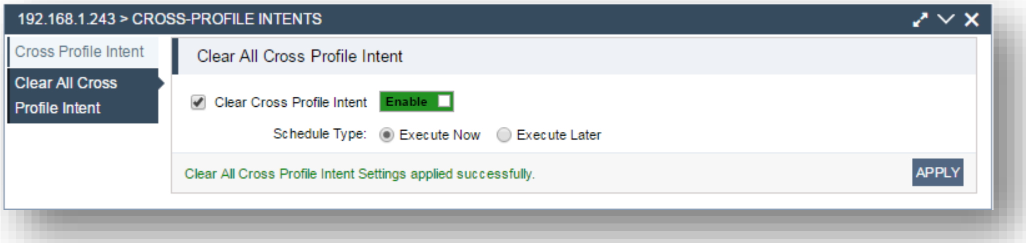
Cross Profile Intent Settings applied successfully.

Configuring Clear All Cross-Profile Intents

In Clear All Cross-Profile Intents, you can clear all the previously applied intents which were applied to the device.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click **Manage Profile Policy**, then click **Cross-Profile Intents**.
4. Click **Clear All Cross-Profile Intents** sub-menu.
5. Select the checkbox to enable the Enable/Disable button.
6. Toggle the button to **Enable** state.
7. Select the required **Schedule Type**.
8. Click **Apply**.

The Cross Profile Intents Settings applied successfully message is displayed.



192.168.1.243 > CROSS-PROFILE INTENTS

Clear All Cross Profile Intent

☑ Clear Cross Profile Intent Enable

Schedule Type: ● Execute Now ○ Execute Later

Clear All Cross Profile Intent Settings applied successfully.

Working with the Device Manager for Apple iOS

Viewing General Information

Under **System Information**, you can also view the following general information:

- System Information
- System Profile
- Certificate Details
- Application information
- Security information
- Profile List
- Provision Profile List

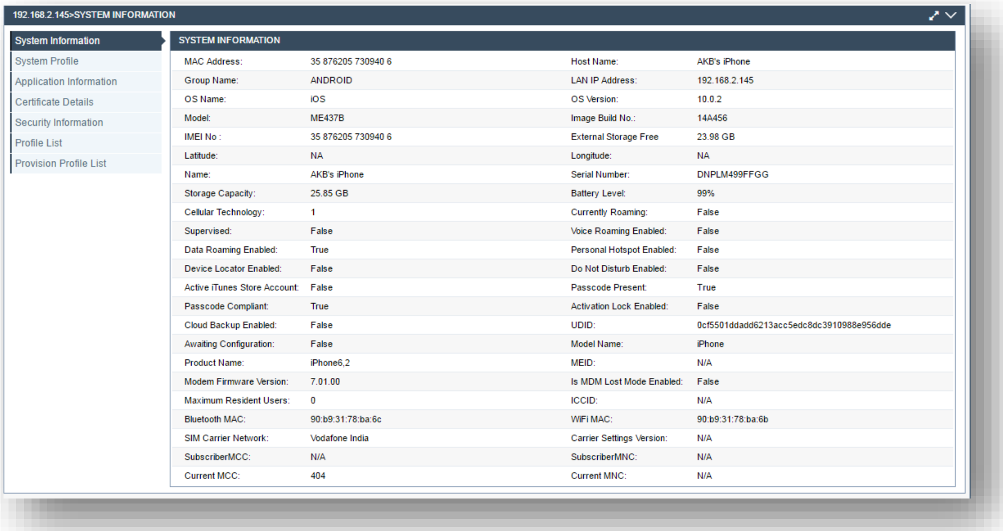
Viewing System Information

System Information provides an overview of system-related information for a network-connected device.

The information displayed is specific to the operating device. For example, the information displayed for an Android based device will be different from the information displayed for a iOS based device.

To view system information

1. In the devices tree, click the required device.
2. The **System Information** pane is display.



SYSTEM INFORMATION

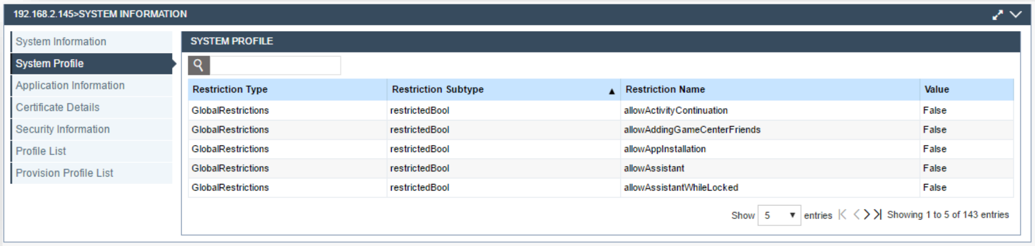
MAC Address:	35 876205 730940 6	Host Name:	AKB's iPhone
Group Name:	ANDROID	LAN IP Address:	192.168.2.145
OS Name:	iOS	OS Version:	10.0.2
Model:	ME437B	Image Build No.:	14A456
IMEI No :	35 876205 730940 6	External Storage Free	23.98 GB
Latitude:	NA	Longitude:	NA
Name:	AKB's iPhone	Serial Number:	DNPLM499FFGG
Storage Capacity:	25.85 GB	Battery Level:	99%
Cellular Technology:	1	Currently Roaming:	False
Supervised:	False	Voice Roaming Enabled:	False
Data Roaming Enabled:	True	Personal Hotspot Enabled:	False
Device Locator Enabled:	False	Do Not Disturb Enabled:	False
Active iTunes Store Account:	False	Passcode Present:	True
Passcode Compliant:	True	Activation Lock Enabled:	False
Cloud Backup Enabled:	False	UDID:	0cf5501ddadd6213acc5edc8dc3910988e956dde
Awaiting Configuration:	False	Model Name:	iPhone
Product Name:	iPhone6,2	MEID:	N/A
Modem Firmware Version:	7.01.00	Is MDM Lost Mode Enabled:	False
Maximum Resident Users:	0	ICCID:	N/A
Bluetooth MAC:	90:b9:31:78:ba:6c	WiFi MAC:	90:b9:31:78:ba:6b
SIM Carrier Network:	Vodafone India	Carrier Settings Version:	N/A
SubscriberMCC:	N/A	SubscriberMNC:	N/A
Current MCC:	404	Current MNC:	N/A

Viewing System Profile

Restriction type displayed which comes under particular system.

To view the system profile

1. In the devices tree, click the required device.
2. Under **System Information**, click **System Profile**.

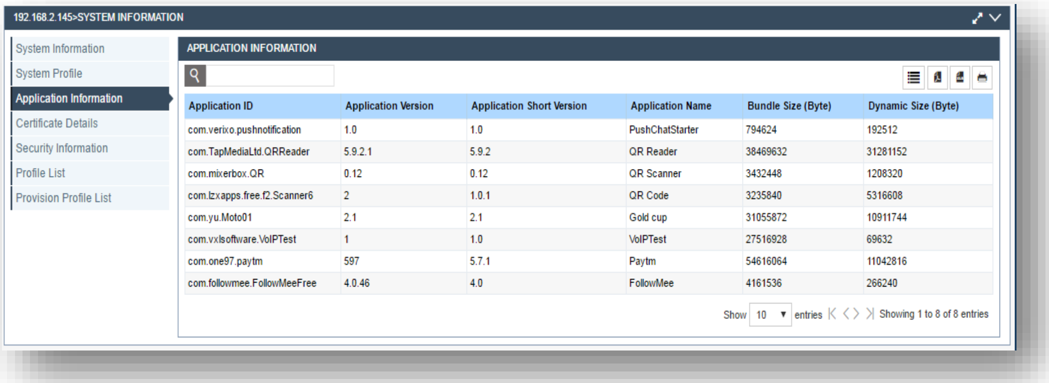


Restriction Type	Restriction Subtype	Restriction Name	Value
GlobalRestrictions	restrictedBool	allowActivityContinuation	False
GlobalRestrictions	restrictedBool	allowAddingGameCenterFriends	False
GlobalRestrictions	restrictedBool	allowAppInstallation	False
GlobalRestrictions	restrictedBool	allowAssistant	False
GlobalRestrictions	restrictedBool	allowAssistantWhileLocked	False

Show 5 entries Showing 1 to 5 of 143 entries

Viewing Application Information

All detailed information about each of the applications installed in the selected device are listed out. The information includes the following: Software Name, Package Name, Version Name, Description, Last Update Date, Install Location, Install Size, Data Size, Total Size, Hidden Status, App Disable, Blocked Status, Widget Disable, Work Profile App and App Type.

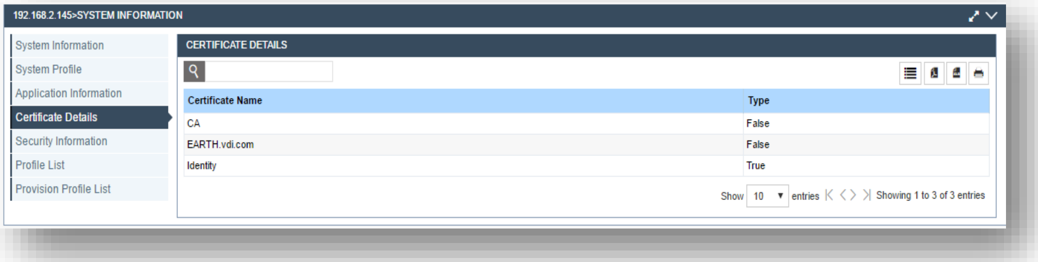


Application ID	Application Version	Application Short Version	Application Name	Bundle Size (Byte)	Dynamic Size (Byte)
com.verixo.pushnotification	1.0	1.0	PushChatStarter	794624	192512
com.TapMediaLtd.QRReader	5.9.2.1	5.9.2	QR Reader	38469632	31281152
com.mixerbox.QR	0.12	0.12	QR Scanner	3432448	1208320
com.lzxapps.free.f2.Scanner6	2	1.0.1	QR Code	3235840	5316608
com.yu.Moto01	2.1	2.1	Gold cup	31055872	10911744
com.vxlsoftware.VoIPTest	1	1.0	VoIPTest	27516928	69632
com.one97.paytm	597	5.7.1	Paytm	54616064	11042816
com.followmee.FollowMeeFree	4.0.46	4.0	FollowMee	4161536	266240

Show 10 entries Showing 1 to 8 of 8 entries

Viewing Certificate Details

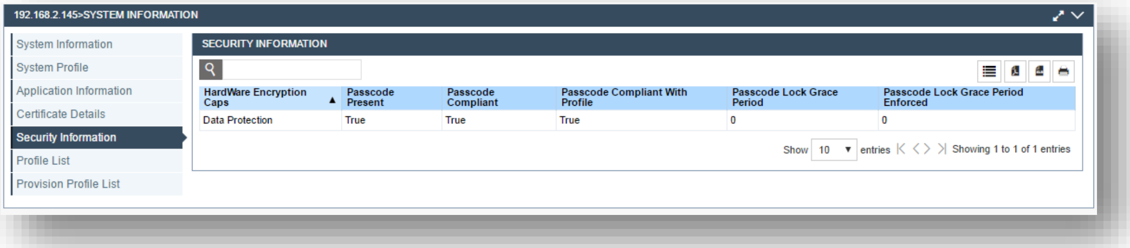
All system and manually added certificates are listed out in certificate details where all information about all certificates present in device such as Certificate name, issued to, Issue by, Valid from date and Valid to date is display.



Certificate Name	Type
CA	False
EARTH.vdi.com	False
Identity	True

Show 10 entries Showing 1 to 3 of 3 entries

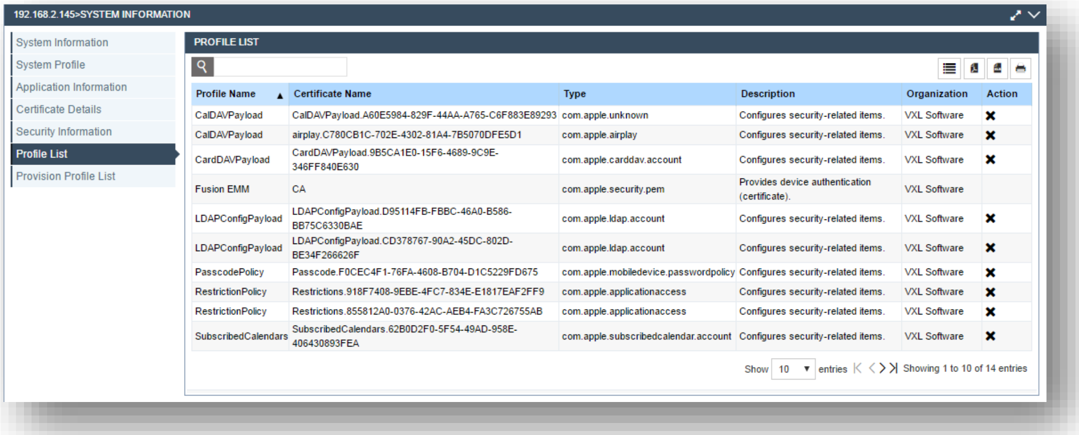
Viewing Security Information



HardWare Encryption Caps	Passcode Present	Passcode Compliant	Passcode Compliant With Profile	Passcode Lock Grace Period	Passcode Lock Grace Period Enforced
Data Protection	True	True	True	0	0

Show 10 entries Showing 1 to 1 of 1 entries

Viewing Profile List



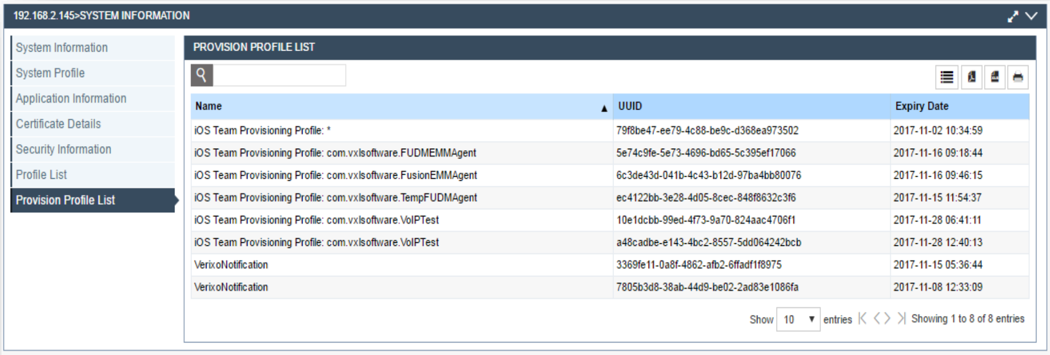
192.168.2.145>SYSTEM INFORMATION

PROFILE LIST

Profile Name	Certificate Name	Type	Description	Organization	Action
CalDAVPayload	CalDAVPayload.A60E5984-829F-44AA-A765-C6F883E89293	com.apple.unknown	Configures security-related items.	VXL Software	✖
CalDAVPayload	airplay.C780CB1C-702E-4302-81A4-7B5070DFE5D1	com.apple.airplay	Configures security-related items.	VXL Software	✖
CardDAVPayload	CardDAVPayload.9B5CA1E0-15F6-4689-9C9E-346FF840E630	com.apple.carddav.account	Configures security-related items.	VXL Software	✖
Fusion EMM	CA	com.apple.security.pem	Provides device authentication (certificate).	VXL Software	
LDAPConfigPayload	LDAPConfigPayload.D95114FB-FBBC-46A0-B586-BB75C6330BAE	com.apple.ldap.account	Configures security-related items.	VXL Software	✖
LDAPConfigPayload	LDAPConfigPayload.CD378767-90A2-45DC-802D-BE34F266626F	com.apple.ldap.account	Configures security-related items.	VXL Software	✖
PasscodePolicy	Passcode.F0CEC4F1-76FA-4608-B704-D1C5229FD675	com.apple.mobiledevice.passwordpolicy	Configures security-related items.	VXL Software	✖
RestrictionPolicy	Restrictions.918F7408-9EBE-4FC7-834E-E1817EAF2FF9	com.apple.applicationaccess	Configures security-related items.	VXL Software	✖
RestrictionPolicy	Restrictions.855812A0-0376-42AC-AEB4-FA3C726755AB	com.apple.applicationaccess	Configures security-related items.	VXL Software	✖
SubscribedCalendars	SubscribedCalendars.62B0D2F0-5F54-49AD-958E-406430893FEA	com.apple.subscribedcalendar.account	Configures security-related items.	VXL Software	✖

Show 10 entries Showing 1 to 10 of 14 entries

Viewing Provision Profile List



192.168.2.145>SYSTEM INFORMATION

PROVISION PROFILE LIST

Name	UUID	Expiry Date
iOS Team Provisioning Profile: *	79f8be47-ee79-4c88-be9c-d368ea973502	2017-11-02 10:34:59
iOS Team Provisioning Profile: com.vxlsoftware.FUDMEMMAgent	5e74c9fe-5e73-4696-bd65-5c395ef17066	2017-11-16 09:18:44
iOS Team Provisioning Profile: com.vxlsoftware.FusionEMMAgent	6c3de43d-041b-4c43-b12d-97ba4bb80076	2017-11-16 09:46:15
iOS Team Provisioning Profile: com.vxlsoftware.TempFUDMAgent	ec4122bb-3e28-4d05-8cec-848f8632c3f6	2017-11-15 11:54:37
iOS Team Provisioning Profile: com.vxlsoftware.VoIPTest	10e1dcbb-99ed-4f73-9a70-824aac4706f1	2017-11-28 06:41:11
iOS Team Provisioning Profile: com.vxlsoftware.VoIPTest	a48cadbe-e143-4bc2-8557-5dd064242bcb	2017-11-28 12:40:13
VerixoNotification	3369fe11-0a8f-4862-afb2-6ffadf1f8975	2017-11-15 05:36:44
VerixoNotification	7805b3d8-38ab-44d9-be02-2ad83e1086fa	2017-11-08 12:33:09

Show 10 entries Showing 1 to 8 of 8 entries

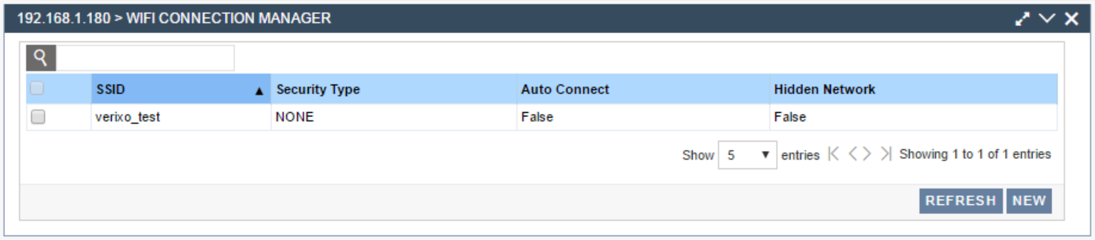
Configuring System Settings

Configuring Wifi Connection Manager Settings

User able to **Add and View** connections

Viewing the List of network connections

1. Click on **system settings** then click on **Network Settings** & then click on **WIFI connection manager.**
2. WiFi connection manager module displayed list of connections present on device and made by user.
3. User able to refresh table content by click on **REFRESH** button.

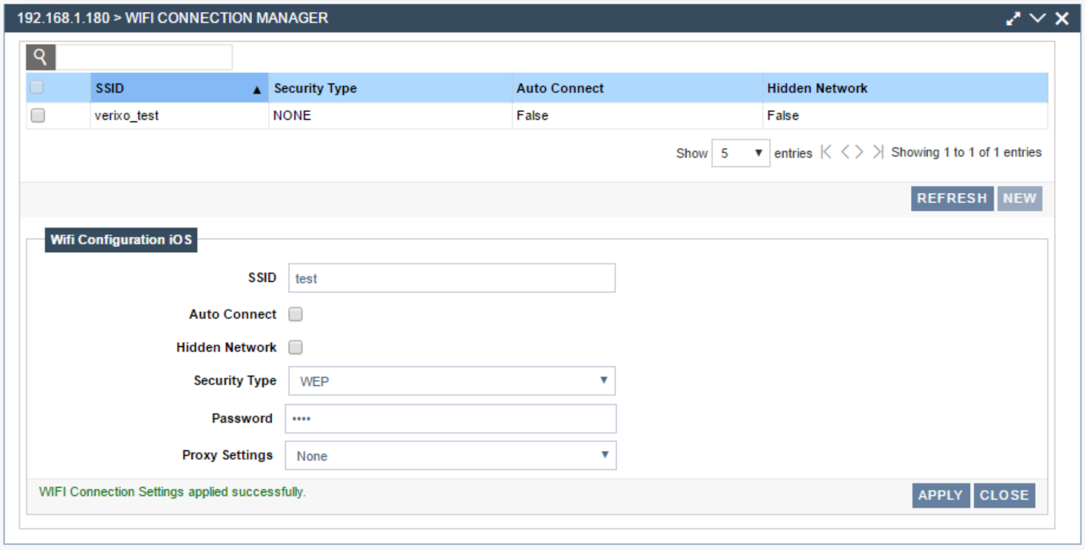

192.168.1.180 > WIFI CONNECTION MANAGER

☐	SSID ▲	Security Type	Auto Connect	Hidden Network
☐	verixo_test	NONE	False	False

Show 5 entries Showing 1 to 1 of 1 entries

Adding a network connection

1. Click on **system settings** then click on **Network Settings** & then click on **WIFI connection manager.**
2. Click on **New** Button to add new connection.
3. User able to enter all mandatory data.
4. Select Security type from drop down value.
5. Enter password for WIFI connection.
6. Click on **APPLY** button to create connection.


192.168.1.180 > WIFI CONNECTION MANAGER

☐	SSID ▲	Security Type	Auto Connect	Hidden Network
☐	verixo_test	NONE	False	False

Show 5 entries Showing 1 to 1 of 1 entries

Wifi Configuration iOS

SSID: test

Auto Connect ☐

Hidden Network ☐

Security Type: WEP

Password: ••••

Proxy Settings: None

WIFI Connection Settings applied successfully.

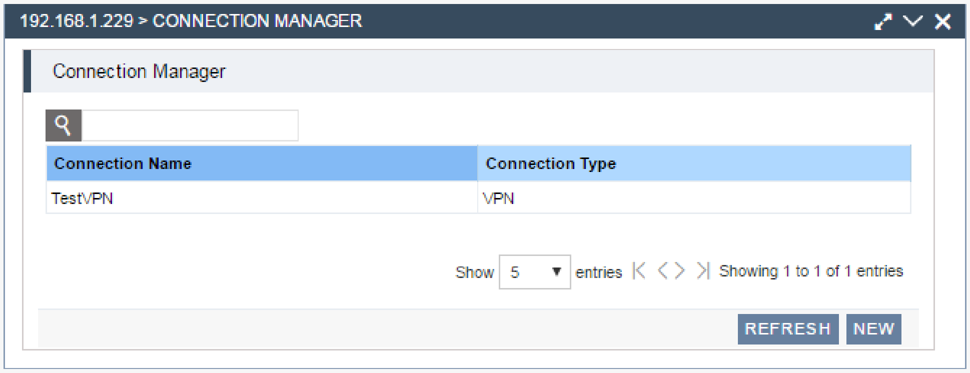
7. **WIFI connection settings applied successfully** message displayed.
8. Click on **CLOSE** button to close connection form

Configuring Connection Manager

User able to **Add and View** Email, Exchange and VPN connections.

Viewing the List of VPN connections

1. Click on **System Settings** then click on **Network Settings** & then click on **Connection Manager.**
2. Connection Manager module displays the list of connections made by user.
3. User able to refresh the table content by click on **REFRESH** button.



192.168.1.229 > CONNECTION MANAGER

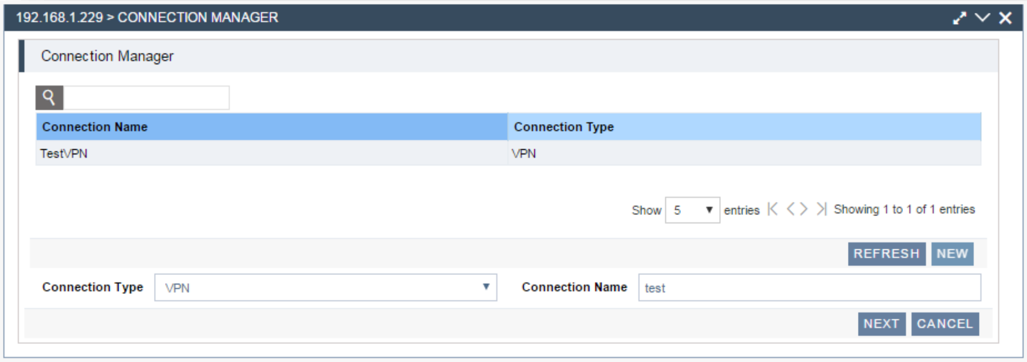
Connection Manager

Connection Name	Connection Type
TestVPN	VPN

Show 5 entries Showing 1 to 1 of 1 entries

Adding a VPN connection

2. Click on **System Settings** then click on **Network Settings** & then click on **Connection Manager.**
3. Click on **New** button to create a new connection.
4. By default, connection name Email is selected. Select **VPN** connection.
5. Enter **Connection Name**, click on **Next** button to open new connection form.



192.168.1.229 > CONNECTION MANAGER

Connection Manager

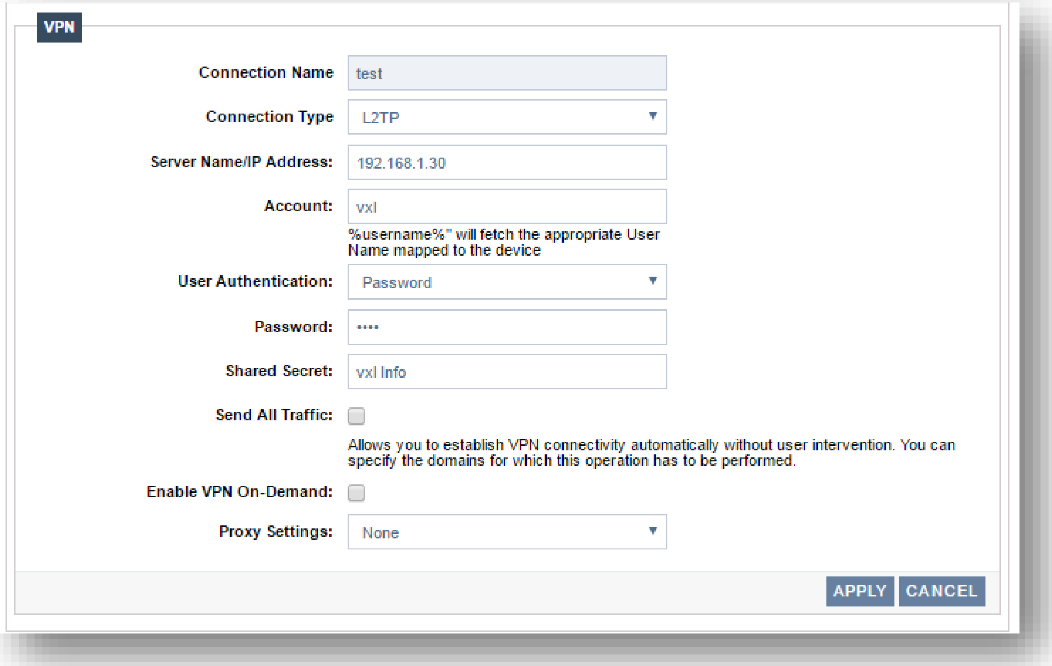
Connection Name	Connection Type
TestVPN	VPN

Show 5 entries Showing 1 to 1 of 1 entries

Connection Type: VPN
Connection Name: test

6. User able to enter all mandatory data.

7. Select checkboxes as per instructions given.



Connection Name: test

Connection Type: L2TP

Server Name/IP Address: 192.168.1.30

Account: vxl

%username%" will fetch the appropriate User Name mapped to the device

User Authentication: Password

Password: ••••

Shared Secret: vxl Info

Send All Traffic: □

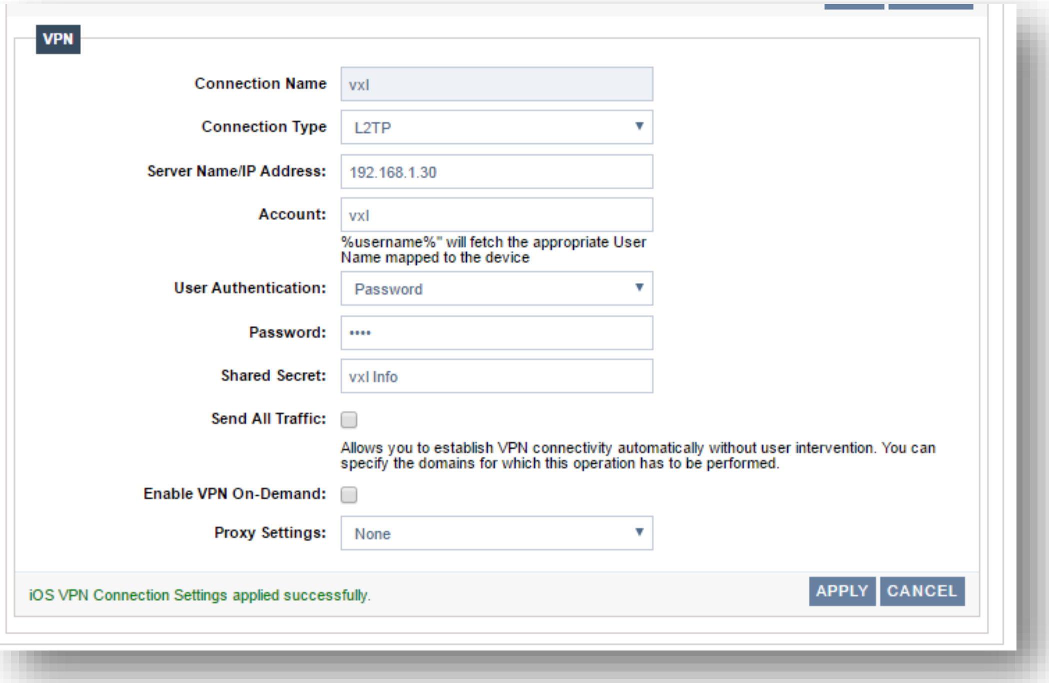
Allows you to establish VPN connectivity automatically without user intervention. You can specify the domains for which this operation has to be performed.

Enable VPN On-Demand: □

Proxy Settings: None

8. Click on **APPLY** button to create connection.

9. **iOS VPN connection Settings applied successfully** message displayed.



Connection Name: vxl

Connection Type: L2TP

Server Name/IP Address: 192.168.1.30

Account: vxl

%username%" will fetch the appropriate User Name mapped to the device

User Authentication: Password

Password: ••••

Shared Secret: vxl Info

Send All Traffic: □

Allows you to establish VPN connectivity automatically without user intervention. You can specify the domains for which this operation has to be performed.

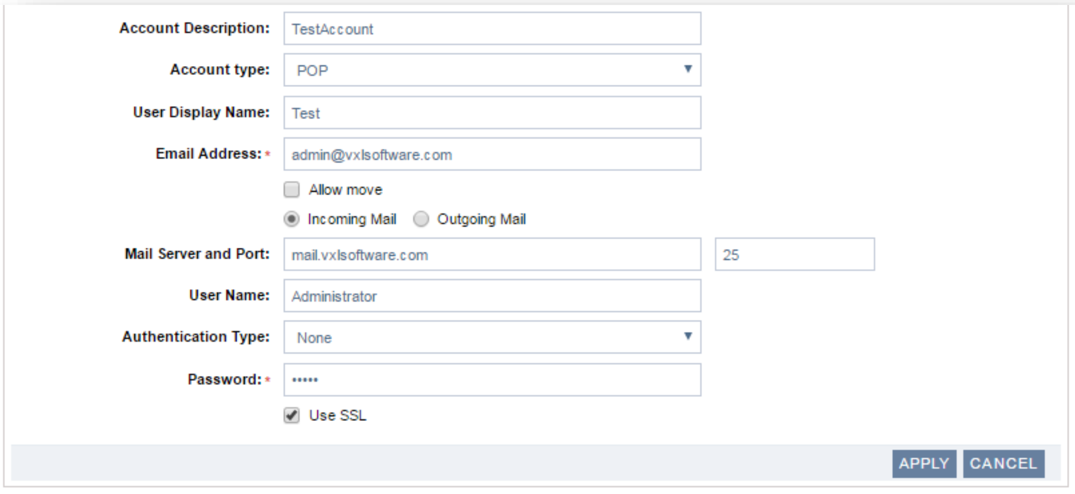
Enable VPN On-Demand: □

Proxy Settings: None

iOS VPN Connection Settings applied successfully.

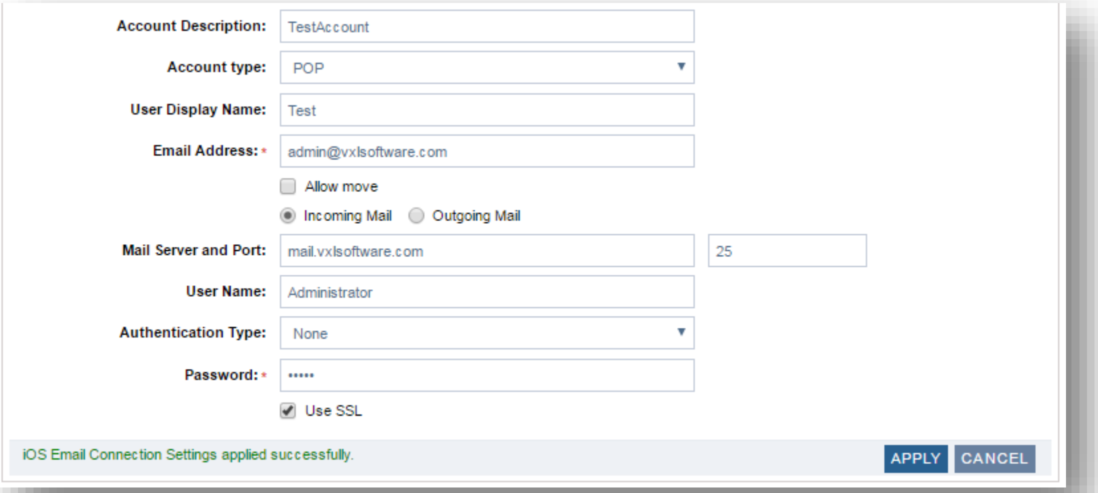
Adding a Email connection

1. Click on **System Settings** -> **Network Settings** -> **Connection Manager.**
2. Click on New button to create a new connection.
3. Choose 'Email' as the Connection Type (This is the default)
4. Enter a connection name and click on the Next button to open a New Connection dialog box.



Account Description:	TestAccount	
Account type:	POP ▾	
User Display Name:	Test	
Email Address:*	admin@vxlsoftware.com	
	☐ Allow move	
	● Incoming Mail ○ Outgoing Mail	
Mail Server and Port:	mail.vxlsoftware.com	25
User Name:	Administrator	
Authentication Type:	None ▾	
Password:*	•••••	
	☑ Use SSL	

5. Fill in all the mandatory data.
6. Click on **Apply** to create a connection.
7. **iOS Email connection Settings applied successfully** message is displayed.



Account Description: TestAccount

Account type: POP

User Display Name: Test

Email Address: * admin@vxlsoftware.com

□ Allow move

● Incoming Mail ○ Outgoing Mail

Mail Server and Port: mail.vxlsoftware.com 25

User Name: Administrator

Authentication Type: None

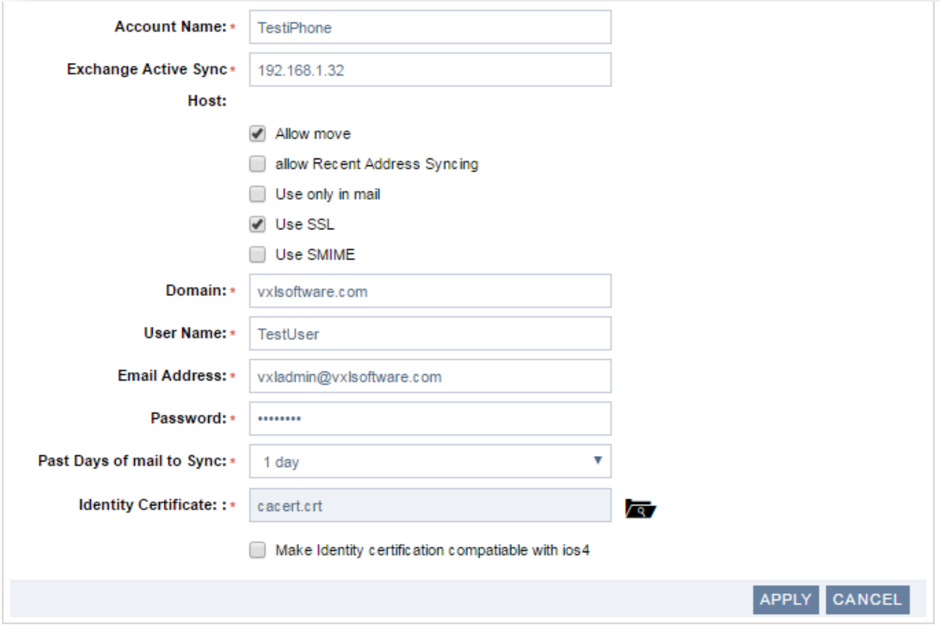
Password: * •••••

☑ Use SSL

iOS Email Connection Settings applied successfully.

Adding an Exchange Connection

1. Click on **System Settings** -> **Network Settings** -> **Connection Manager.**
2. Click on New button to create a new connection.
3. Choose 'Exchange' as the Connection Type.
4. Enter a connection name an click on the Next button to open a new connection dialog box.



Account Name: * TestiPhone

Exchange Active Sync Host: * 192.168.1.32

☑ Allow move

□ allow Recent Address Syncing

□ Use only in mail

☑ Use SSL

□ Use SMIME

Domain: * vxlsoftware.com

User Name: * TestUser

Email Address: * vxladmin@vxlsoftware.com

Password: * ••••••••

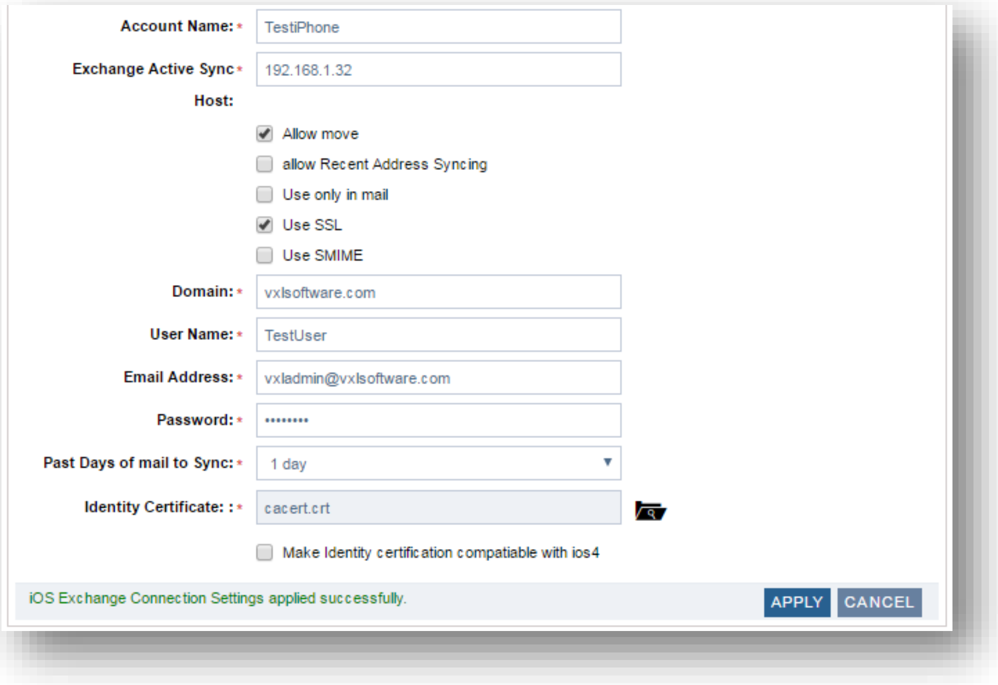
Past Days of mail to Sync: * 1 day

Identity Certificate: : * cacert.crt

□ Make Identity certification compatiable with ios4

5. Fill in all the mandatory data.

6. Click on **Apply** to create a connection.
7. **iOS Exchange Connection added successfully** message is displayed.



Account Name: *	TestiPhone
Exchange Active Sync Host: *	192.168.1.32
	☑ Allow move
	□ allow Recent Address Syncing
	□ Use only in mail
	☑ Use SSL
	□ Use SMIME
Domain: *	vxlsoftware.com
User Name: *	TestUser
Email Address: *	vxladmin@vxlsoftware.com
Password: *	••••••••
Past Days of mail to Sync: *	1 day
Identity Certificate: : *	cacert.crt
	□ Make Identity certification compatiable with ios4

iOS Exchange Connection Settings applied successfully.

Working with Security Settings

Configuring Password Policy Settings

You can change security settings for a group of devices or a single device.

You can configure the password policy for a remotely connected device.

The following password type can be set from the server:

- **Numeric**: PIN/ Password

  The user must have entered a password containing at least numeric characters.
- **Alphabetic**: Password

  The user must have entered a password containing at least alphabetic characters.
- **Alphanumeric**: Password

  The user must have entered a password containing at least both numeric and alphabetic characters.
- **Complex**: Password

  The user must have entered a password containing at least a letter, a numerical digit and a special symbol.
- **Unspecified**: None/Swipe/Pin/Pattern/Password

  The policy has no requirements for the password.

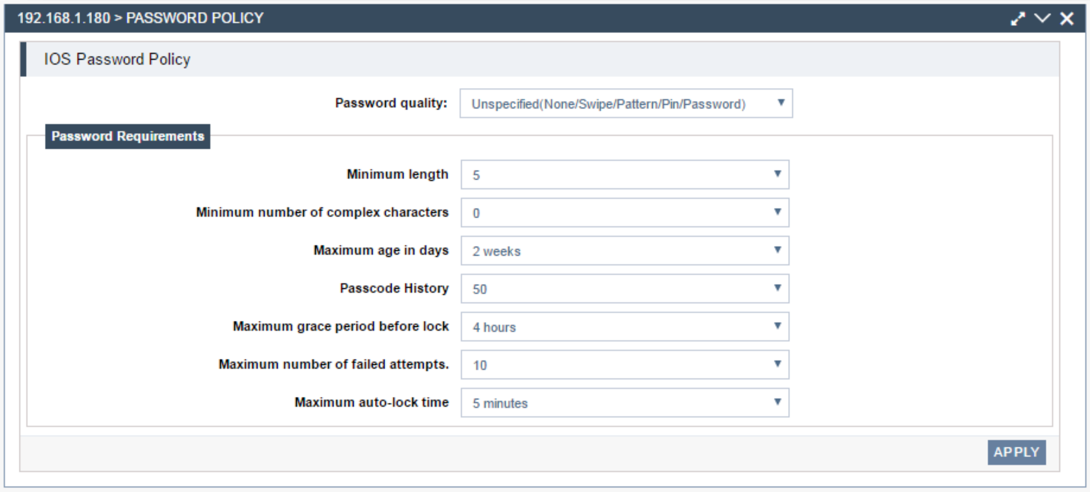
- **Something:** Pin/Password/Pattern

  The policy requires some kind of password or pattern, but doesn't care what it is.
- **Numeric (Complex)**: Pin/Password

  The user must enter a password containing at least numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.

To configure Password settings

1. In the devices tree, click the required device.
2. Expand the right menu. Click **Security Settings**, and then click **Password Policy**.
3. Select the required **Password quality**.


192.168.1.180 > PASSWORD POLICY

IOS Password Policy

Password quality: Unspecified(None/Swipe/Pattern/Pin/Password)

Password Requirements

Minimum length: 5

Minimum number of complex characters: 0

Maximum age in days: 2 weeks

Passcode History: 50

Maximum grace period before lock: 4 hours

Maximum number of failed attempts.: 10

Maximum auto-lock time: 5 minutes

2. The following fields are displayed for each password type:

- Maximum inactive time to lock device
- Password history length
- Maximum failed password attempts for wipe
- Password expiration timeout
- Minimum password length

For Alphabetic password type, following extra fields are displayed:

- Minimum lower case letters
- Minimum upper case letter

For Alphanumeric password type, following extra fields are displayed:

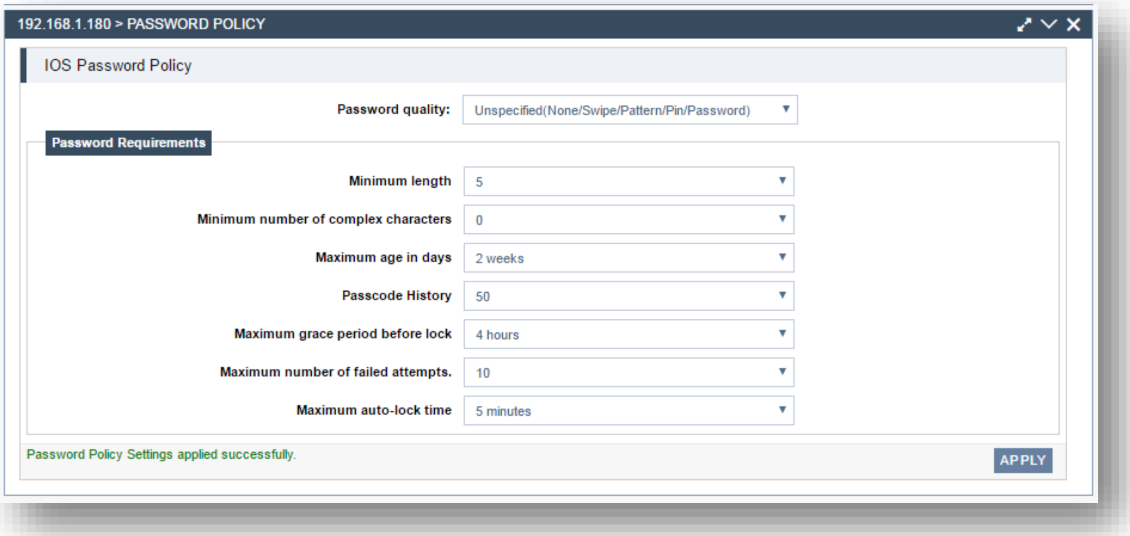
- Minimum letters
- Minimum lower case letters
- Minimum upper case letter
- Minimum non-letters characters
- Minimum numeric digits

For Complex, Unspecified, Something, Numeric (Complex) password type, following extra fields are displayed:

- Minimum letters
- Minimum lower case letters
- Minimum upper case letter
- Minimum non-letters characters
- Minimum numeric digits
- Minimum symbols required

3. In **Password Minimum Letter**, enter the minimum number of letters a password must contain.
4. In **Password Minimum Lower Case**, enter the minimum number of lower case letters a password must contain.
5. In **Password Minimum Upper Case**, enter the minimum number of upper case letters a password must contain.
6. In **Password Minimum Non Letter,** enter the minimum number of non-letters password must contain.
7. In **Password Minimum Numeric**, enter the minimum number of digits a password must contain.
8. In **Password Expiration Timeout,** enter the number of days to expire the user's password.
9. In **Password Minimum Symbols,** enter the minimum number of symbols a password must contain.
10. In **Password History Length,** enter the number of new passwords the user needs to use before using an old password.
11. In **Maximum Failed Password for Wipe** enter the maximum number of times an incorrect password can be entered before the device is locked or its data is wiped out.
12. Click **Apply**.

The **Password Policy Settings applied successfully** message is display.



Password quality: Unspecified(None/Swipe/Pattern/Pin/Password)

Minimum length: 5

Minimum number of complex characters: 0

Maximum age in days: 2 weeks

Passcode History: 50

Maximum grace period before lock: 4 hours

Maximum number of failed attempts.: 10

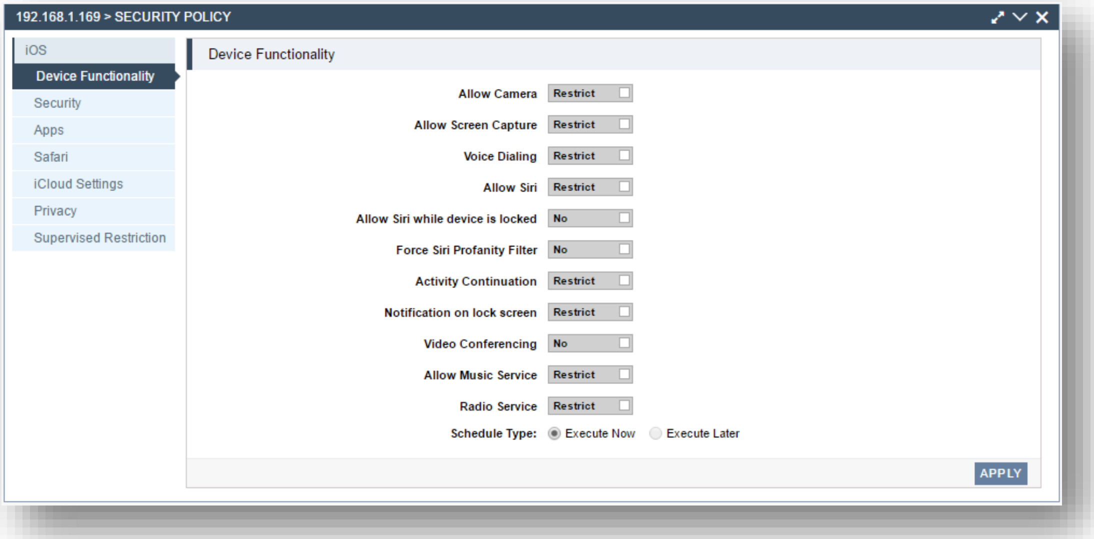
Maximum auto-lock time: 5 minutes

Password Policy Settings applied successfully.

Configuring Security Policy Settings

You can set various security policies to a remote device on the network.

User able to Allow or Restrict security policies.



Allow Camera: Restrict □

Allow Screen Capture: Restrict □

Voice Dialing: Restrict □

Allow Siri: Restrict □

Allow Siri while device is locked: No □

Force Siri Profanity Filter: No □

Activity Continuation: Restrict □

Notification on lock screen: Restrict □

Video Conferencing: No □

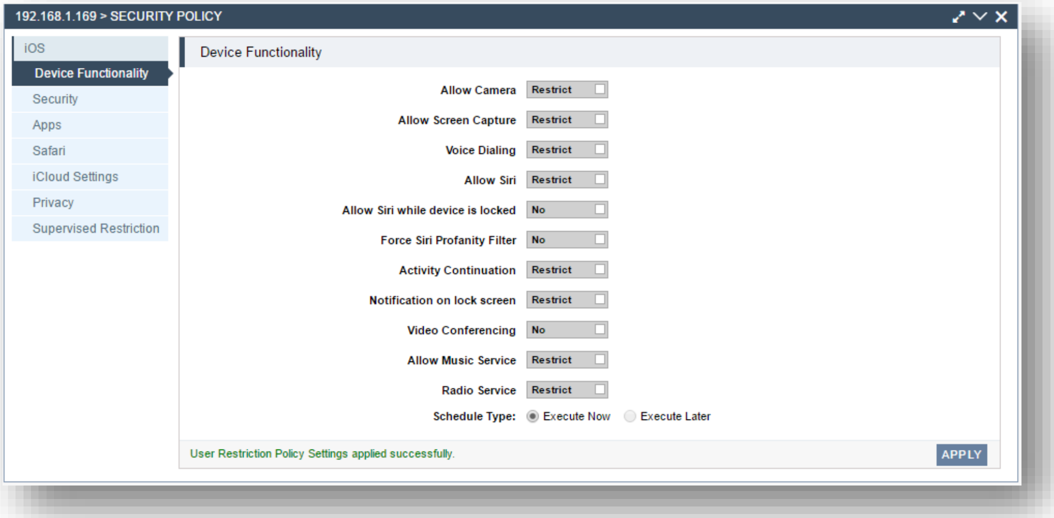
Allow Music Service: Restrict □

Radio Service: Restrict □

Schedule Type: ● Execute Now ○ Execute Later

Configuring Device Functionality

User able to Allow or Restrict Device security policies (like enable/Disable camera).



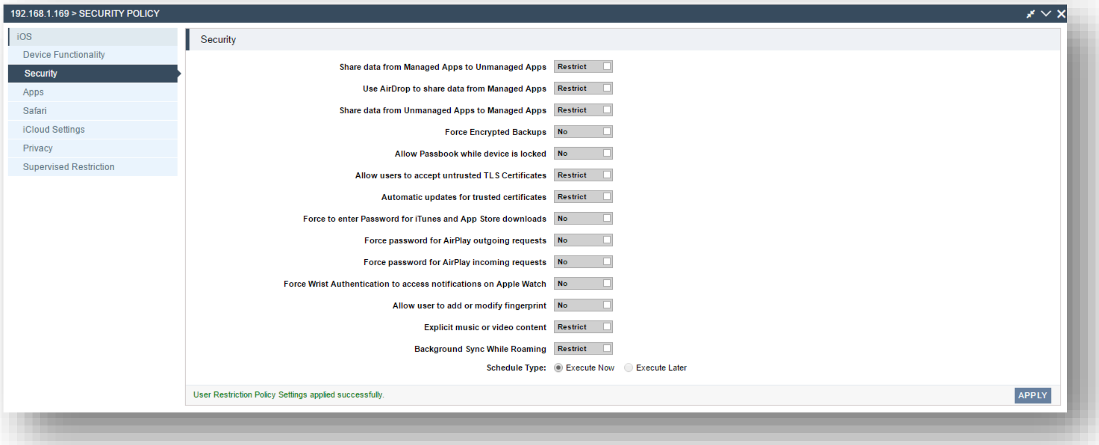
Device Functionality

Allow Camera	Restrict □
Allow Screen Capture	Restrict □
Voice Dialing	Restrict □
Allow Siri	Restrict □
Allow Siri while device is locked	No □
Force Siri Profanity Filter	No □
Activity Continuation	Restrict □
Notification on lock screen	Restrict □
Video Conferencing	No □
Allow Music Service	Restrict □
Radio Service	Restrict □
Schedule Type:	● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Security

User able to Allow or Restrict security policies related to applications.



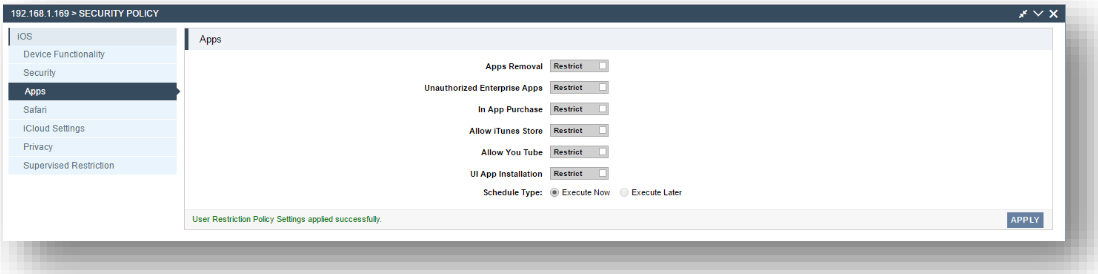
Security

Share data from Managed Apps to Unmanaged Apps	Restrict □
Use AirDrop to share data from Managed Apps	Restrict □
Share data from Unmanaged Apps to Managed Apps	Restrict □
Force Encrypted Backups	No □
Allow Passbook while device is locked	No □
Allow users to accept untrusted TLS Certificates	Restrict □
Automatic updates for trusted certificates	Restrict □
Force to enter Password for iTunes and App Store downloads	No □
Force password for AirPlay outgoing requests	No □
Force password for AirPlay incoming requests	No □
Force Wrist Authentication to access notifications on Apple Watch	No □
Allow user to add or modify fingerprint	No □
Explicit music or video content	Restrict □
Background Sync While Roaming	Restrict □
Schedule Type:	● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Apps

To Restrict or Allow the policies related to application.



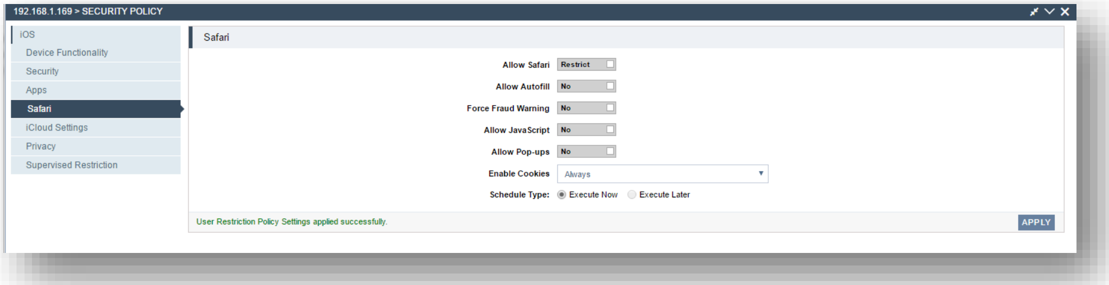
Apps

Apps Removal: Restrict □
Unauthorized Enterprise Apps: Restrict □
In App Purchase: Restrict □
Allow iTunes Store: Restrict □
Allow You Tube: Restrict □
UI App Installation: Restrict □
Schedule Type: ● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Safari

To Restrict/Allow the Safari browser.



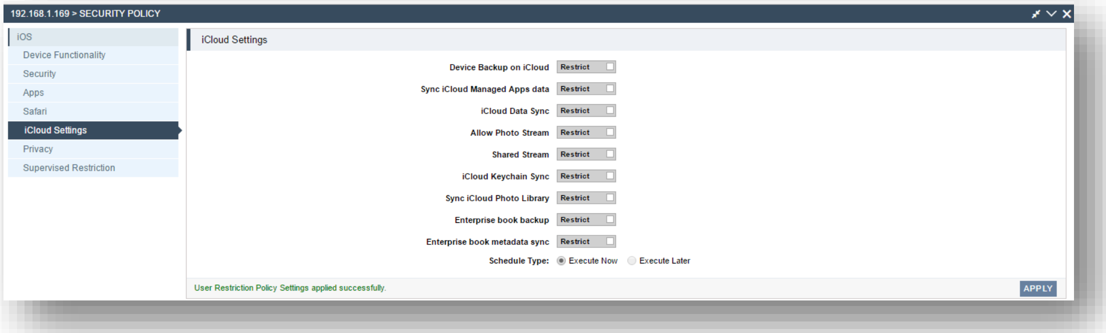
Safari

Allow Safari: Restrict □
Allow Autofill: No □
Force Fraud Warning: No □
Allow JavaScript: No □
Allow Pop-ups: No □
Enable Cookies: Always
Schedule Type: ● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring iCloud Settings

To restrict or Allow iCloud settings.



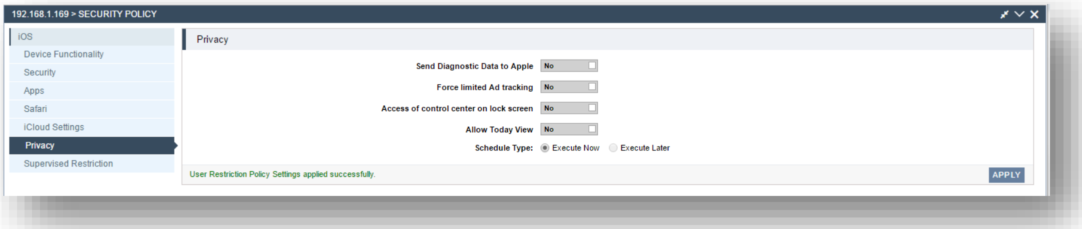
iCloud Settings

Device Backup on iCloud: Restrict □
Sync iCloud Managed Apps data: Restrict □
iCloud Data Sync: Restrict □
Allow Photo Stream: Restrict □
Shared Stream: Restrict □
iCloud Keychain Sync: Restrict □
Sync iCloud Photo Library: Restrict □
Enterprise book backup: Restrict □
Enterprise book metadata sync: Restrict □
Schedule Type: ● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Privacy

To restrict /Allow the privacy settings.



Privacy

Send Diagnostic Data to Apple: No

Force limited Ad tracking: No

Access of control center on lock screen: No

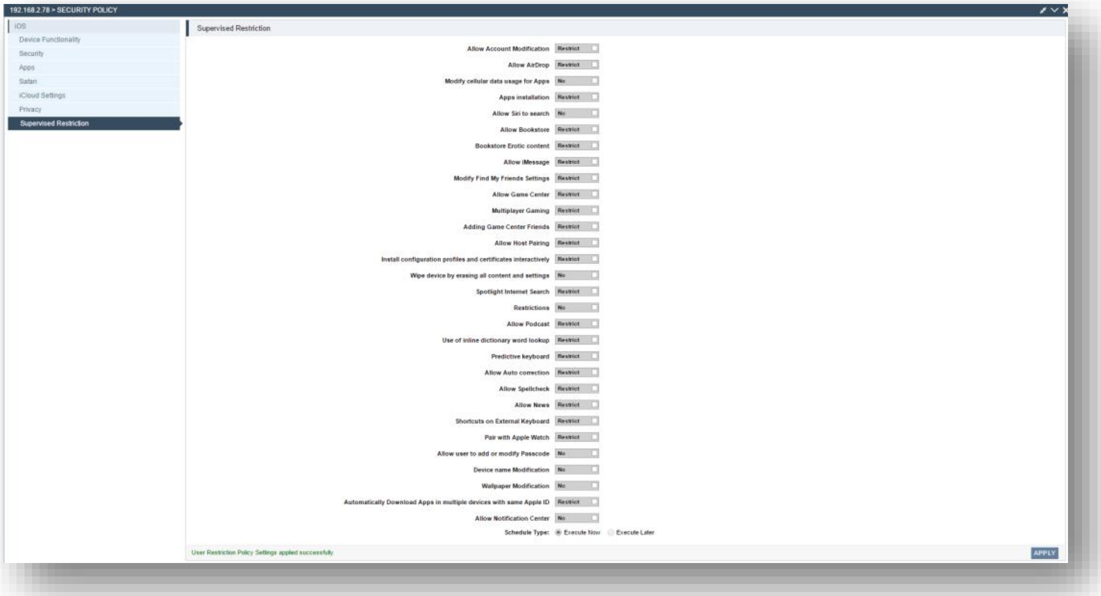
Allow Today View: No

Schedule Type: ● Execute Now ○ Execute Later

User Restriction Policy Settings applied successfully.

Configuring Supervised Devices Only

To restrict/Allow the security policies for supervised device.



Supervised Restriction

Allow Account Modification: Restrict

Allow AirDrop: Restrict

Modify cellular data usage for Apps: No

Apps installation: Restrict

Allow Siri to search: No

Allow Bookstore: Restrict

Bookstore Erotic content: Restrict

Allow iMessage: Restrict

Modify Find My Friends Settings: Restrict

Allow Game Center: Restrict

Multiplayer Gaming: Restrict

Adding Game Center Friends: Restrict

Allow Host Pairing: Restrict

Install configuration profiles and certificates interactively: Restrict

Wipe device by erasing all content and settings: No

Spotlight Internet Search: Restrict

Restrictions: No

Allow Podcast: Restrict

Use of inline dictionary word lookup: Restrict

Predictive keyboard: Restrict

Allow Auto correction: Restrict

Allow Spellcheck: Restrict

Allow News: Restrict

Shortcuts on External Keyboard: Restrict

Pair with Apple Watch: Restrict

Allow user to add or modify Passcode: No

Device name Modification: No

Wallpaper Modification: No

Automatically Download Apps in multiple devices with same Apple ID: Restrict

Allow Notification Center: No

Schedule Type: ● Execute Now ○ Execute Later

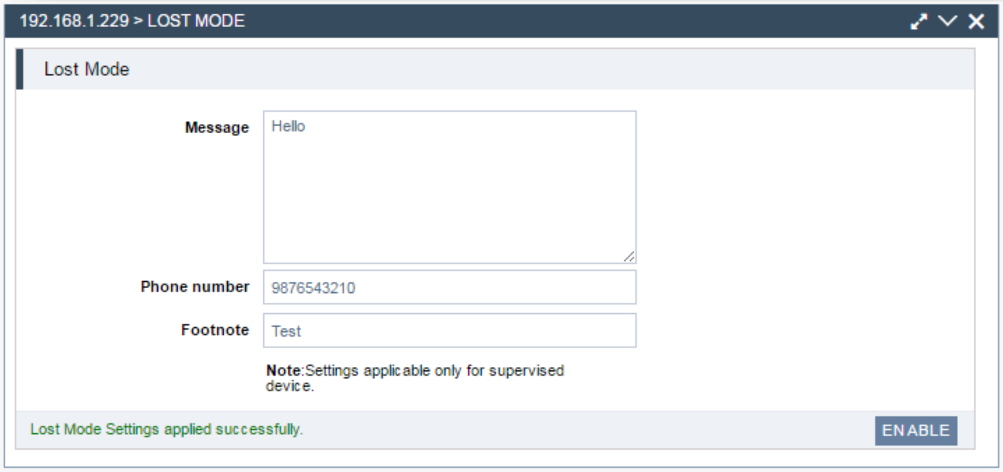
User Restriction Policy Settings applied successfully

Configuring Lost Mode Settings

Lost Mode feature is used to lock an iOS device instantly and keep track of its location. Lost Mode locks the device with a passcode thereby denying access to the personal information.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Security Settings**
3. Select **Lost Mode.**
4. Enter a message to be displayed on the device in the **Message** textbox.
5. Enter the phone number of the lost device in **Phone number** textbox.
6. Enter a footnote in the **Footnote textbox**.
7. Click on the **ENABLE** button.

'Lost Mode Settings applied successfully' summary message is displayed.



Message: Hello

Phone number: 9876543210

Footnote: Test

Note:Settings applicable only for supervised device.

Lost Mode Settings applied successfully.

8. Disable button is displayed only after the task is successful and sync gets applied.

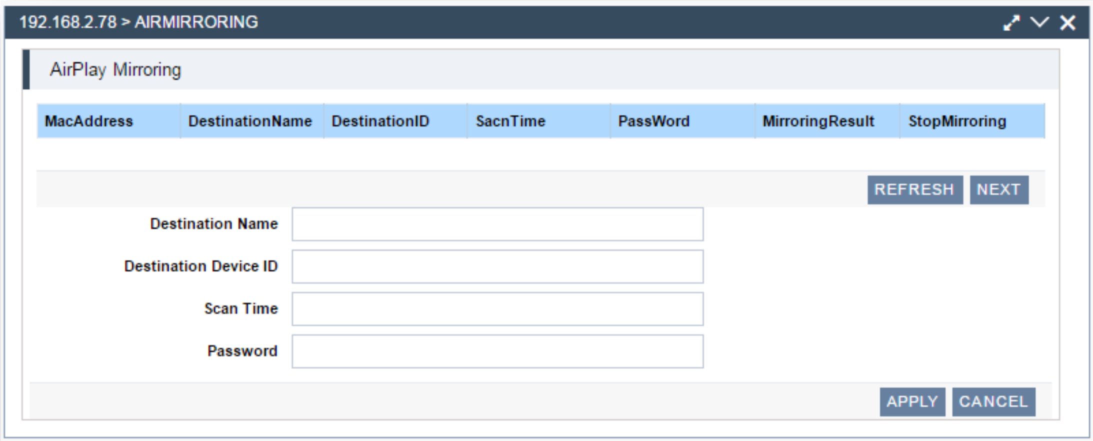
The settings will only be applied on supervised devices.

Configuring AirMirroring Settings

Mirror the screen of iPhone, iPad or iPod touch on any Apple TV using this feature.

On your **iOS** device, swipe up from the bottom of your screen to open Control Center. In Control Center, tap **Air Mirroring**, then select your Apple TV from the list.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Security Settings**
3. Select **AirMirroring.**
4. Click on the **NEXT** button to add new device details.



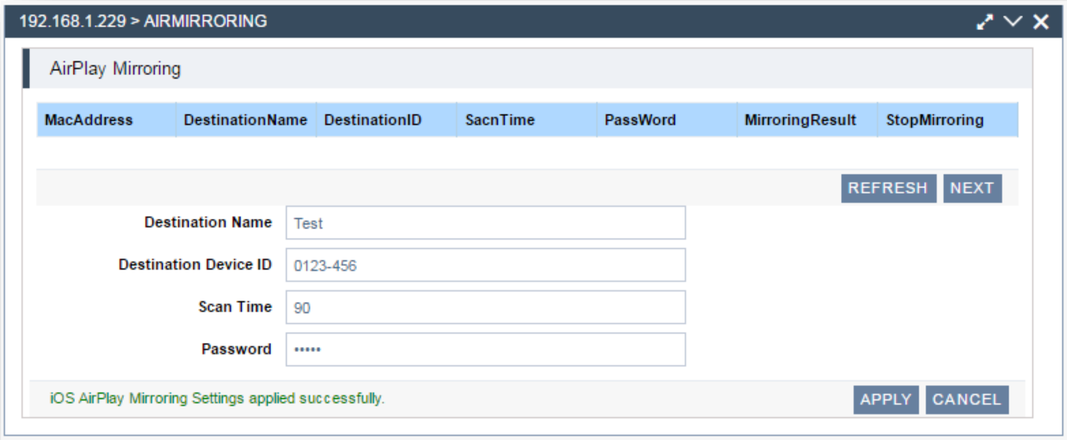
AirPlay Mirroring

MacAddress	DestinationName	DestinationID	SacnTime	PassWord	MirroringResult	StopMirroring

Destination Name	
Destination Device ID	
Scan Time	
Password	

5. Enter the name of the destination device in **Destination Name** textbox.
6. Enter the device ID of the destination device in the **Destination Device ID** textbox.
7. Enter the scan time in the **Scan Time** textbox.
8. Enter the password in the **Password** textbox.
9. Click on the **Apply** button.

   'iOS Airplay Mirroring Settings applied successfully' summary message is displayed.



AirPlay Mirroring

MacAddress	DestinationName	DestinationID	SacnTime	PassWord	MirroringResult	StopMirroring

Destination Name	Test
Destination Device ID	0123-456
Scan Time	90
Password	•••••

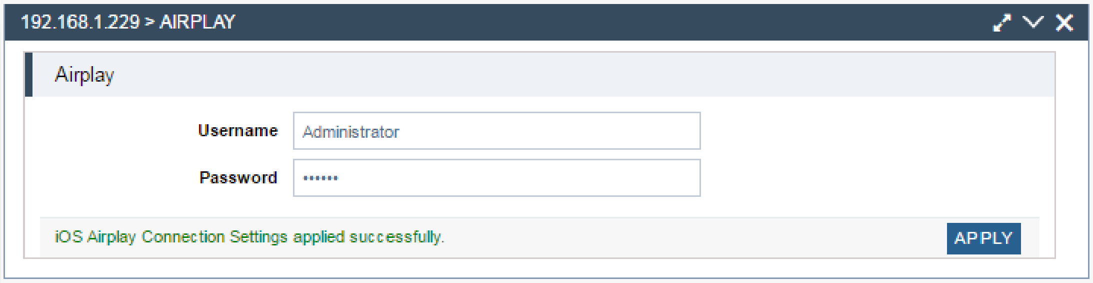
iOS AirPlay Mirroring Settings applied successfully.

Configuring AirPlay Settings

AirPlay allows to connect AirPlay-compatible devices together, allowing you to wirelessly stream music amongst other things. AirPlay even allows mirroring your entire display on the TV with minimal delay. Airplay works over a WiFi connection.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Security Settings**
3. Select **AirPlay.**
4. Enter a valid **Username** and **Password** in the respective text boxes.
5. Click on the **Apply** button.

   ‘**iOS Airplay Connection Settings applied successfully’** summary message is displayed.



192.168.1.229 > AIRPLAY

Airplay

Username: Administrator

Password: ••••••

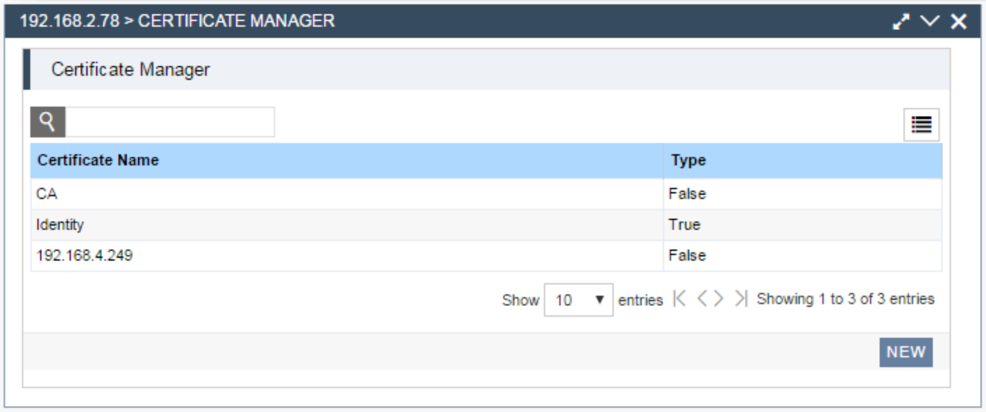
iOS Airplay Connection Settings applied successfully.

Working with Administration Settings

Configuring Certificate Manager Settings

User can view the list of certificates available or can upload a new certificate on an iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Administration.**
3. Select **Certificate Manager.**
4. The list of certificates present on the device will be displayed.



192.168.2.78 > CERTIFICATE MANAGER

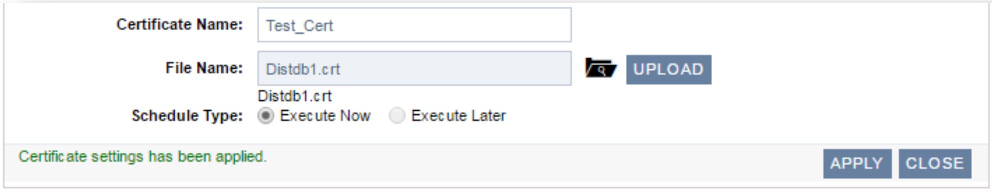
Certificate Manager

Certificate Name	Type
CA	False
Identity	True
192.168.4.249	False

Show 10 entries Showing 1 to 3 of 3 entries

5. Click on NEW button to upload a new certificate.
6. Enter the certificate name in the **Certificate Name** textbox.
7. Click the 📂 icon to browse the certificate file.
8. Click on the **Upload** button to upload the selected certificate file.
9. Click on the **APPLY** button

   'Certificate Settings has been applied' summary message is displayed.



Certificate Name: Test_Cert

File Name: Distdb1.crt

Distdb1.crt

Schedule Type: ● Execute Now ○ Execute Later

Certificate settings has been applied.

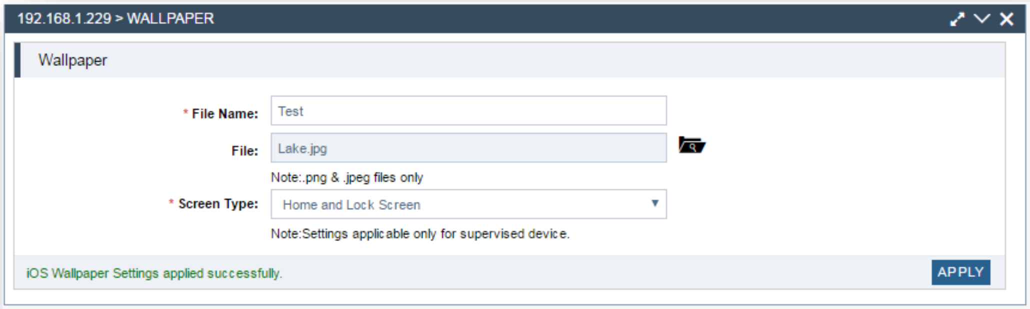
Configuring Wallpaper Settings

You can set wallpaper to a remote iOS device on the network.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click iOS device, then click **Administration Settings**
4. Select **Wallpaper Settings**
5. In **File Name** textbox, enter the File name.
6. In **File**, browse the wallpaper image.
7. Select **Screen Type** from dropdown list.

8. Click on **APPLY** button

   The Settings applied summary message displayed.



192.168.1.229 > WALLPAPER

Wallpaper

* File Name: Test

File: Lake.jpg

Note:.png & .jpeg files only

* Screen Type: Home and Lock Screen

Note:Settings applicable only for supervised device.

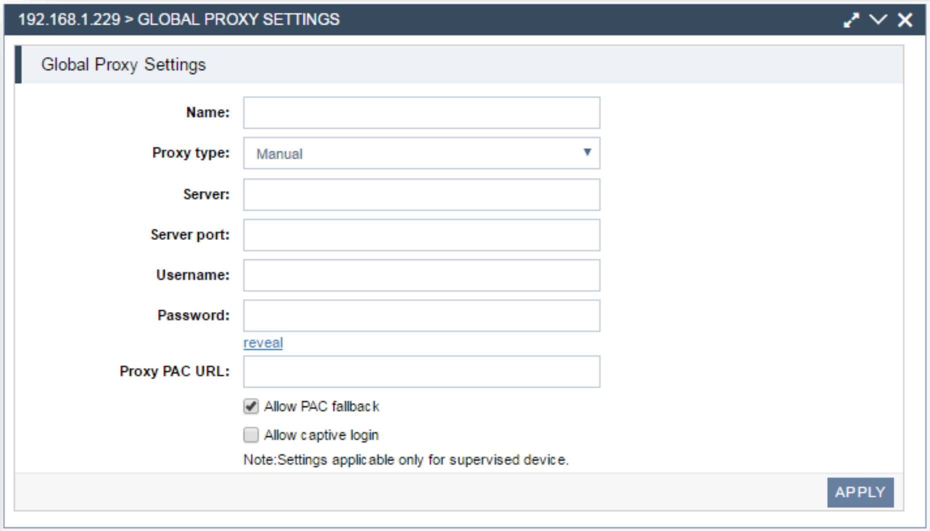
iOS Wallpaper Settings applied successfully.

The settings will only be applied on supervised devices.

Configuring Global Proxy Settings

Global HTTP **proxy** is a feature that can only be applied to **iOS** Supervised devices. By imposing this profile on the user's mobile devices, you can ensure that the internet connectivity is always re-directed through one **proxy**.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click iOS device, then click **Administration Settings**
4. Select **Global Proxy Settings.**



192.168.1.229 > GLOBAL PROXY SETTINGS

Global Proxy Settings

Name:

Proxy type: Manual

Server:

Server port:

Username:

Password:

reveal

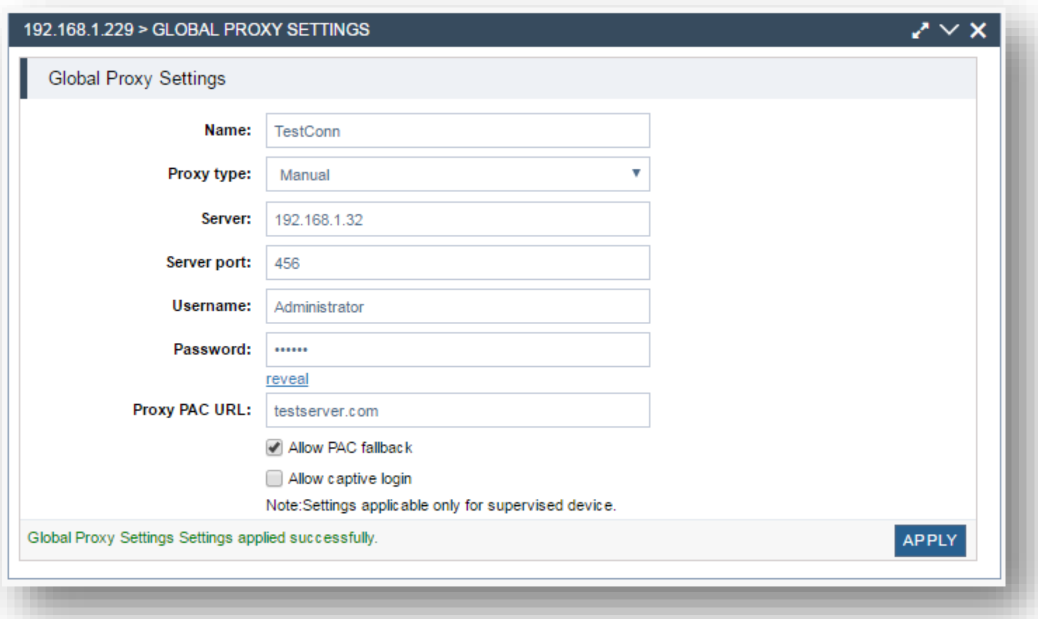
Proxy PAC URL:

☑ Allow PAC fallback

□ Allow captive login

Note:Settings applicable only for supervised device.

5. In **Name** textbox, enter name of Global Proxy settings.
6. Select **Proxy type** from drop-down list.
7. Enter Server name in **Sever** textbox.
8. In **Server Port**, enter port number of server.
9. Enter Username and password
10. After selecting reveal label, it shows the actual entered password and on selecting hide, it shows the password in encrypted format.
11. In **Proxy PAC URL**, Enter the URL link for proxy PAC.
12. Click on Apply button.



192.168.1.229 > GLOBAL PROXY SETTINGS

Global Proxy Settings

Name:	TestConn
Proxy type:	Manual
Server:	192.168.1.32
Server port:	456
Username:	Administrator
Password:	••••••
Proxy PAC URL:	testserver.com

☑ Allow PAC fallback

☐ Allow captive login

Note:Settings applicable only for supervised device.

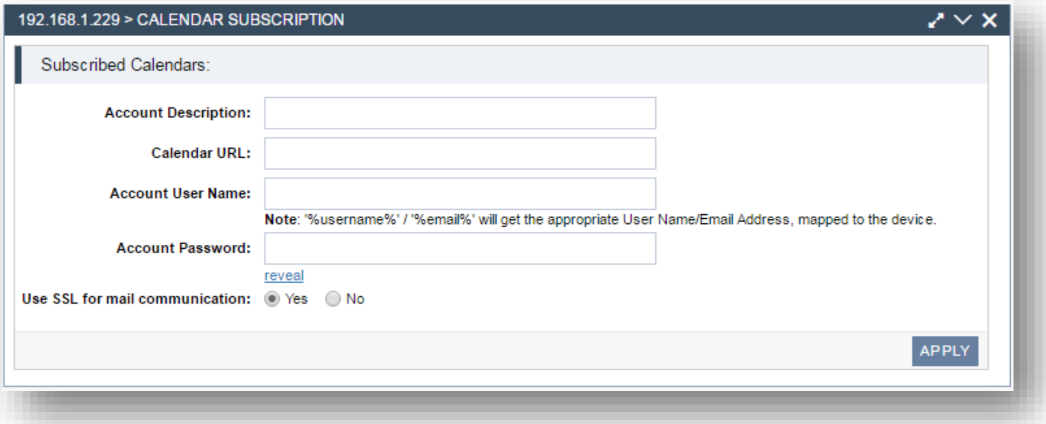
Global Proxy Settings Settings applied successfully.

The settings will only be applied on supervised devices.

Configuring Calendar Subscription Settings

Calendar subscriptions are a great way to stay up to date with holidays, sports, social media, and more. And with iCloud, you see all the calendar subscriptions across all devices.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Administration**
3. Select **Calendar Subscription.**



192.168.1.229 > CALENDAR SUBSCRIPTION

Subscribed Calendars:

Account Description:

Calendar URL:

Account User Name:

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

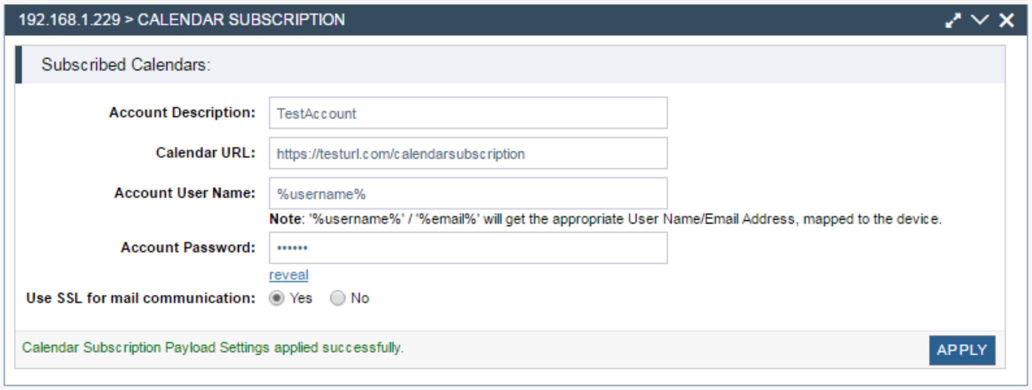
Account Password:

reveal

Use SSL for mail communication: ● Yes ○ No

4. Enter a description In the **Account Description** textbox.
5. Enter a valid calendar URL in the **Calendar URL** textbox.
6. Enter a valid Username and Password in respective text boxes.
7. Click on '**reveal**' to view the password.
8. Choose the desired option for '**Use SSL for mail communication**'
9. Click on the **Apply** button.

   '**Calendar Subscription Settings applied successfully'** summary message is displayed.



192.168.1.229 > CALENDAR SUBSCRIPTION

Subscribed Calendars:

Account Description: TestAccount

Calendar URL: https://testurl.com/calendarsubscription

Account User Name: %username%

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

Account Password: ••••••

reveal

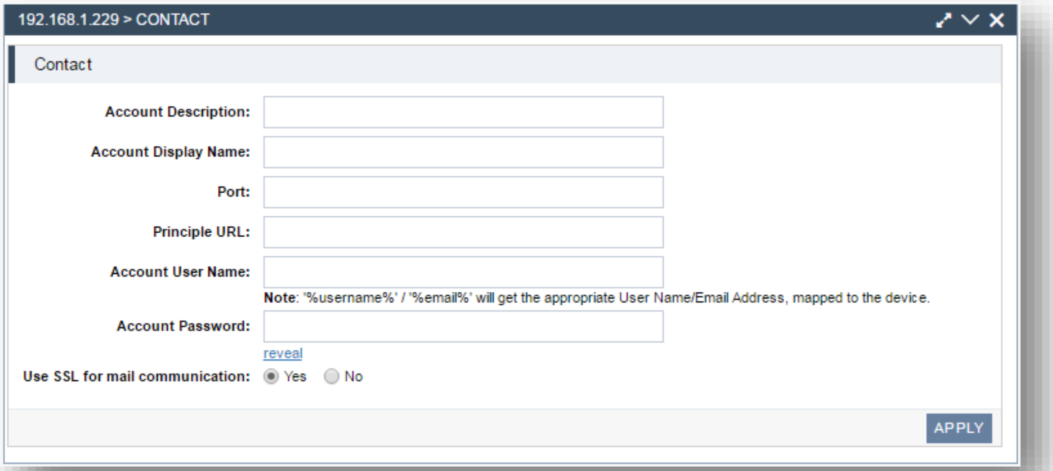
Use SSL for mail communication: ● Yes ○ No

Calendar Subscription Payload Settings applied successfully.

Configuring Contact Settings

Contact profile can be created on device using the feature.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Administration.**
3. Select **Contact.**



192.168.1.229 > CONTACT

Contact

Account Description:

Account Display Name:

Port:

Principle URL:

Account User Name:

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

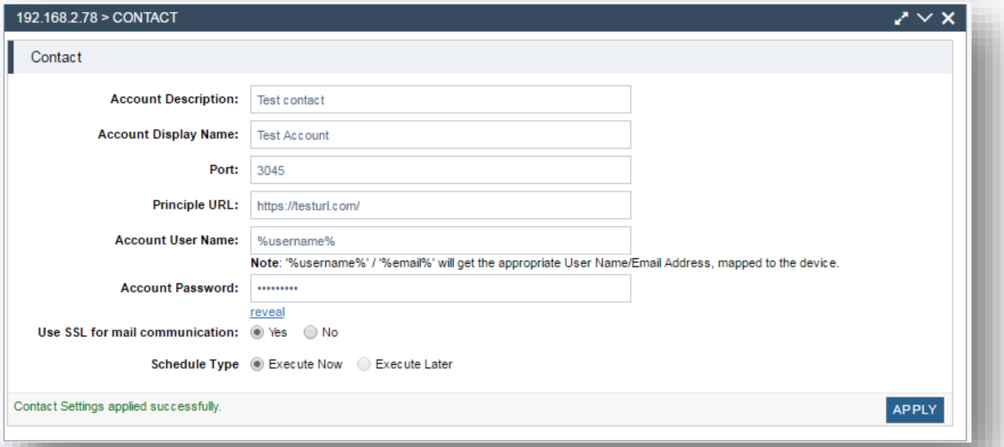
Account Password:

reveal

Use SSL for mail communication: ● Yes ○ No

4. Enter a description in the **Account Description** textbox.
5. Enter a display name in the **Account Display Name** textbox.
6. Enter the port number in **Port** textbox.
7. Enter a valid URL in the **Principle URL** textbox.
8. Enter a valid Username and password in the respective text boxes.
9. Click on '**reveal**' to view the password.
10. Choose the desired option for '**Use SSL for mail communication**'.
11. Click on the **APPLY** button.

    'Contact Settings applied successfully' summary message is displayed.



192.168.2.78 > CONTACT

Contact

Account Description: Test contact

Account Display Name: Test Account

Port: 3045

Principle URL: https://testurl.com/

Account User Name: %username%

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

Account Password: •••••••••

reveal

Use SSL for mail communication: ● Yes ○ No

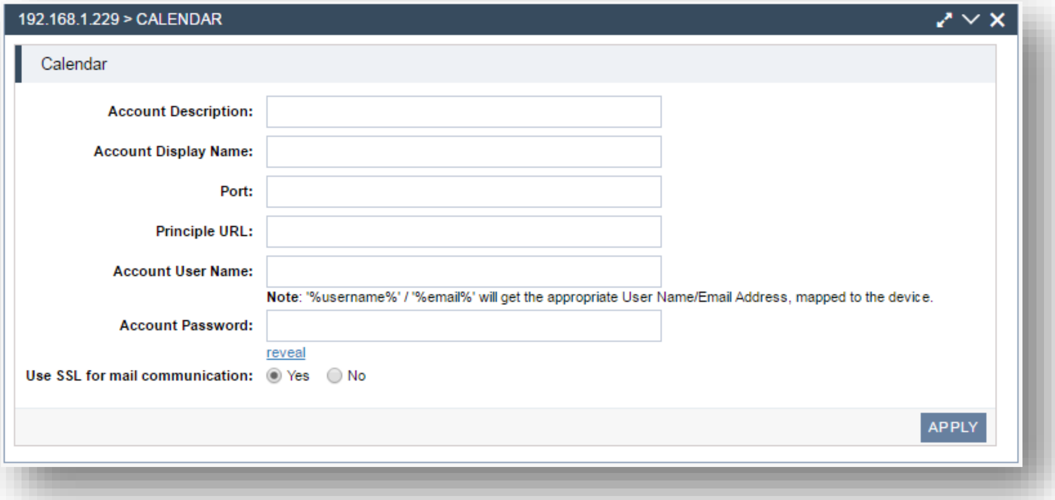
Schedule Type ● Execute Now ○ Execute Later

Contact Settings applied successfully.

Configuring Calendar Settings

Date-time and calendar features can be set from the server to the device using this feature.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Administration.**
3. Select **Calendar.**



192.168.1.229 > CALENDAR

Calendar

Account Description:

Account Display Name:

Port:

Principle URL:

Account User Name:

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

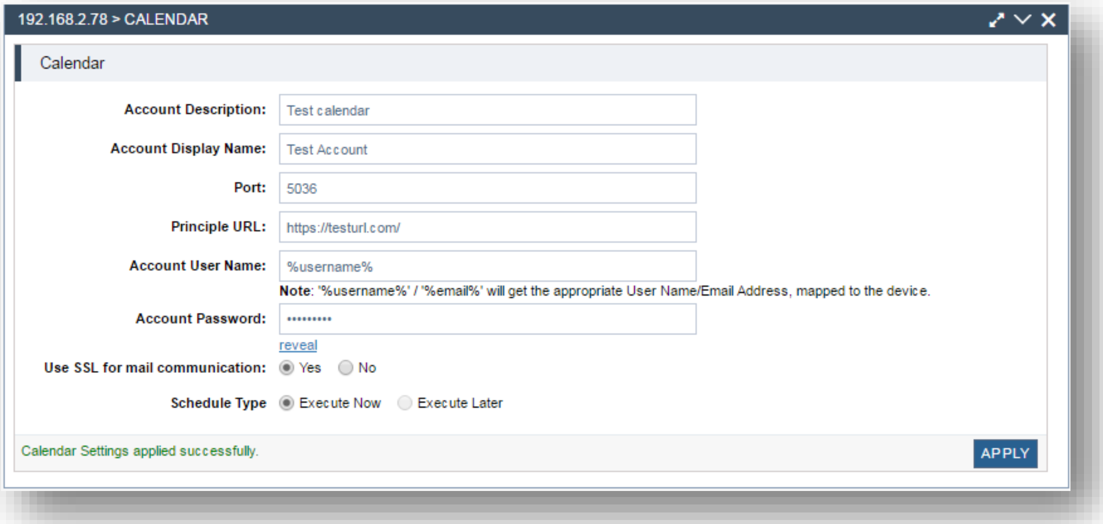
Account Password:

reveal

Use SSL for mail communication: ● Yes ○ No

4. Enter a description in the **Account Description** textbox.
5. Enter a display name in the **Account Display Name** textbox.
6. Enter the port number in **Port** textbox.
7. Enter a valid URL in the **Principle URL** textbox.
8. Enter a valid Username and password in the respective text boxes.
9. Click on '**reveal**' to view the password.
10. Choose the desired option for '**Use SSL for mail communication**'.
11. Click on the **APPLY** button.

    'Calendar Settings applied successfully' summary message is displayed.



192.168.2.78 > CALENDAR

Calendar

Account Description: Test calendar

Account Display Name: Test Account

Port: 5036

Principle URL: https://testurl.com/

Account User Name: %username%

Note: '%username%' / '%email%' will get the appropriate User Name/Email Address, mapped to the device.

Account Password: •••••••••

reveal

Use SSL for mail communication: ● Yes ○ No

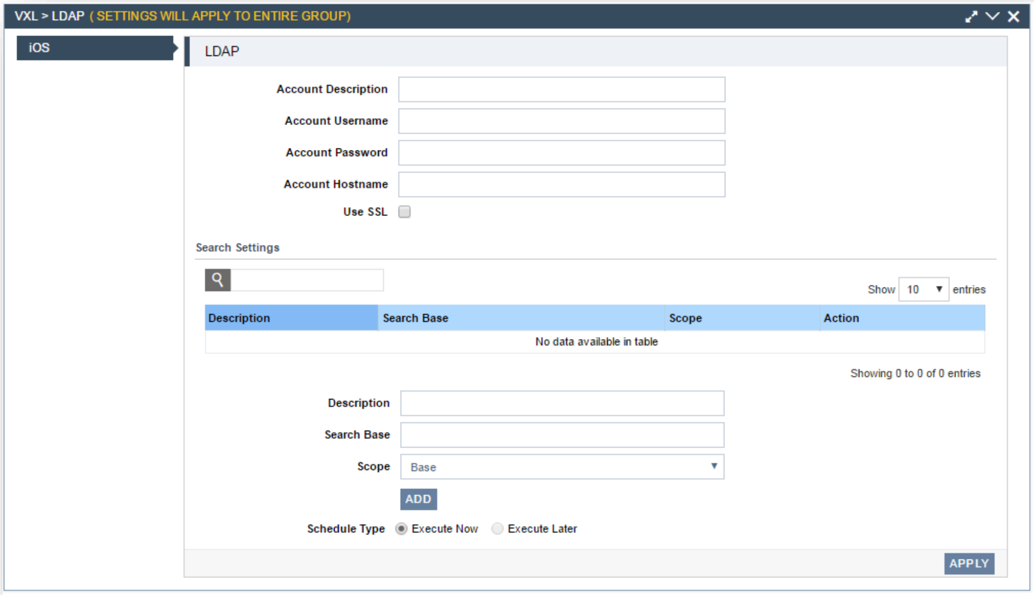
Schedule Type ● Execute Now ○ Execute Later

Calendar Settings applied successfully.

APPLY

Configuring LDAP Settings

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Administration.**
3. Select **LDAP.**



VXL > LDAP (SETTINGS WILL APPLY TO ENTIRE GROUP)

iOS

LDAP

Account Description

Account Username

Account Password

Account Hostname

Use SSL □

Search Settings

Show 10 entries

Description	Search Base	Scope	Action
No data available in table			

Showing 0 to 0 of 0 entries

Description

Search Base

Scope: Base

ADD

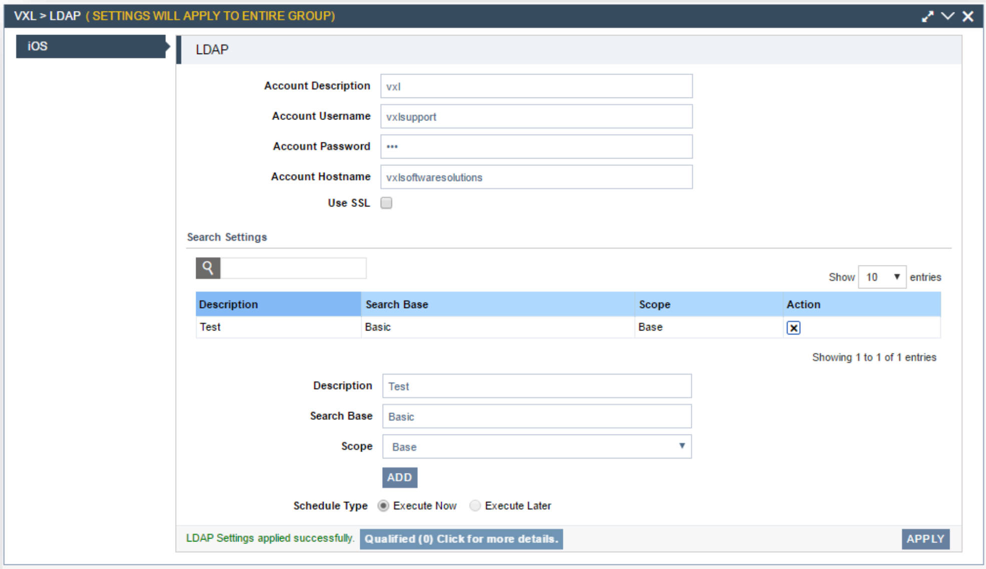
Schedule Type ● Execute Now ○ Execute Later

APPLY

4. Enter a description in the **Account Description** textbox.

5. Enter a valid Username and Password in the respective text boxes.
6. Enter a hostname in the **Account Hostname** textbox.
7. Select the SSL checkbox as required.
8. In the **Search Settings** section, enter the **Description**, **Search Base** & select **Scope** as required.
9. Click on the **ADD** button to add the details.
10. Click on the **APPLY** button.

    'LDAP Settings applied successfully' summary message is displayed.



VXL > LDAP (SETTINGS WILL APPLY TO ENTIRE GROUP)

iOS

LDAP

Account Description: vxl

Account Username: vxlsupport

Account Password: •••

Account Hostname: vxlsoftwaresolutions

Use SSL □

Search Settings

Show 10 entries

Description	Search Base	Scope	Action
Test	Basic	Base	☒

Showing 1 to 1 of 1 entries

Description: Test

Search Base: Basic

Scope: Base

ADD

Schedule Type ● Execute Now ○ Execute Later

LDAP Settings applied successfully. Qualified (0) Click for more details.

APPLY

Working with Software Deployment Settings

Configuring Software & Patch Install/Uninstall Settings

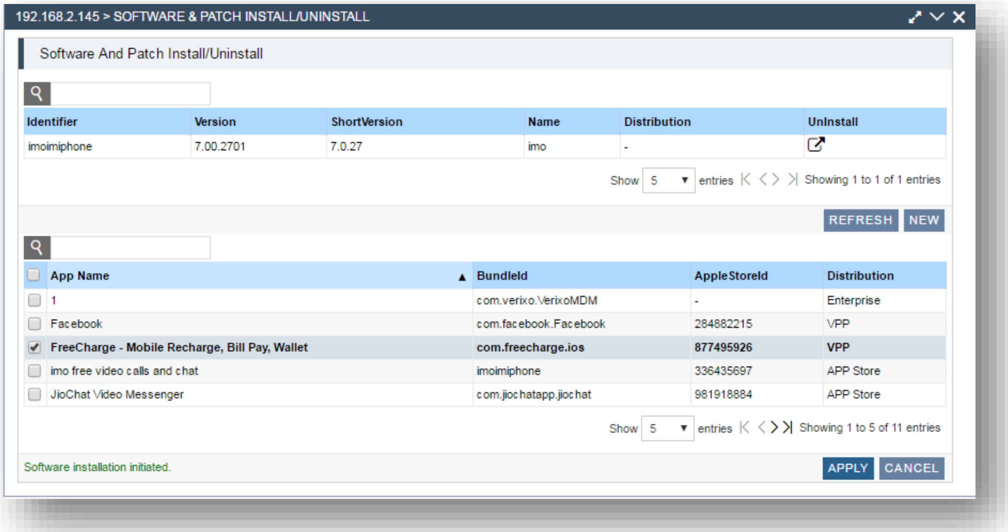
You can remotely check and update software installed on a client device.

You can view, install and uninstall software from a client iOS device.

Installing Software:

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click Software Deployment, then click **Software& Patch Install/Uninstall.**
4. It will show the list of installed applications on the device.
5. Click Refresh to refresh the application list.
6. Click **New** to install a new application. List of all company approved applications will be displayed.
7. Select the applications to be installed on the device.
8. Click on Apply button.

The **Software installation initiated** message is displayed.



192.168.2.145 > SOFTWARE & PATCH INSTALL/UNINSTALL

Software And Patch Install/Uninstall

Identifier	Version	ShortVersion	Name	Distribution	Uninstall
imoimiphone	7.00.2701	7.0.27	imo	-	↗

Show 5 entries Showing 1 to 1 of 1 entries

☐	App Name ▲	BundleId	AppleStoreId	Distribution
☐	1	com.verixo.VerixoMDM	-	Enterprise
☐	Facebook	com.facebook.Facebook	284882215	VPP
☑	FreeCharge - Mobile Recharge, Bill Pay, Wallet	com.freecharge.ios	877495926	VPP
☐	imo free video calls and chat	imoimiphone	336435697	APP Store
☐	JioChat Video Messenger	com.jiochatapp.jiochat	981918884	APP Store

Show 5 entries Showing 1 to 5 of 11 entries

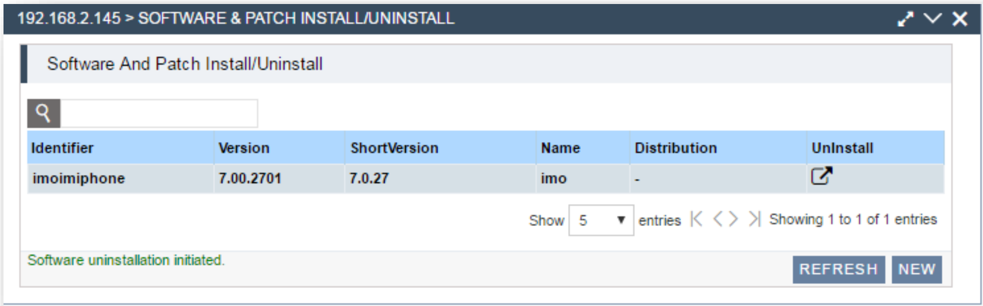
Software installation initiated.

Uninstalling Software:

You can remotely uninstall software from an Android based device.

1. In the devices tree, click the required device.
2. Expand the right menu.
3. Click Software **Deployment, then** click **Software & Patch Install/Uninstall.**
4. In the table, select the software to uninstall.
5. Click the **Uninstall icon**.

   The **Software uninstallation summary** message is display.



192.168.2.145 > SOFTWARE & PATCH INSTALL/UNINSTALL

Software And Patch Install/Uninstall

Identifier	Version	ShortVersion	Name	Distribution	Uninstall
imoimiphone	7.00.2701	7.0.27	imo	-	↗

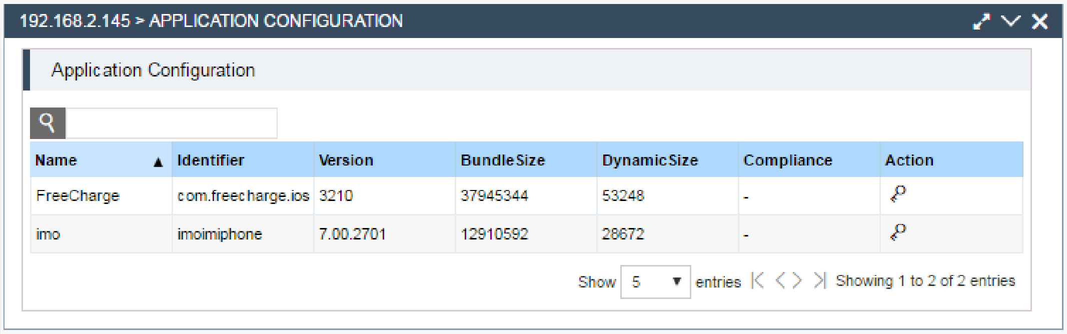
Show 5 entries Showing 1 to 1 of 1 entries

Software uninstallation initiated.

Configuring Application Configuration Settings

You can view the detailed information of the installed applications on an iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Software Deployment -> Application Configuration.**



192.168.2.145 > APPLICATION CONFIGURATION

Application Configuration

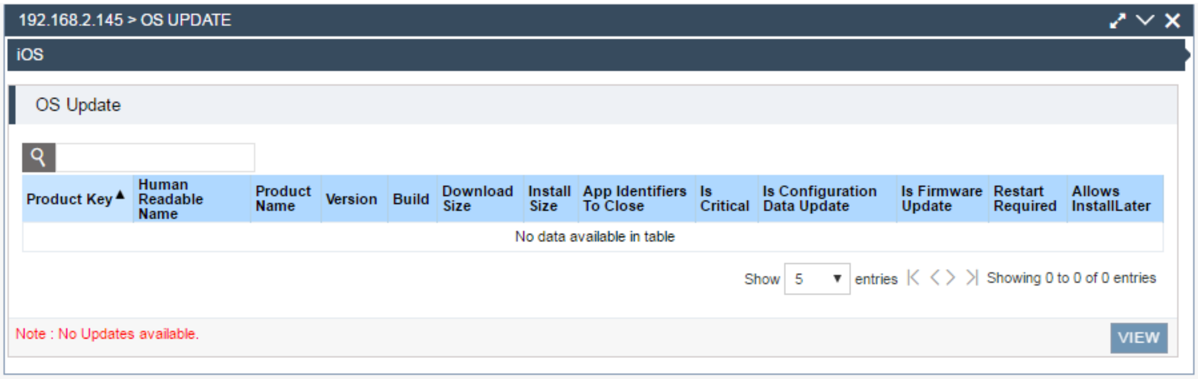
Name ▲	Identifier	Version	BundleSize	DynamicSize	Compliance	Action
FreeCharge	com.freecharge.ios	3210	37945344	53248	-	🔍
imo	imoimiphone	7.00.2701	12910592	28672	-	🔍

Show 5 entries Showing 1 to 2 of 2 entries

Configuring OS Update

User can keep track of the available OS version updates on an iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Software Deployment** -> **OS Update.**



192.168.2.145 > OS UPDATE

iOS

OS Update

Product Key ▲	Human Readable Name	Product Name	Version	Build	Download Size	Install Size	App Identifiers To Close	Is Critical	Is Configuration Data Update	Is Firmware Update	Restart Required	Allows InstallLater
No data available in table												

Show 5 entries Showing 0 to 0 of 0 entries

Note : No Updates available.

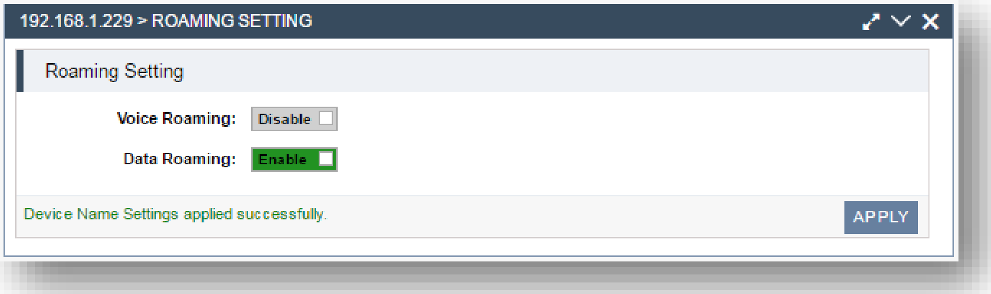
Working with Device Settings

Configuring Roaming Settings

User can configure roaming settings for an iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Device Setting -> Roaming setting.**
3. Select the required option for **Voice Roaming** and **Data Roaming.**
4. Click on the **APPLY** button

   The Settings applied summary message displayed.



192.168.1.229 > ROAMING SETTING

Roaming Setting

Voice Roaming: Disable □

Data Roaming: Enable □

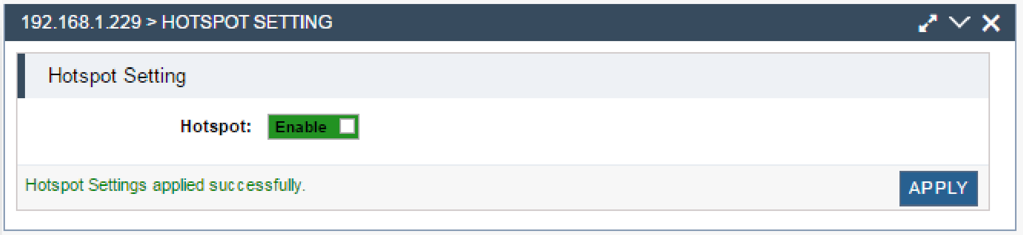
Device Name Settings applied successfully.

Configuring Hotspot Settings

User can configure hotspot settings for an iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Device Setting -> Hotspot Setting.**
3. Select the required option for **Hotspot**.
4. Click on the **APPLY** button

   'Hotspot Settings applied successfully' summary message is displayed.


192.168.1.229 > HOTSPOT SETTING

Hotspot Setting

Hotspot: Enable ☐

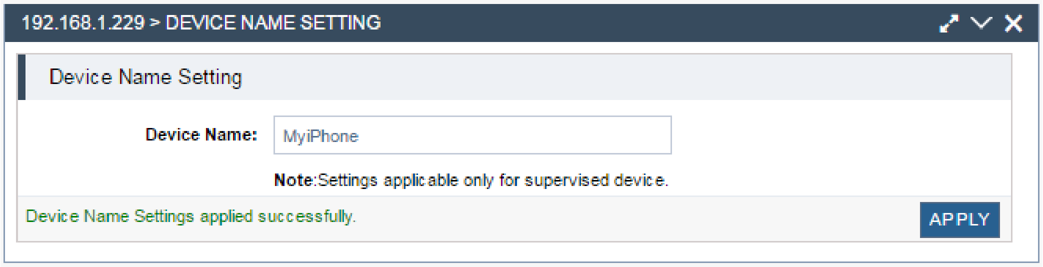
Hotspot Settings applied successfully.

Configuring Device Name Settings

User can change the device name of the registered iOS device.

1. Choose the desired device from the devices tree.
2. Expand the right hand side menu and click on **Device Setting -> Device Name Setting.**
3. Enter a name to be set on the device in the **Device Name** textbox.
4. Click on the **APPLY** button

   '**Device Name Settings applied successfully'** summary message is displayed.


192.168.1.229 > DEVICE NAME SETTING

Device Name Setting

Device Name: MyiPhone

Note:Settings applicable only for supervised device.

Device Name Settings applied successfully.

The settings will only be applied on supervised devices.

Remote Control Tools for iOS MDM

Remote control enables the administrator to remotely control functions such as capturing device data, locking device, wipe, clear passcode.

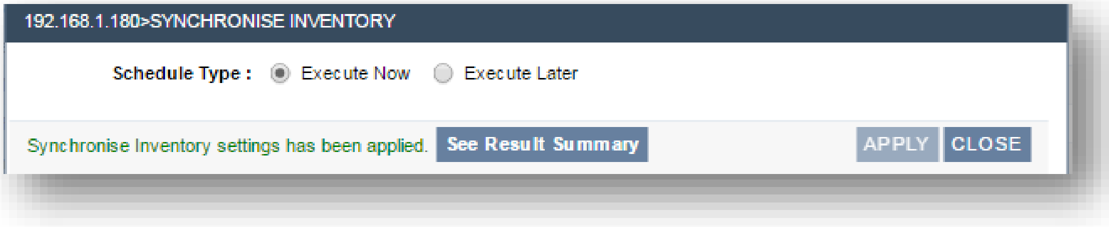
Synchronizing Inventory

Inventory synchronization enables the administrator to acquire details of all devices in a group.

To synchronize inventory

1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Synchronise Inventory**.
3. Select the required **Schedule Type**.
4. Click **Apply**.

   The **Request for settings update processed** message is display.



192.168.1.180>SYNCHRONISE INVENTORY

Schedule Type : ● Execute Now ○ Execute Later

Synchronise Inventory settings has been applied.

Send Message

Allows administrator to send a message to all the devices in a group.

To send a message

1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Send Message**.
3. Select the required **Schedule Type**.
4. Click **Apply**.

   The **Client message settings has been applied** message is displayed.

An application 'PushChatStarter' needs to be pre-installed on the iOS device for receiving messages.

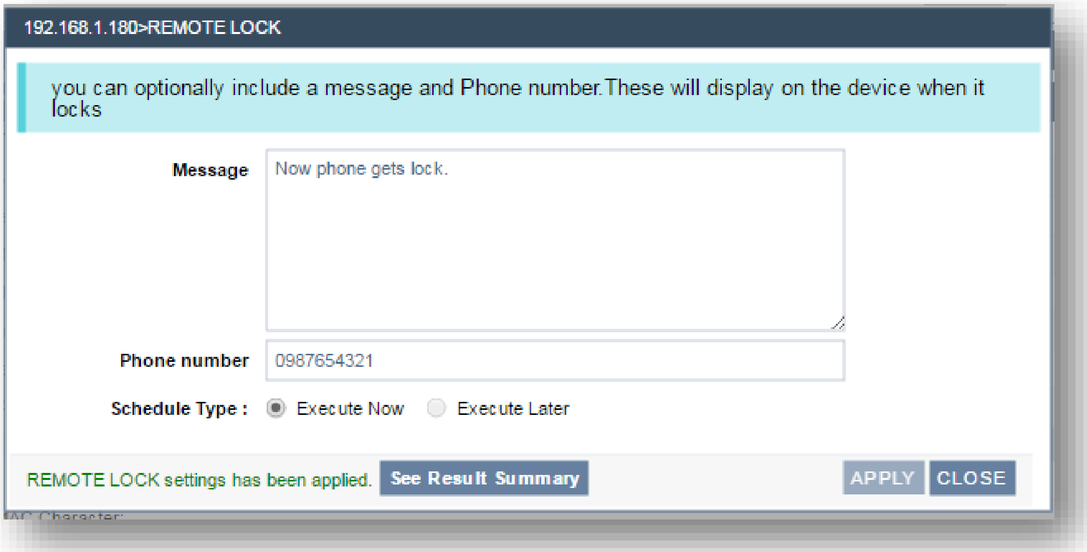
Remote Lock

Allow administrator to lock device as soon as settings get applied.

To lock device

1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Remote Lock.**
3. User able to send message and contact number while locking device.
4. Select the required **Schedule Type**.

5. Click **Apply**.



192.168.1.180>REMOTE LOCK

you can optionally include a message and Phone number.These will display on the device when it locks

Message: Now phone gets lock.

Phone number: 0987654321

Schedule Type : ● Execute Now ○ Execute Later

REMOTE LOCK settings has been applied.

The **Request for settings update processed** message is display.

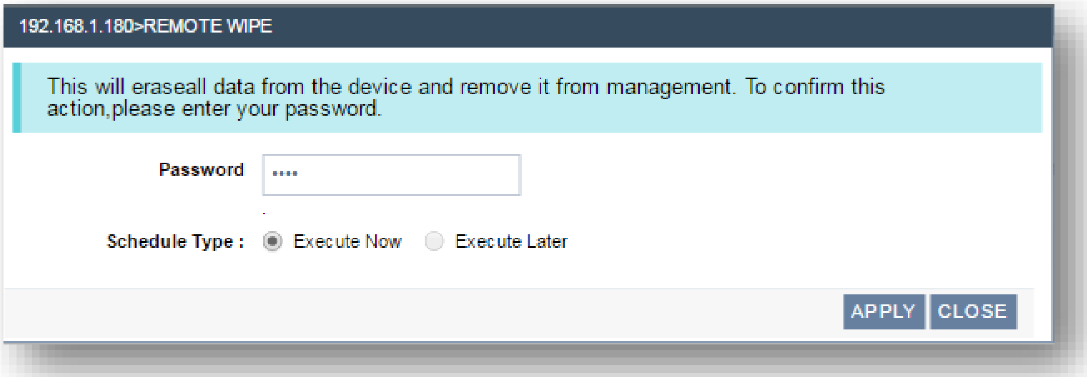
6. Click on **Close** to close open form.

Remote Wipe

Allow administrator to wipe data from device once task get succeeded.

To Lock device

1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Remote Wipe.**



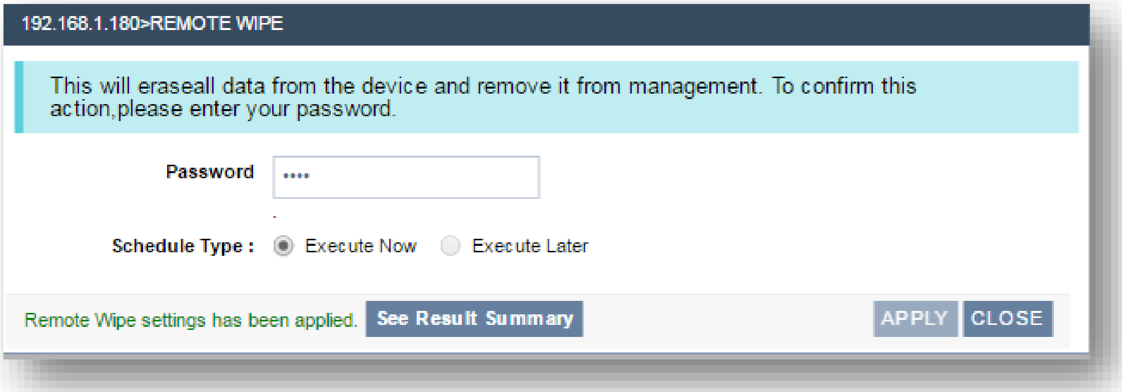
192.168.1.180>REMOTE WIPE

This will eraseall data from the device and remove it from management. To confirm this action,please enter your password.

Password: ••••

Schedule Type : ● Execute Now ○ Execute Later

3. User able to erase data from device, before that user have to enter device password to perform this action.


192.168.1.180>REMOTE WIPE

This will eraseall data from the device and remove it from management. To confirm this action,please enter your password.

Password: ••••

Schedule Type : ● Execute Now ○ Execute Later

Remote Wipe settings has been applied.

4. Select the required **Schedule Type**.
5. Click **Apply**.

   The **Request for settings update processed** message is display.

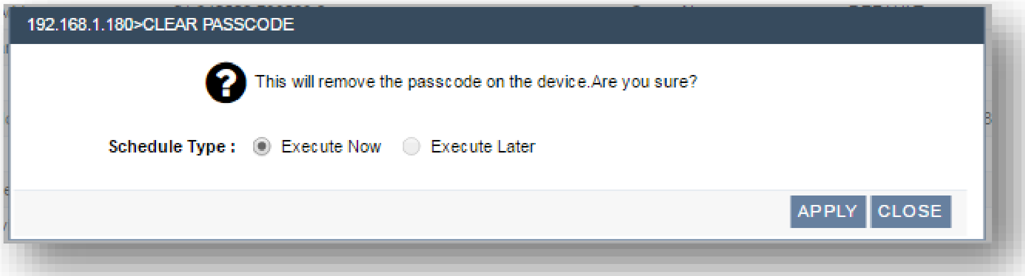
6. Click on **Close** to close open form.

Clear Passcode

Allow administrator to clear passcode from device after task get succeeded.

To Clear Passcode

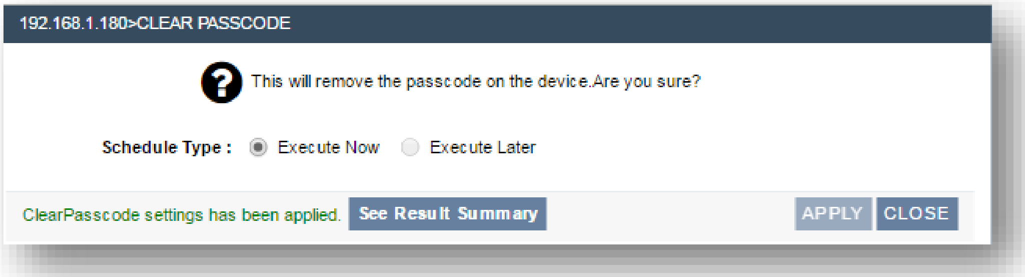
1. In the devices tree, right-click the group node.
2. In **Remote Control**, select **Clear Passcode.**
3. User able to remove passcode from device after performing this action.


192.168.1.180>CLEAR PASSCODE

This will remove the passcode on the device.Are you sure?

Schedule Type : ● Execute Now ○ Execute Later

4. Select the required **Schedule Type**.



192.168.1.180>CLEAR PASSCODE

This will remove the passcode on the device.Are you sure?

Schedule Type : ● Execute Now ○ Execute Later

ClearPasscode settings has been applied.

5. Click **Apply**.

   The **Request for settings update processed** message is display.

6. Click on **Close** to close open form.

Working with the Task Manager in Android

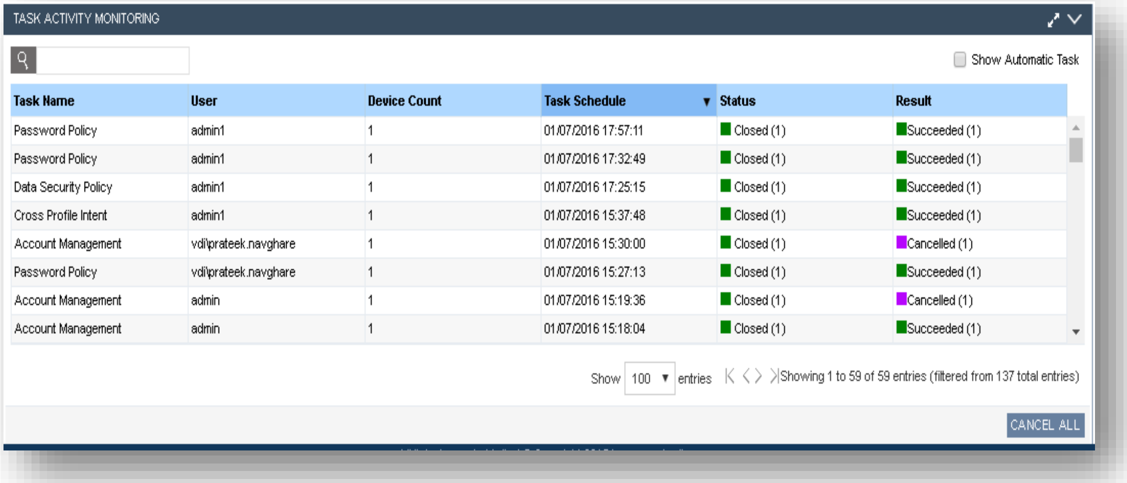
Task Manager is used to create, track, and maintain the tasks that have been performed as a part of the management process. It is also used to examine the tasks on a granular basis when required to indicate why tasks may have failed or otherwise.

It displays the status of settings applied on the devices as well as any activity executed on the server.

The **Device Count** column displays the number of devices to which a particular administrator has applied a specific task.

The settings applied on a device are reflected on task activity with the status as ‘Pending’ and the status changes to ‘In Process’ when the server sends these settings to the devices.

The last status shows as ‘Completed' or 'Unsuccessful' when the settings have been successfully applied to the devices. The schedules that are pending can be deleted through this option. Details of the applied schedule can be viewed by clicking on the schedule.



Task Name	User	Device Count	Task Schedule	Status	Result
Password Policy	admin1	1	01/07/2016 17:57:11	🟩 Closed (1)	🟩Succeeded (1)
Password Policy	admin1	1	01/07/2016 17:32:49	🟩 Closed (1)	🟩Succeeded (1)
Data Security Policy	admin1	1	01/07/2016 17:25:15	🟩 Closed (1)	🟩Succeeded (1)
Cross Profile Intent	admin1	1	01/07/2016 15:37:48	🟩 Closed (1)	🟩Succeeded (1)
Account Management	vdi\prateek.navghare	1	01/07/2016 15:30:00	🟩 Closed (1)	🟪Cancelled (1)
Password Policy	vdi\prateek.navghare	1	01/07/2016 15:27:13	🟩 Closed (1)	🟩Succeeded (1)
Account Management	admin	1	01/07/2016 15:19:36	🟩 Closed (1)	🟪Cancelled (1)
Account Management	admin	1	01/07/2016 15:18:04	🟩 Closed (1)	🟩Succeeded (1)

Show 100 ▾ entries |< < > >| Showing 1 to 59 of 59 entries (filtered from 137 total entries)

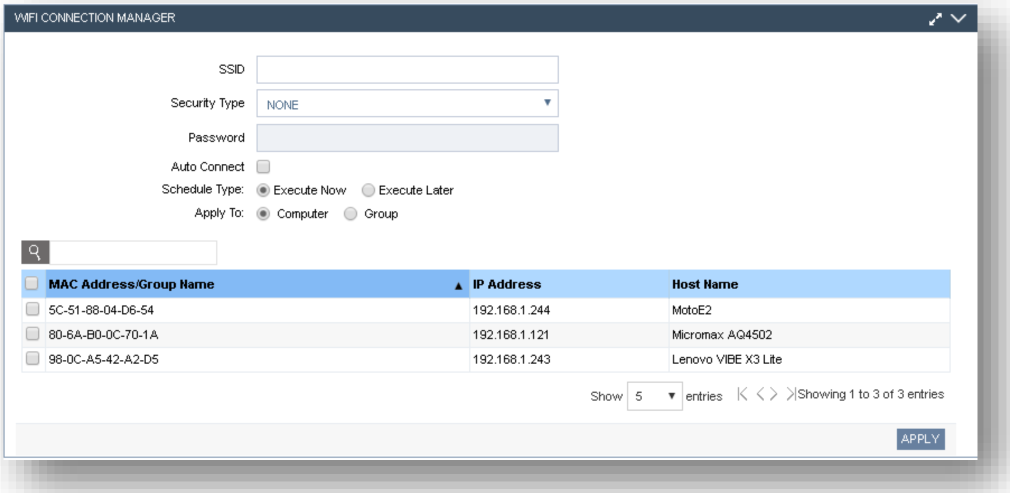
Configuring System Settings

Creating Tasks to Configure WiFi connection settings

Under Wi-Fi connection settings, you can set the date and time, the time zone, and also the time server. These settings can then be applied to one device or to all the devices in a group.

1. In the devices tree, click the required group.
2. From the toolbar, click Views ☰.

   Click on Task Management. The **Task Management** page is displayed.
3. Expand the right menu.
4. Click **Android.**
5. Click **System Settings**, then click **Network Settings**, and then click **WiFi connection Manager**.
6. In the **SSID** box, enter the required SSID name.
7. In the **security Type** box, Select security type (NONE or WEP or WPA/WPA2).
8. If Select WEP or WAP/WAP2 as Security type, enter password.
9. Select the required **Schedule Type**.
10. Under **Apply To**, select any one of the following:
    a. **Computer** – enables you to select a device and implement the settings
    b. **Group –** enables you to implement the settings to all devices in a group on the devices tree



WIFI CONNECTION MANAGER

SSID:

Security Type: NONE

Password:

Auto Connect □

Schedule Type: ● Execute Now ○ Execute Later

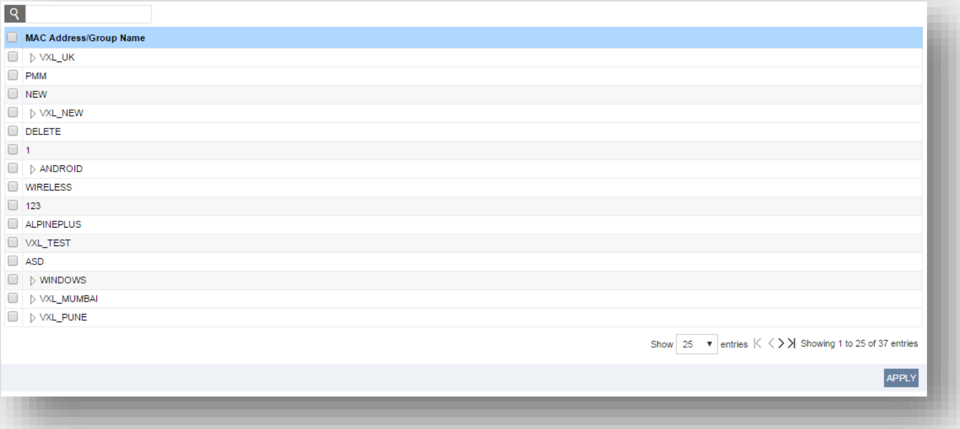
Apply To: ● Computer ○ Group

□ MAC Address/Group Name ▲	IP Address	Host Name
□ 5C-51-88-04-D6-54	192.168.1.244	MotoE2
□ 80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□ 98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

APPLY

- On selecting option, Group in Apply to, groups along with hierarchy structure if present will be display.
- All subgroup present under those groups will be list out.
- If user select parent group all child group should get select.
- This Group Hierarchy feature not implemented for all modules.

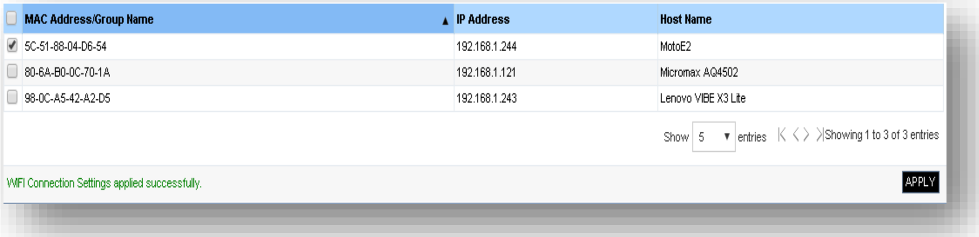


□	MAC Address/Group Name
□	▷ VXL_UK
□	PMM
□	NEW
□	▷ VXL_NEW
□	DELETE
□	1
□	▷ ANDROID
□	WIRELESS
□	123
□	ALPINEPLUS
□	VXL_TEST
□	ASD
□	▷ WINDOWS
□	▷ VXL_MUMBAI
□	▷ VXL_PUNE

Show 25 entries Showing 1 to 25 of 37 entries

11. From the table, select the check box against the required device/group.
12. Click **Apply**.

    The **Request for settings update processed** message is display.



□	MAC Address/Group Name	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

WIFI Connection Settings applied successfully.

Configuring Security Settings

Creating a Task to Configure the Password Policy

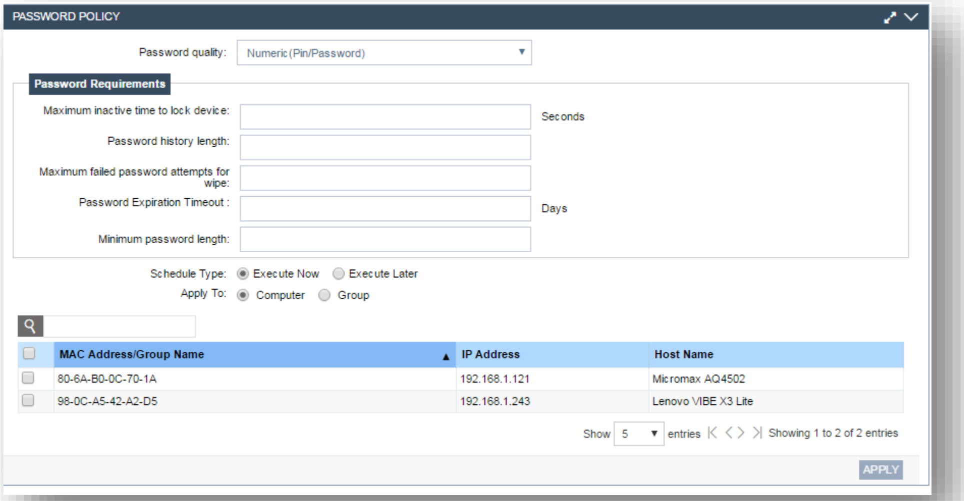
You can configure the password policy for a remotely connected device. Its useful for security purpose.

The following password type can be set from the server:

- **Numeric**: PIN/ Password
- **Alphabetic**: Password

- **Alpha Numeric**: Password
- **Complex**: Password
- **Unspecified**: None/Swipe/Pin/Pattern/Password
- **Something:** Pin/Password/Pattern

1. From the toolbar, click Views ☰.
    a. Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**
4. Click **Security Settings**, then click **Password Policy.**



PASSWORD POLICY

Password quality: Numeric (Pin/Password)

Password Requirements

Maximum inactive time to lock device: Seconds

Password history length:

Maximum failed password attempts for wipe:

Password Expiration Timeout : Days

Minimum password length:

Schedule Type: ● Execute Now ○ Execute Later

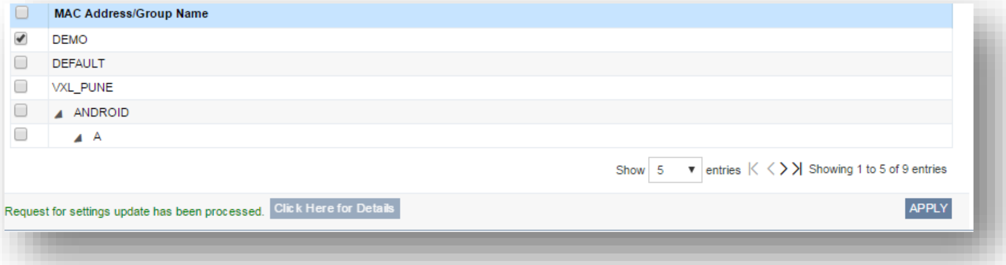
Apply To: ● Computer ○ Group

□	MAC Address/Group Name	IP Address	Host Name
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 2 of 2 entries

APPLY

5. Select Password Quality, as mention above.
6. According to password quality, enter different parameters.
7. Select the required **Schedule Type**.
8. Under **Apply To**, select any one of the following:
    a. Computer – enables you to select a device and implement the settings
    b. Group – enables you to implement the settings to all devices in a group on the devices tree
9. From the table, select the check box against the required device/group.
10. Click **Apply**.
    The **Request for settings update processed** message is displayed.



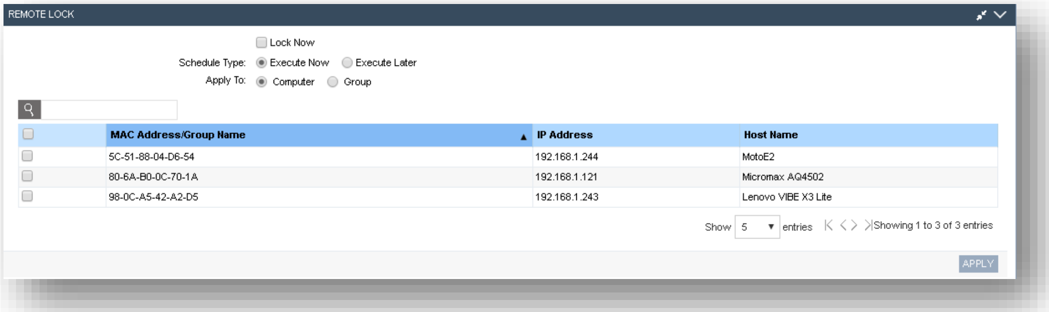
□	MAC Address/Group Name
☑	DEMO
□	DEFAULT
□	VXL_PUNE
□	◢ ANDROID
□	◢ A

Show 5 ▾ entries Showing 1 to 5 of 9 entries

Request for settings update has been processed. Click Here for Details

Creating a Task to Configure Remote Lock Settings

1. From the toolbar, click Views ☰ .
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **Remote Lock.**



REMOTE LOCK

□ Lock Now

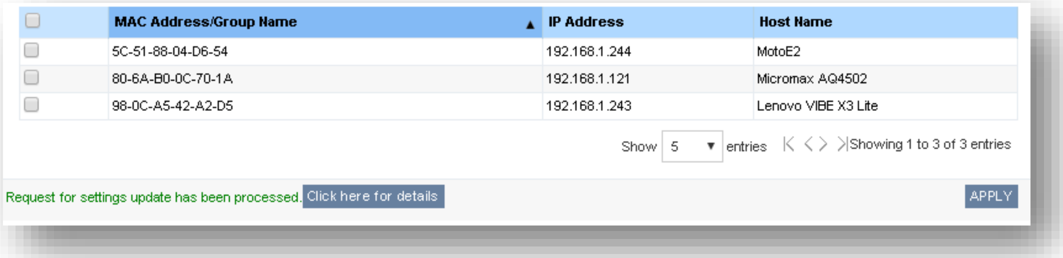
Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	MAC Address/Group Name	IP Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries Showing 1 to 3 of 3 entries

5. From the **Remote lock, select the checkbox.**
6. Select the required **Schedule Type**.
7. Under **Apply To**, select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group**– enables you to implement the settings to all devices in a group on the devices tree
8. From the table, select the check box against the required device/group.
9. Click **Apply**.
   The **Settings applied** message is displayed.



☐	MAC Address/Group Name ▲	IP Address	Host Name
☐	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 3 of 3 entries

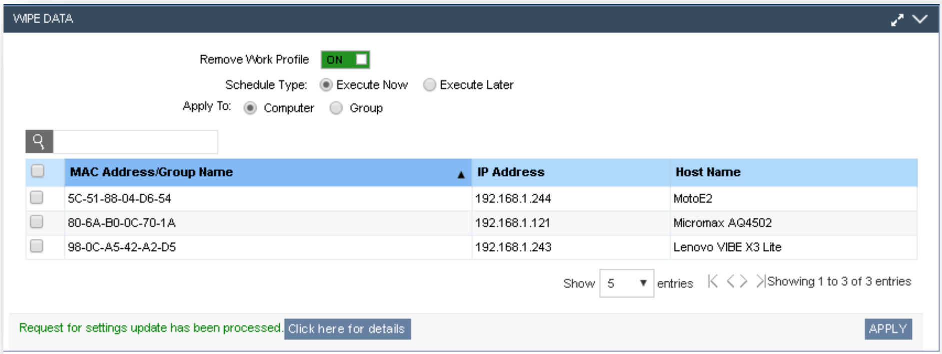
Request for settings update has been processed. Click here for details

Creating a Task to Configure Wipe Data Settings

To remotely remove the work profile from a device

1. In the devices tree, click the required group.
2. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.
3. Expand the right menu.
4. Click **Android.**
5. Click **Security Settings**, then click **Wipe Data**
6. Enable the Wipe data Settings
7. Select the required **Schedule Type**.
8. Under **Apply To**, select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
9. From the table, select the check box against the required device/group.
10. Click **Apply**.

    The **Request for settings update processed** message is display.



WIPE DATA

Remove Work Profile ON

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

☐	MAC Address/Group Name ▲	IP Address	Host Name
☐	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 3 of 3 entries

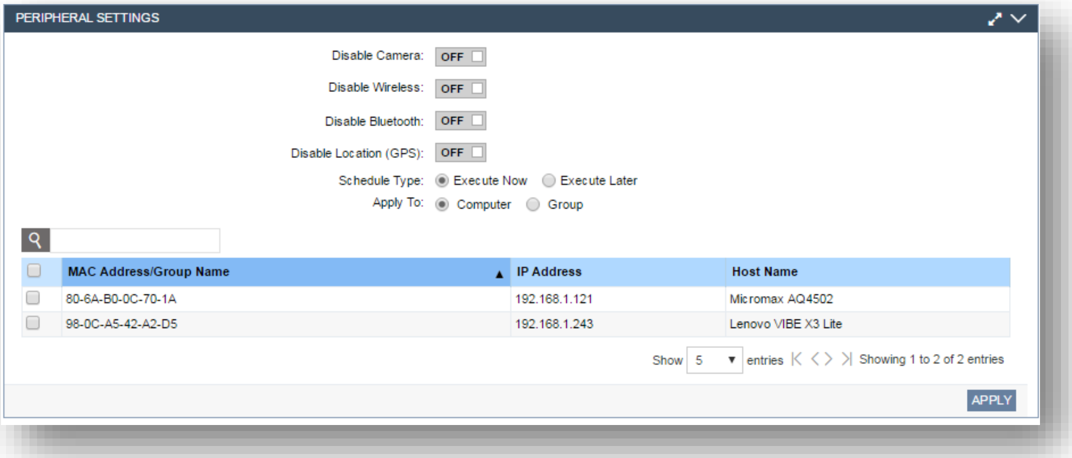
Request for settings update has been processed. Click here for details

Creating a Task to Configuring Peripheral Settings

You can disable a Camera, Wifi, Bluetooth, GPS attached to a remote device on the network.

To enable or disable a required option:

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **Peripheral settings.**



PERIPHERAL SETTINGS

Disable Camera: OFF □

Disable Wireless: OFF □

Disable Bluetooth: OFF □

Disable Location (GPS): OFF □

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	MAC Address/Group Name ▲	IP Address	Host Name
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 2 of 2 entries

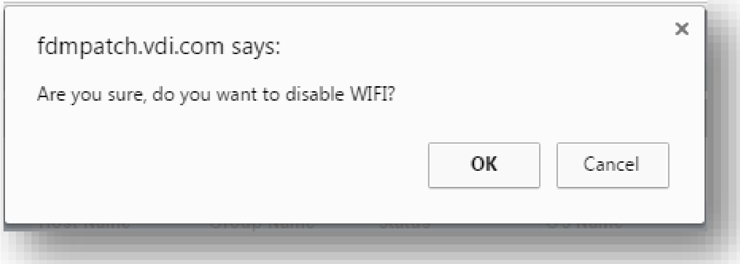
APPLY

5. Enable/Disable the settings.
6. Select the required **Schedule Type**.
7. Under **Apply To**, select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
8. From the table, select the check box against the required device/group.
9. Click **Apply**.

   The **Request for settings update processed**message is display.

When we disable Wi-Fi settings, server shows confirmation popup “Are you sure, do you want to disable Wi-Fi?”

If Ok is clicked, after task completion, the client will get off due no network connection.



fdmpatch.vdi.com says:

Are you sure, do you want to disable WIFI?

Creating Tasks to Configure Data Security Policy

You can configure data security policies to the connected Android device. On occurrence of any of the mentioned event, the selected security action will be applied on the device.

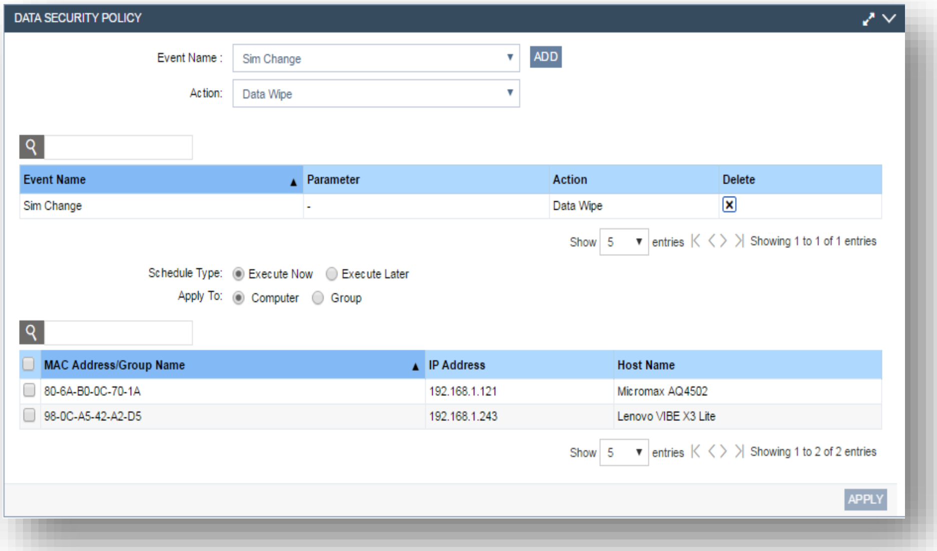
Events and Actions explained in short as follows:

Event Name:

- **Sim Change**: Change of SIM card on the device.
- **Device Rooting**: Rooting of an Android device.
- **Number of days not communicated:** Number of days not communicated with the server.
- **Password Policy:** Changing the password type on the device.
- **No of failed password attempts:** Number of failed password attempts on the device.

Action:

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **data Security policy.**
5. Select the required **Schedule Type**.
6. Under **Apply To**, select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree.



DATA SECURITY POLICY

Event Name : Sim Change ▾ ADD

Action: Data Wipe ▾

Event Name	Parameter	Action	Delete
Sim Change	-	Data Wipe	☒

Show 5 ▾ entries Showing 1 to 1 of 1 entries

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

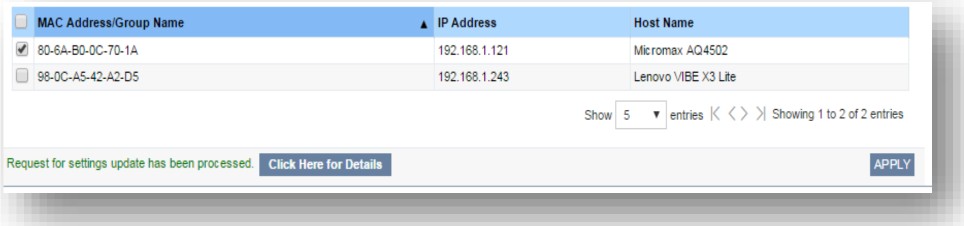
□	MAC Address/Group Name	IP Address	Host Name
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries Showing 1 to 2 of 2 entries

APPLY

7. From the table, select the check box against the required device/group.
8. Click **Apply**.

   The **Request for settings update processed** message is display.



□	MAC Address/Group Name	IP Address	Host Name
☑	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries Showing 1 to 2 of 2 entries

Request for settings update has been processed. Click Here for Details APPLY

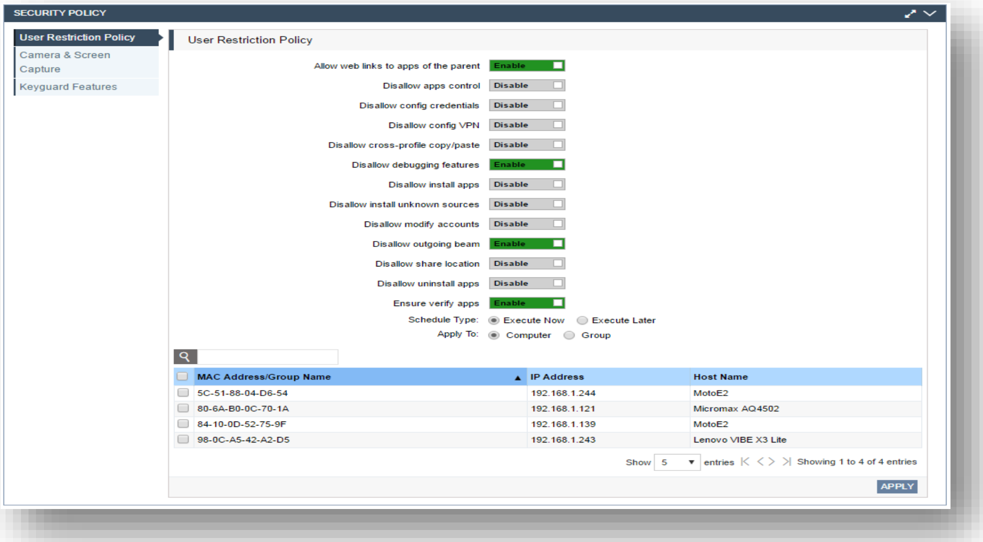
Creating a Task to Configure Security Policy

You can set various security policies to a remote device on the network.

Creating a Task to Configuring User Restriction

1. From the toolbar, click Views ☰.

   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **Security Policy.**
5. Select **User Restriction.**



User Restriction Policy

Allow web links to apps of the parent	Enable
Disallow apps control	Disable
Disallow config credentials	Disable
Disallow config VPN	Disable
Disallow cross-profile copy/paste	Disable
Disallow debugging features	Enable
Disallow install apps	Disable
Disallow install unknown sources	Disable
Disallow modify accounts	Disable
Disallow outgoing beam	Enable
Disallow share location	Disable
Disallow uninstall apps	Disable
Ensure verify apps	Enable

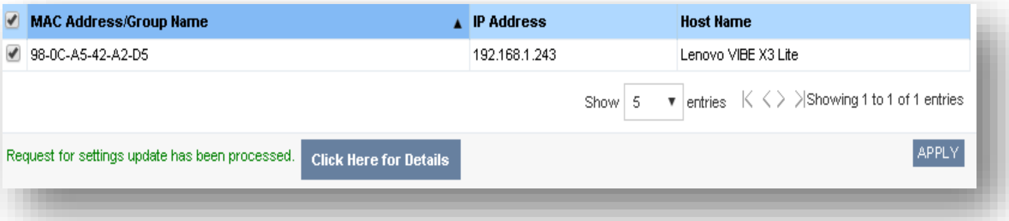
Schedule Type: ● Execute Now ○ Execute Later
Apply To: ● Computer ○ Group

□	MAC Address/Group Name ▲	IP Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

6. Enable/Disable the required User restrictions
7. Under Apply To , select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group**– enables you to implement the settings to all devices in a group on the devices tree
8. From the table, select the check box against the required device/group.
9. Click **Apply**.

   The **Request for settings update processed** message is displayed.



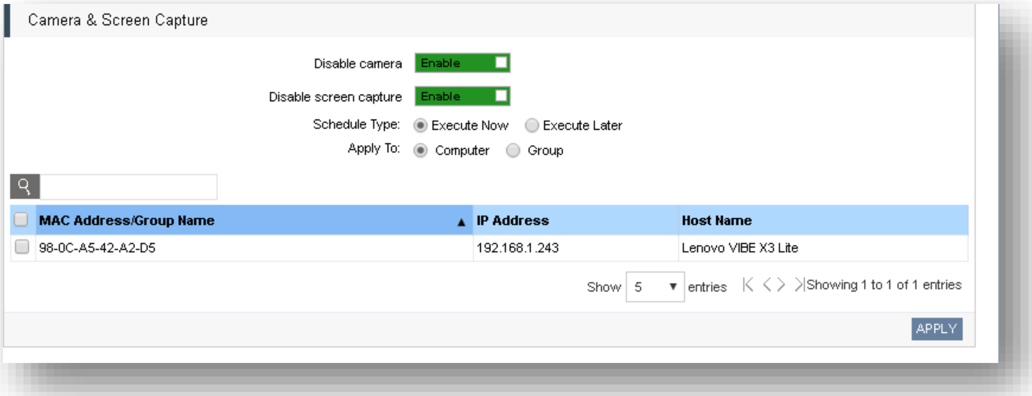
☑	MAC Address/Group Name ▲	IP Address	Host Name
☑	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 1 of 1 entries

Request for settings update has been processed.

Creating a Task to Configure Camera & Screen Capture settings

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **Security Policy.**
5. Select **Camera & Screen Capture** settings**.**



Camera & Screen Capture

Disable camera: Enable

Disable screen capture: Enable

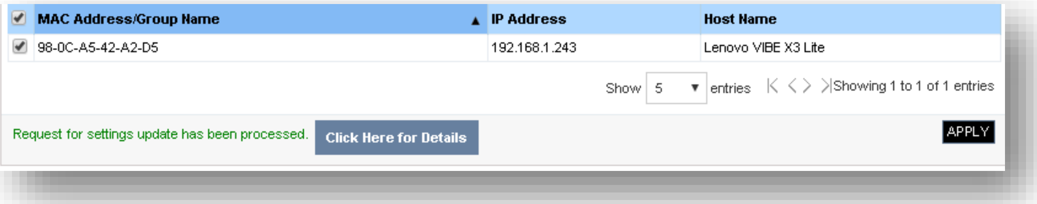
Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	MAC Address/Group Name	IP Address	Host Name
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 1 of 1 entries

6. Enable/Disable **Camera & Screen capture** settings as required**.**
7. Select the required **Schedule Type**.
8. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the properties
    b. **Group** – enables you to implement the properties to all devices in a group
9. From the table, select the check box against the required device/group.
10. Click Apply.
11. The **Request for settings update processed** message is displayed.



☑	MAC Address/Group Name	IP Address	Host Name
☑	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

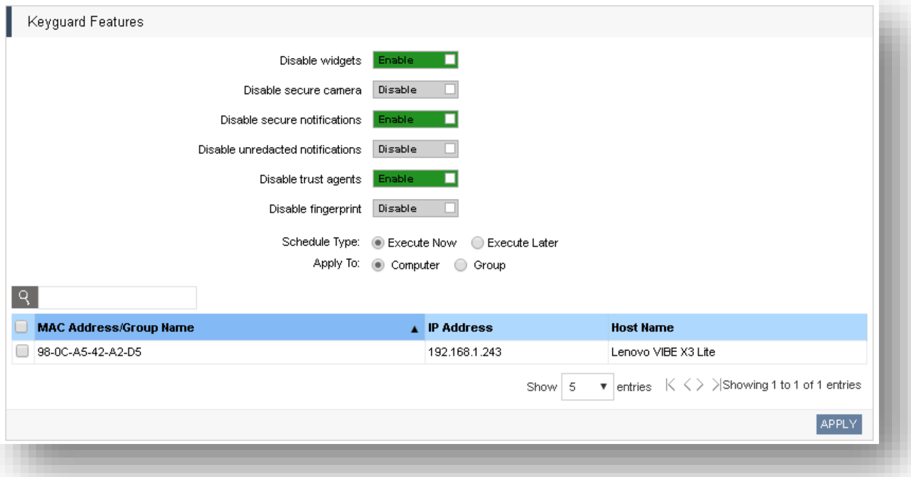
Show 5 entries Showing 1 to 1 of 1 entries

Request for settings update has been processed.

Creating a Task to Configure Key guard Features.

You can configure various key guard features on the connected Android device.

1. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Security Settings**, then click **Security Policy.**
5. Select **Keyguard Features.**



Keyguard Features

Disable widgets: Enable

Disable secure camera: Disable

Disable secure notifications: Enable

Disable unredacted notifications: Disable

Disable trust agents: Enable

Disable fingerprint: Disable

Schedule Type: ● Execute Now ○ Execute Later

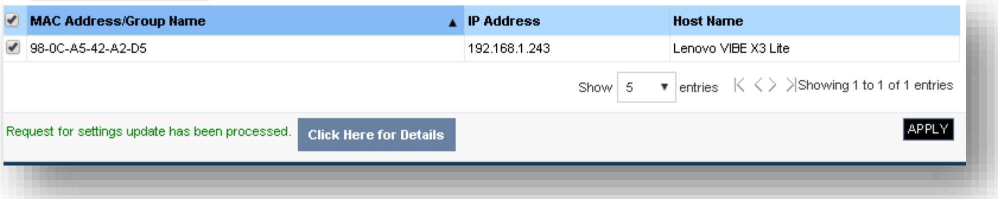
Apply To: ● Computer ○ Group

□	MAC Address/Group Name ▲	IP Address	Host Name
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 1 of 1 entries

6. Enable/Disable **Camera & Screen Capture** settings as required**.**
7. Select the required **Schedule Type**.
8. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the properties
    b. **Group** – enables you to implement the properties to all devices in a group
9. From the table, select the check box against the required device/group.
10. Click Apply.

    The **Request for settings update processed** message is displayed.



☑	MAC Address/Group Name ▲	IP Address	Host Name
☑	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 1 of 1 entries

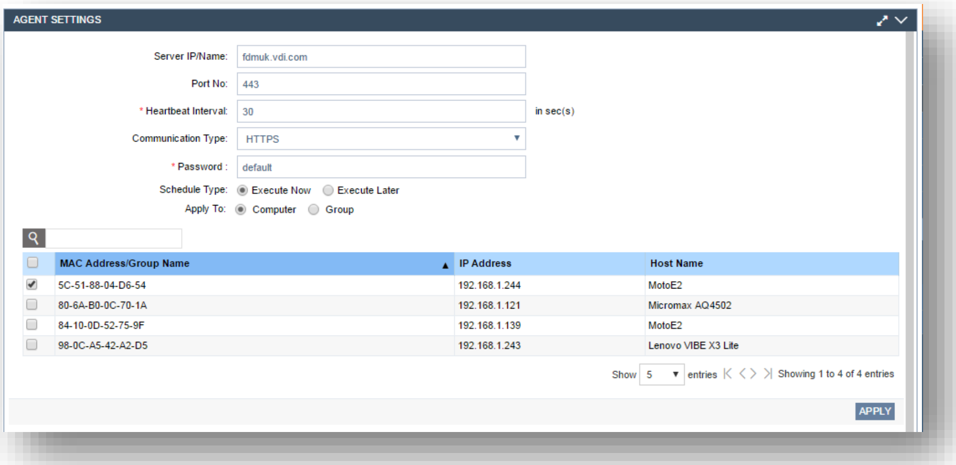
Request for settings update has been processed.

Configuring Administration

Creating a Task to Configure Agent settings.

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**.

4. Click **Administration**, then click **Agent Settings.**



Server IP/Name: fdmuk.vdi.com

Port No: 443

* Heartbeat Interval: 30 in sec(s)

Communication Type: HTTPS

* Password : default

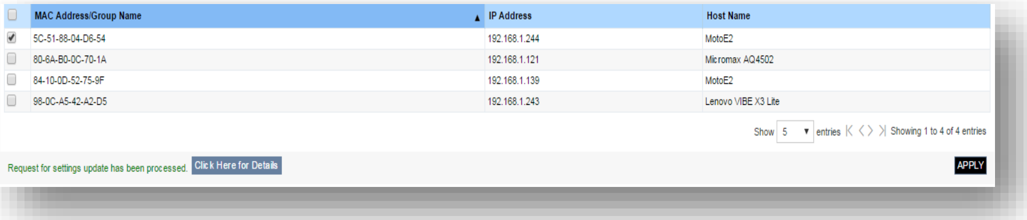
Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	MAC Address/Group Name ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

5. In **Server IP/Name**, enter any one of the following:
    a. **Server IP Address**
    b. **Server Name**
6. In **Port No**, enter the port number.
7. In **Heartbeat Interval**, enter the required value.
8. From the **Communication Type** list, select the required option.
9. In **Password**, enter the required password.
10. Select the required **Schedule Type**.
11. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the Agent settings
    b. **Group** – enables you to implement the Agent settings to all devices in a group
12. From the table, select the check box against the required device/group.
13. Click **Apply**.
    The **Request for settings update processed** message is display.



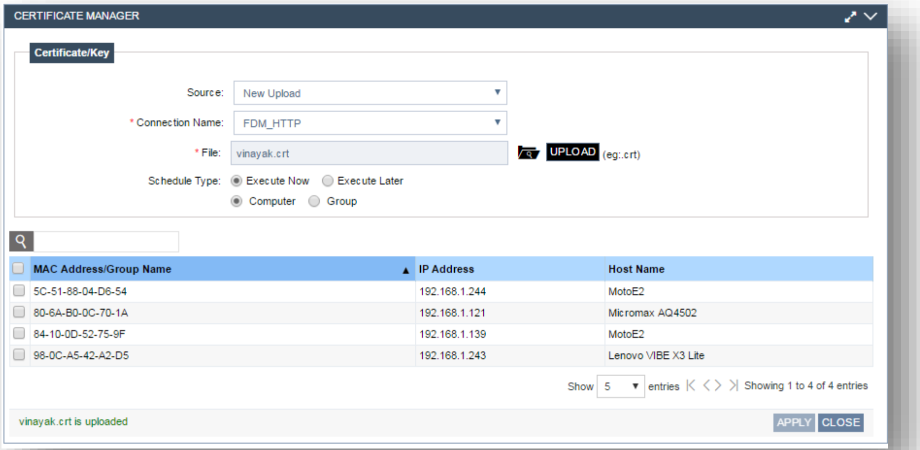
□	MAC Address/Group Name ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

Request for settings update has been processed.

Creating a Task to Configure CertificateManager

1. From the toolbar, click Views.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**.
4. Click **Administration**, then click **Certificate Manger.**
5. To upload a new certificate, from **Source** dropdown select **New Upload**.
6. Select the required **Connection Name**.
7. Click the file browser icon to browse the file & click **Upload** button to upload the file.



CERTIFICATE MANAGER

Certificate/Key

Source: New Upload

* Connection Name: FDM_HTTP

* File: vinayak.crt UPLOAD (eg:.crt)

Schedule Type: ● Execute Now ○ Execute Later

● Computer ○ Group

□	MAC Address/Group Name	IP Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

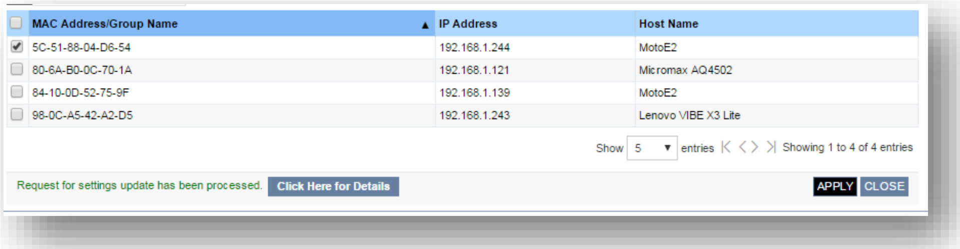
Show 5 entries Showing 1 to 4 of 4 entries

vinayak.crt is uploaded

APPLY CLOSE

Certificates of ‘crt’ extension file format are valid for the Android devices.

8. To use a previously uploaded certificate, select **Repository** from Source dropdown.
9. Select the required **Connection Name**.
10. Select the certificate **File**.
11. Select the required **Schedule Type**.
12. Under **Apply To**, select any one of the following:
    a. **Computer** – enables you to select a device and implement the Certificate Manger
    b. **Group** – enables you to implement the Certificate Manger to all devices in a group
13. From the table, select the check box against the required device/group.
14. Click **Apply**.
    The **Request for settings update processed** message is display.



☐ MAC Address/Group Name ▲	IP Address	Host Name
☑ 5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐ 80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐ 84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐ 98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

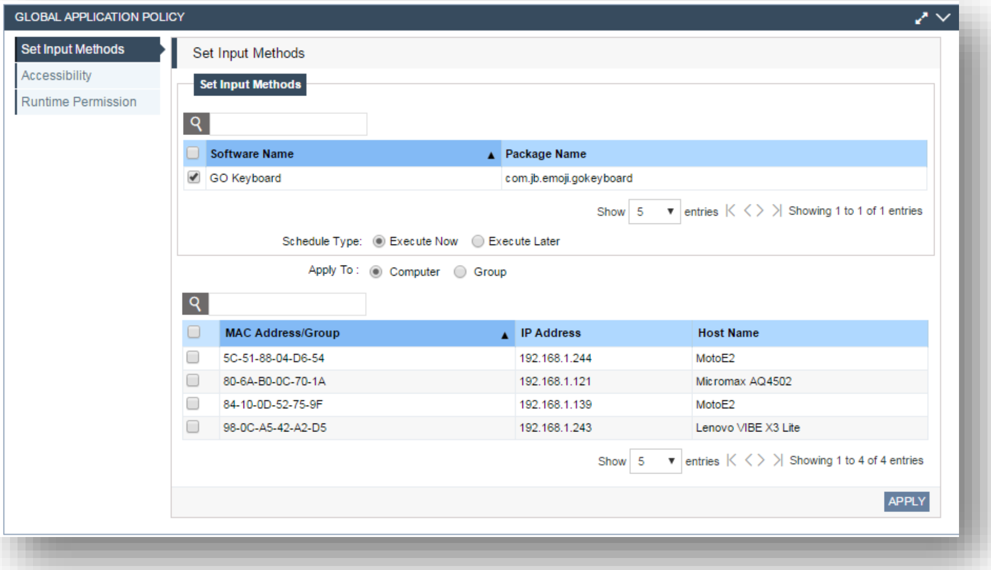
Show 5 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

Request for settings update has been processed.

Creating a Task to Configure Global Application Policy

Creating a Task to Execute a Set Input Method:

1. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**
4. Click **Administration** and then click **Global Application Policy.**
5. Select **Set Input Methods**.



☐ Software Name ▲	Package Name
☑ GO Keyboard	com.jb.emoji.gokeyboard

Show 5 ▾ entries |< < > >| Showing 1 to 1 of 1 entries

Schedule Type: ● Execute Now ○ Execute Later

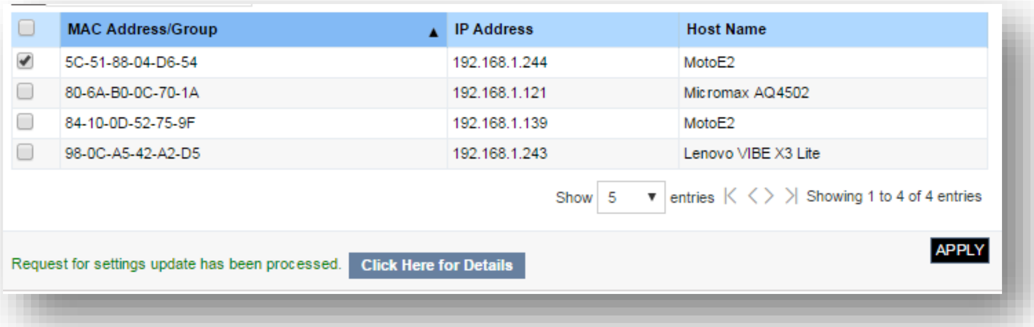
Apply To : ● Computer ○ Group

☐ MAC Address/Group ▲	IP Address	Host Name
☐ 5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐ 80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐ 84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐ 98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

6. Select / unselect the required input method to enable/disable purpose respectively.
7. Select the required **Schedule Type**.
8. Under **Apply To** , select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
9. From the table, select the check box against the required device/group.

10. Click **Apply**.
    The **Request for settings update processed** message is display.



☐	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

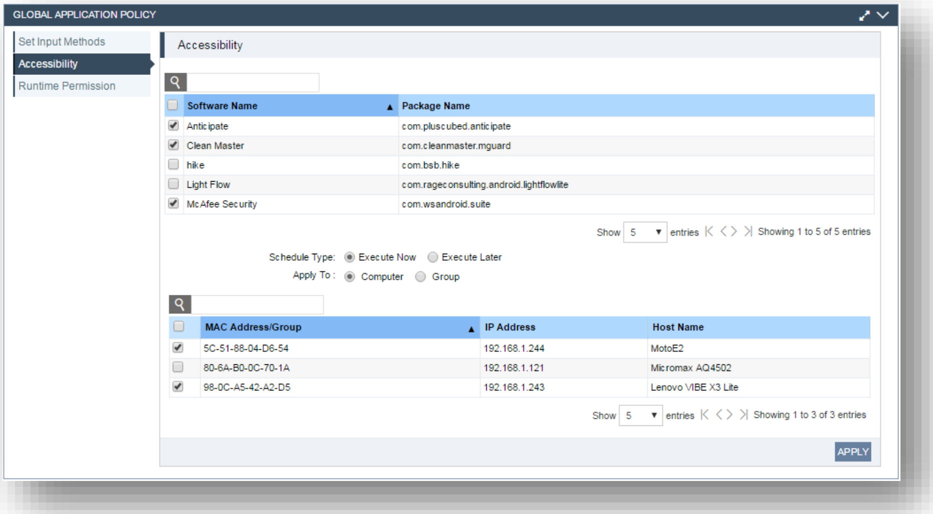
Show 5 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

Request for settings update has been processed. Click Here for Details

APPLY

Creating a Task to Execute Accessibility

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**
4. Click **Administration** and then click **Global Application Policy.**
5. Select **Accessibility**.
6. Select / unselect the required Application to enable/disable purpose respectively.



GLOBAL APPLICATION POLICY

Set Input Methods
Accessibility
Runtime Permission

Accessibility

☐	Software Name ▲	Package Name
☑	Anticipate	com.pluscubed.anticipate
☑	Clean Master	com.cleanmaster.mguard
☐	hike	com.bsb.hike
☐	Light Flow	com.rageconsulting.android.lightflowlite
☑	McAfee Security	com.wsandroid.suite

Show 5 ▾ entries |< < > >| Showing 1 to 5 of 5 entries

Schedule Type: ● Execute Now ○ Execute Later
Apply To : ● Computer ○ Group

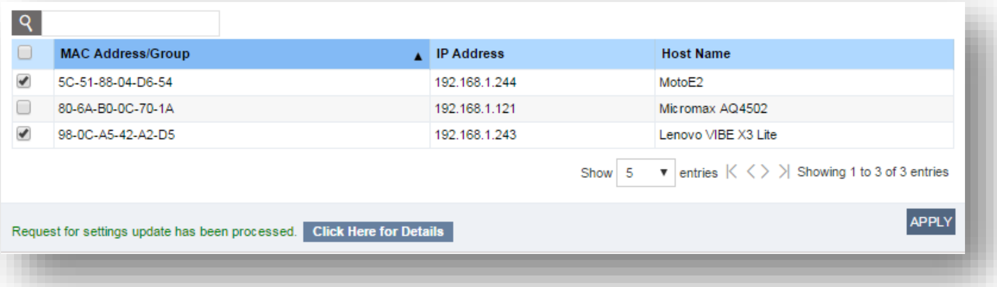
☐	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☑	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 3 of 3 entries

APPLY

7. Select the required **Schedule Type**.
8. Under **Apply To** , select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
9. From the table, select the check box against the required device/group.

10. Click **Apply**.
    The **Request for settings update processed** message is display



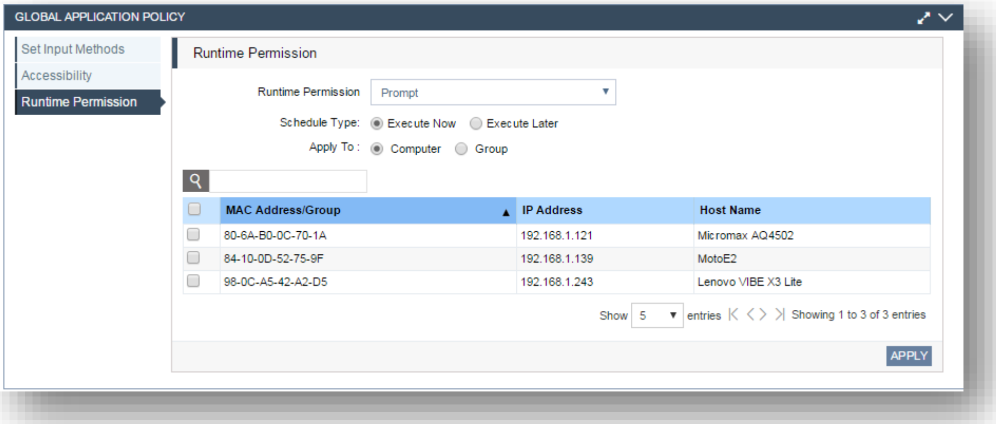
☐	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☑	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

Request for settings update has been processed.

Creating a Task to Configure Runtime Permission

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**
4. Click **Administration** and then click **Global Application Policy.**
5. Select **Runtime Permission.**
6. Select one value from dropdown.



Runtime Permission

Runtime Permission: Prompt

Schedule Type: ● Execute Now ○ Execute Later

Apply To : ● Computer ○ Group

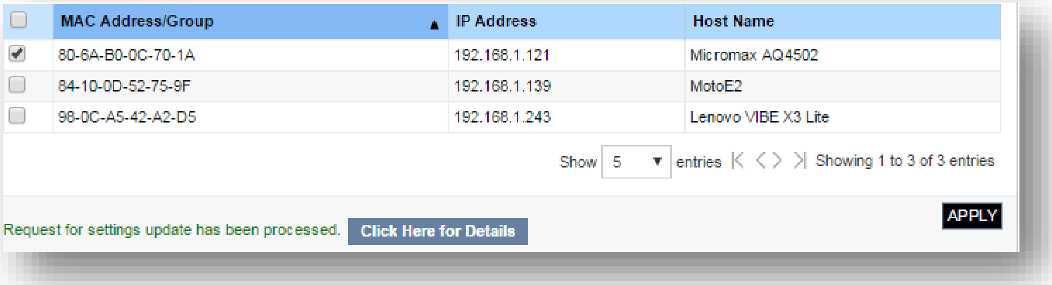
☐	MAC Address/Group ▲	IP Address	Host Name
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

7. Select one value from dropdown.
8. Select the required **Schedule Type**.
9. Under **Apply To** , select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree

10. From the table, select the check box against the required device/group.

11. Click **Apply**.
    The **Request for settings update processed** message is display.



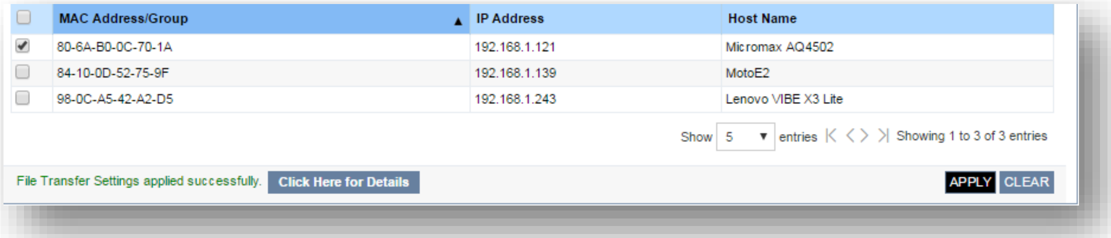
☐	MAC Address/Group ▲	IP Address	Host Name
☑	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Request for settings update has been processed.

Configuring Software Deployment

Creating a Task For File Transfer

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Software Deployment.**
5. Select **File Transfer**.
6. In **Target Folder Path**, enter the folder name where you want to upload the file.
7. Click the **file browser** icon to browse the file to be transferred.
8. Click **Upload** button to upload the selected file.
9. In **File Name**, the uploaded filename will be displayed.
10. Select the required **Schedule Type**.
11. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the File transfer settings
    b. **Group** – enables you to implement the File transfer settings to all devices in a group
12. From the table, select the check box against the required device/group.
13. Click **Apply**.
    The **Request for settings update processed** message is display.



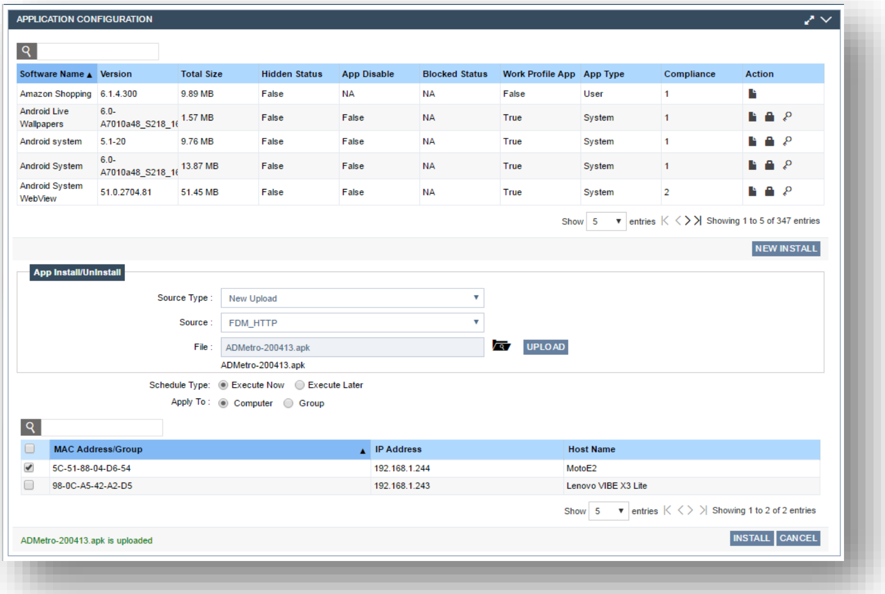
☐	MAC Address/Group ▲	IP Address	Host Name
☑	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

File Transfer Settings applied successfully.

Creating a Task for Application Configuration

In the devices tree, click the required group.

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android**
4. Click **Software Deployment**
5. Select **Application Configuration**
6. Select **New Install**.
7. In the **Source Type** list, select the required source.
8. In the **Source** list, select the required source.
9. In the **File** list, select the required apk for application installation.



APPLICATION CONFIGURATION

Software Name ▲	Version	Total Size	Hidden Status	App Disable	Blocked Status	Work Profile App	App Type	Compliance	Action
Amazon Shopping	6.1.4.300	9.89 MB	False	NA	NA	False	User	1	
Android Live Wallpapers	6.0-A7010a48_S218_16	1.57 MB	False	False	NA	True	System	1	
Android system	5.1-20	9.76 MB	False	False	NA	True	System	1	
Android System	6.0-A7010a48_S218_16	13.87 MB	False	False	NA	True	System	1	
Android System WebView	51.0.2704.81	51.45 MB	False	False	NA	True	System	2	

Show 5 entries Showing 1 to 5 of 347 entries

NEW INSTALL

App Install/UnInstall

Source Type : New Upload

Source : FDM_HTTP

File : ADMetro-200413.apk UPLOAD

ADMetro-200413.apk

Schedule Type: ● Execute Now ○ Execute Later

Apply To : ● Computer ○ Group

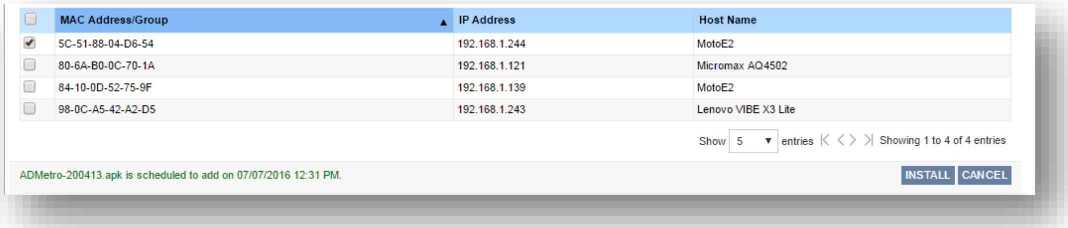
☐	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 2 of 2 entries

ADMetro-200413.apk is uploaded

INSTALL CANCEL

10. Select the required **Schedule Type**.
11. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the File transfer settings
    b. **Group** – enables you to implement the File transfer settings to all devices in a group
12. From the table, select the check box against the required device/group.
13. Click **Apply**.
    The **Request for settings update processed** message is display.



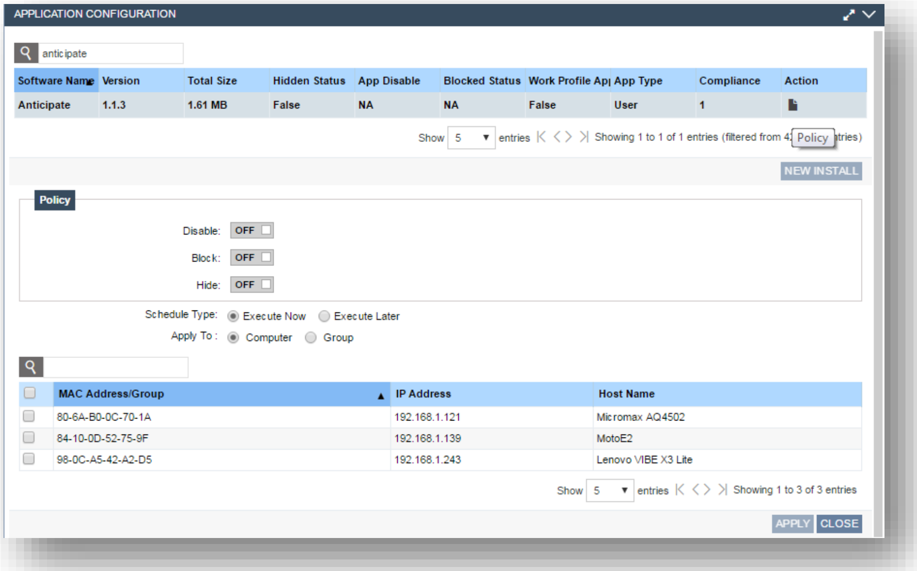
☐	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 4 of 4 entries

ADMetro-200413.apk is scheduled to add on 07/07/2016 12:31 PM.

Creating a Task to Configure Policy

1. From the toolbar, click Views ☰▾.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Software Deployment.**
5. Select **Application Configuration.**
6. Click an application & select **Policy.**



anticipate

Software Name	Version	Total Size	Hidden Status	App Disable	Blocked Status	Work Profile Ap|	App Type	Compliance	Action
Anticipate	1.1.3	1.61 MB	False	NA	NA	False	User	1	🗎

Show 5 ▾ entries |< < > >| Showing 1 to 1 of 1 entries (filtered from 4 Policy ntries)

Disable: OFF ☐

Block: OFF ☐

Hide: OFF ☐

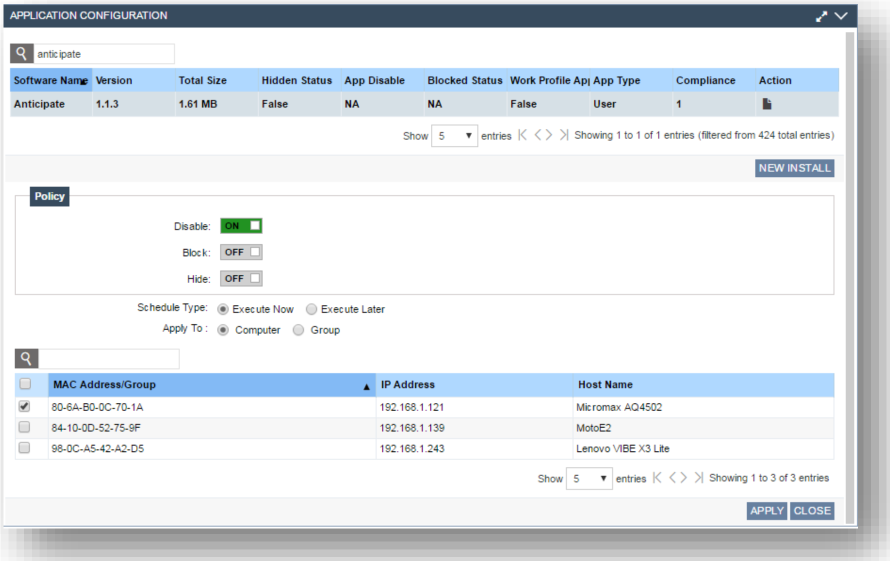
Schedule Type: ● Execute Now ○ Execute Later

Apply To : ● Computer ○ Group

☐	MAC Address/Group ▲	IP Address	Host Name
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries |< < > >| Showing 1 to 3 of 3 entries

7. Change the policy options of Disable, Block & Hide as required.



anticipate

Software Name	Version	Total Size	Hidden Status	App Disable	Blocked Status	Work Profile Ap|	App Type	Compliance	Action
Anticipate	1.1.3	1.61 MB	False	NA	NA	False	User	1	

Show 5 entries Showing 1 to 1 of 1 entries (filtered from 424 total entries)

Policy

Disable: ON

Block: OFF

Hide: OFF

Schedule Type: ● Execute Now ○ Execute Later

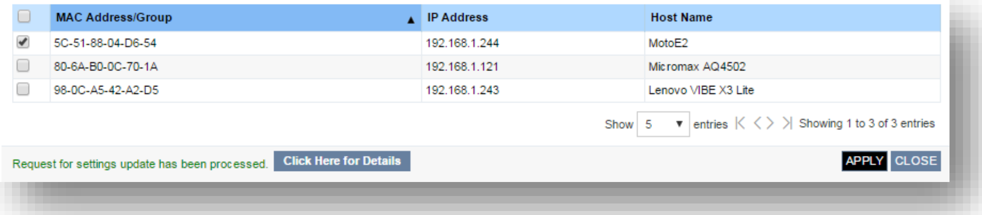
Apply To : ● Computer ○ Group

□	MAC Address/Group ▲	IP Address	Host Name
☑	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

8. Select the required **Schedule Type**.
9. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the File transfer settings
    b. **Group** – enables you to implement the File transfer settings to all devices in a group
10. From the table, select the check box against the required device/group.
11. Click **Apply**.

a. The **Request for settings update processed** message is display.



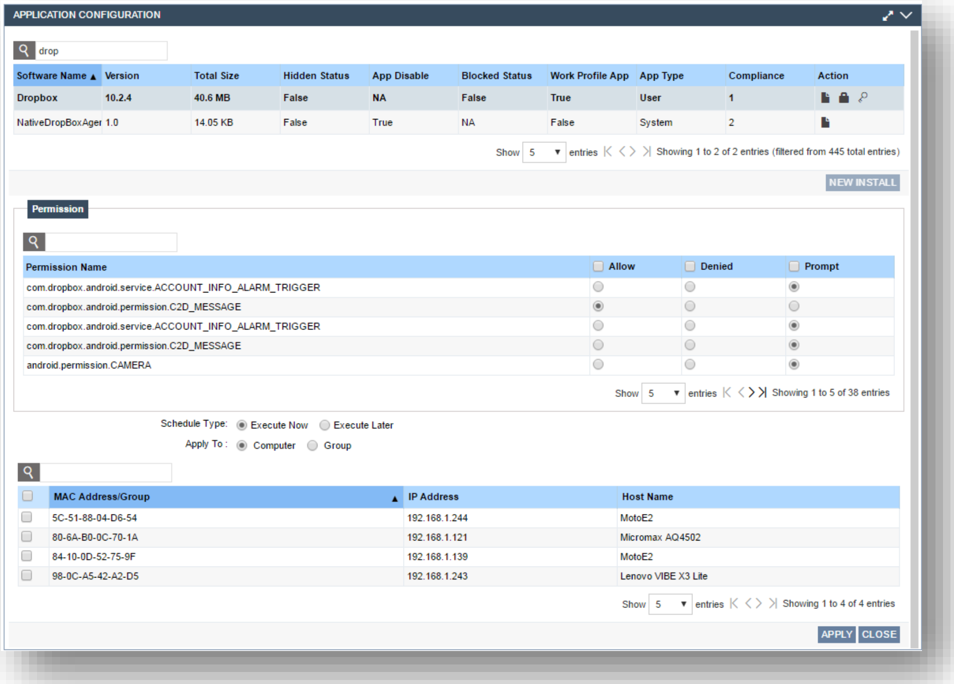
□	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 3 of 3 entries

Request for settings update has been processed.

Creating a Task to Configure Permission

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Software Deployment.**
5. Select **Application Configuration.**
6. Click an application & select **Permission.**



APPLICATION CONFIGURATION

drop

Software Name ▲	Version	Total Size	Hidden Status	App Disable	Blocked Status	Work Profile App	App Type	Compliance	Action
Dropbox	10.2.4	40.6 MB	False	NA	False	True	User	1	
NativeDropBoxAger	1.0	14.05 KB	False	True	NA	False	System	2	

Show 5 entries Showing 1 to 2 of 2 entries (filtered from 445 total entries)

Permission

Permission Name	□ Allow	□ Denied	□ Prompt
com.dropbox.android.service.ACCOUNT_INFO_ALARM_TRIGGER	○	○	●
com.dropbox.android.permission.C2D_MESSAGE	●	○	○
com.dropbox.android.service.ACCOUNT_INFO_ALARM_TRIGGER	○	○	●
com.dropbox.android.permission.C2D_MESSAGE	○	○	●
android.permission.CAMERA	○	○	●

Show 5 entries Showing 1 to 5 of 38 entries

Schedule Type: ● Execute Now ○ Execute Later

Apply To : ● Computer ○ Group

□	MAC Address/Group ▲	IP Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

7. List of permissions of the selected application will be displayed, if present.
8. Select the required option for the permission
9. Select the required **Schedule Type**.
10. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the File transfer settings
    b. **Group** – enables you to implement the File transfer settings to all devices in a group
11. From the table, select the check box against the required device/group.
12. Click **Apply**.

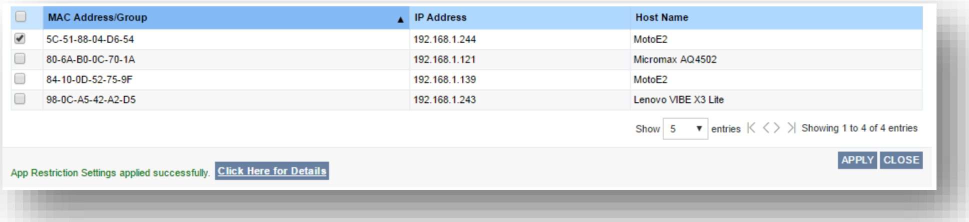
    The **Request for settings update processed** message is display.

Creating a Task to Configure Restriction

1. From the toolbar, click Views ☰.
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Software Deployment.**
5. Select **Application Configuration.**
6. Click an application & select **Restriction.**
7. List of restrictions of the selected application will be displayed, if present.
8. Click on **Edit** button to edit the restriction.

9. Select/edit the **value** as required.

10. Click on **Save** to save the changes.



□	MAC Address/Group ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries Showing 1 to 4 of 4 entries

App Restriction Settings applied successfully.

11. Select the required Schedule Type.

12. Under **Apply To** , select any one of the following:

    a. **Computer** – enables you to select a device and implement the Restriction settings

    b. **Group** – enables you to implement the Restriction settings to all devices in a group

13. From the table, select the check box against the required device/group.

14. Click **Apply**.

    The **Request for settings applied successfully** message is display.

Configuring Manage Profile Policy

Creating Tasks to Profile Policy

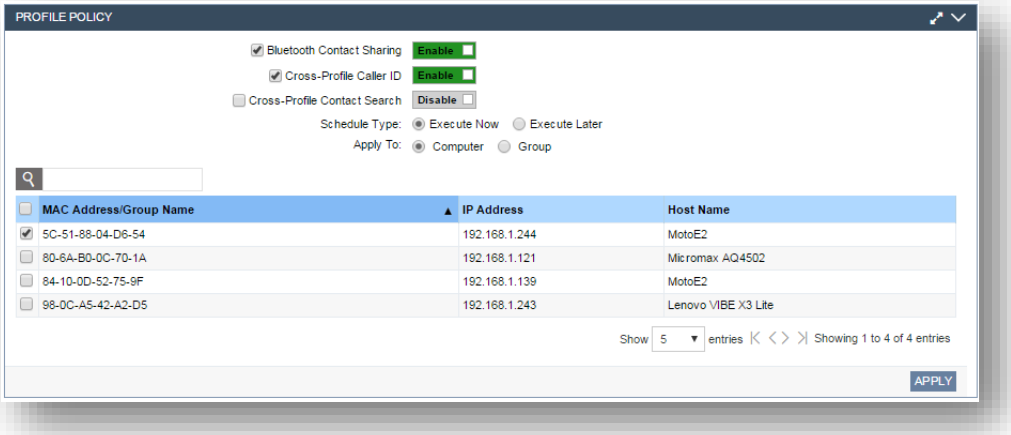
1. From the toolbar, click Views ☰⌄.
   Click on Task Management. The **Task Management** page is displayed.

2. Expand the right menu.

3. Click **Android.**

4. Click **Manage Profile Policy.**

5. Select **Profile Policy.**



PROFILE POLICY

☑ Bluetooth Contact Sharing Enable

☑ Cross-Profile Caller ID Enable

☐ Cross-Profile Contact Search Disable

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

☐	MAC Address/Group Name ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

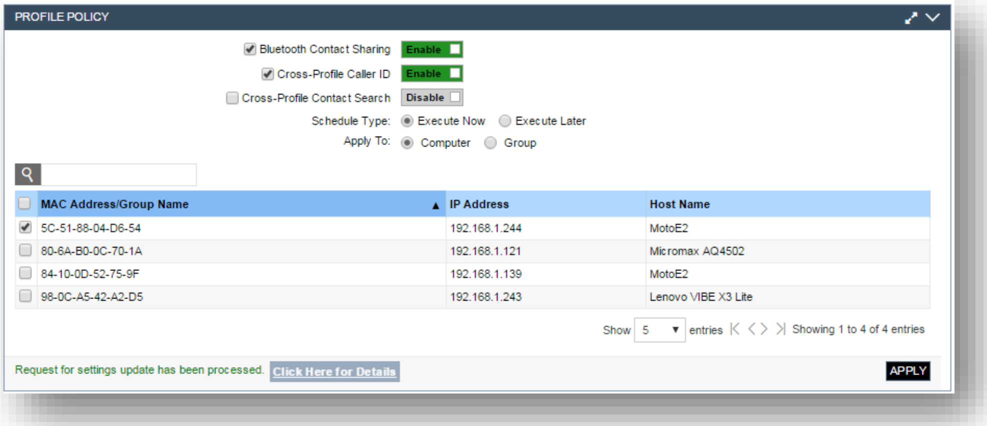
Show 5 entries Showing 1 to 4 of 4 entries

APPLY

6. Select the required **Schedule Type**.
7. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the settings
    b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
8. From the table, select the check box against the required device/group.

9. Click **Apply**.

   The **Request for settings update processed** message is display.



PROFILE POLICY

☑ Bluetooth Contact Sharing Enable

☑ Cross-Profile Caller ID Enable

☐ Cross-Profile Contact Search Disable

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

☐	MAC Address/Group Name ▲	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
☐	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
☐	84-10-0D-52-75-9F	192.168.1.139	MotoE2
☐	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

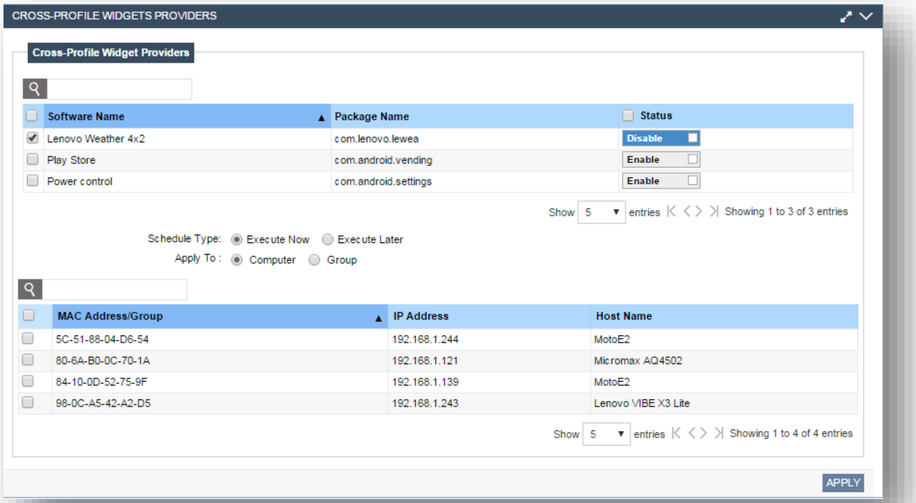
Request for settings update has been processed. Click Here for Details

APPLY

Creating Tasks to Cross Profile Widget Providers

1. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**

4. Click **Manage Profile Policy.**
5. Select **Cross Profile Widget Providers**.
6. Select an **Application**.
7. Toggle the Enable/Disable button against the application as required.



CROSS-PROFILE WIDGETS PROVIDERS

Cross-Profile Widget Providers

□	Software Name ▲	Package Name	□ Status
☑	Lenovo Weather 4x2	com.lenovo.lewea	Disable
□	Play Store	com.android.vending	Enable
□	Power control	com.android.settings	Enable

Show 5 entries Showing 1 to 3 of 3 entries

Schedule Type: ● Execute Now ○ Execute Later

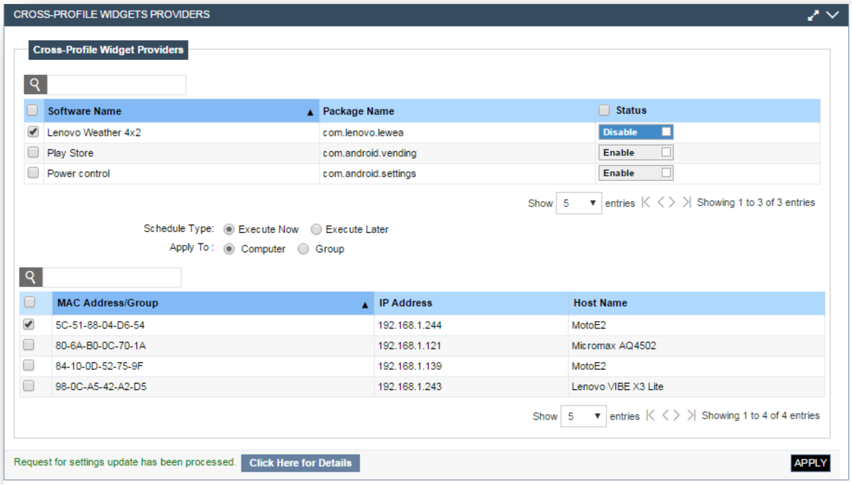
Apply To : ● Computer ○ Group

□	MAC Address/Group ▲	IP Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

8. Select the required **Schedule Type**.
9. Under **Apply To** , select any one of the following:
   a. **Computer** – enables you to select a device and implement the settings
   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree
10. Click **Apply**.

    The **Request for settings update processed** message is displayed.



CROSS-PROFILE WIDGETS PROVIDERS

Cross-Profile Widget Providers

□	Software Name	Package Name	□ Status
☑	Lenovo Weather 4x2	com.lenovo.lewea	Disable
□	Play Store	com.android.vending	Enable
□	Power control	com.android.settings	Enable

Show 5 entries Showing 1 to 3 of 3 entries

Schedule Type: ● Execute Now ○ Execute Later

Apply To : ● Computer ○ Group

□	MAC Address/Group	IP Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

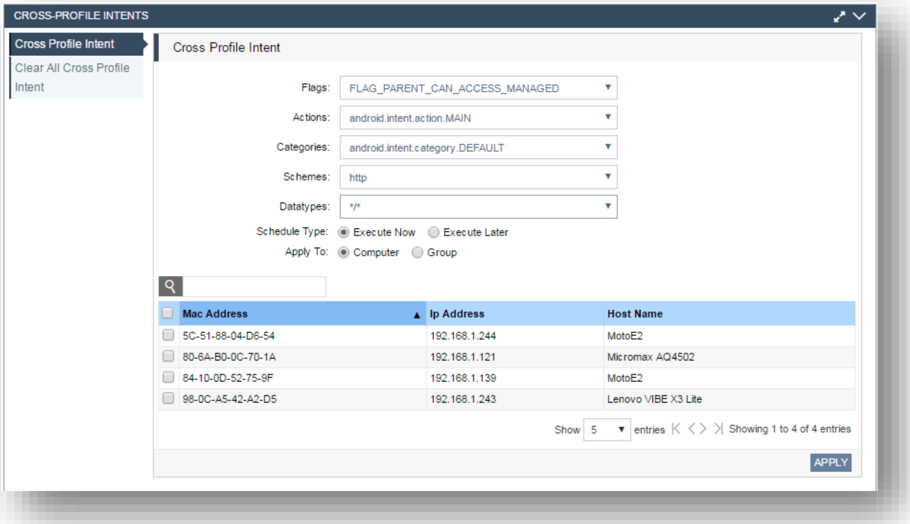
Show 5 entries Showing 1 to 4 of 4 entries

Request for settings update has been processed. Click Here for Details APPLY

Creating Tasks to Cross Profile Intent

Configuring Cross Profile Intent

1. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.
2. Expand the right menu.
3. Click **Android.**
4. Click **Manage Profile Policy.**
5. Select **Cross Profile Intents**.
6. Select value of **Flags**, **Actions**, **Categories**, **Schemes** and **Datatypes** as required.



CROSS-PROFILE INTENTS

Cross Profile Intent

Clear All Cross Profile Intent

Cross Profile Intent

Flags: FLAG_PARENT_CAN_ACCESS_MANAGED

Actions: android.intent.action.MAIN

Categories: android.intent.category.DEFAULT

Schemes: http

Datatypes: */*

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	Mac Address	Ip Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

APPLY

7. Select the required **Schedule Type**.

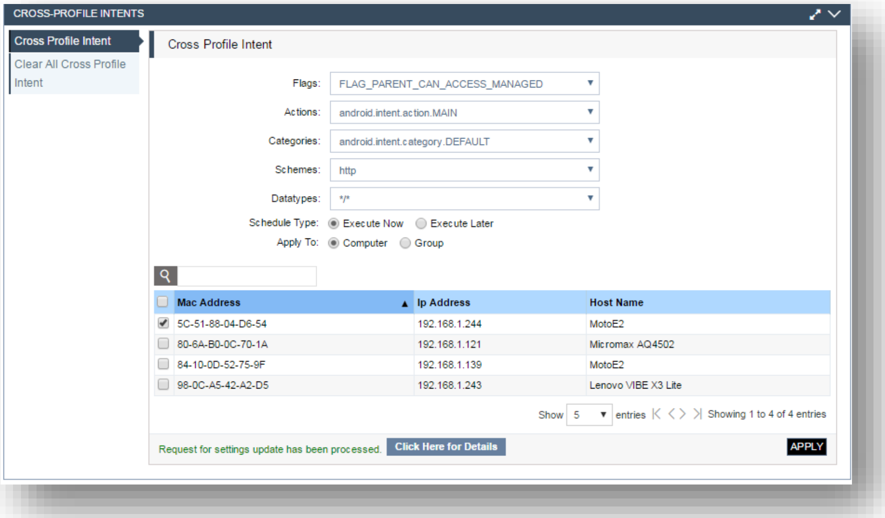
8. Under **Apply To** , select any one of the following:

    a. **Computer** – enables you to select a device and implement the settings

    b. **Group** – enables you to implement the settings to all devices in a group on the devices tree

9. Click **Apply**.

   The **Request for settings update processed** message is display



Flags: FLAG_PARENT_CAN_ACCESS_MANAGED ▾

Actions: android.intent.action.MAIN ▾

Categories: android.intent.category.DEFAULT ▾

Schemes: http ▾

Datatypes: */* ▾

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	Mac Address ▲	Ip Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 ▾ entries Showing 1 to 4 of 4 entries

Request for settings update has been processed. Click Here for Details

APPLY

Creating Tasks to Clear All Cross Profile Intents

1. From the toolbar, click Views .
   Click on Task Management. The **Task Management** page is displayed.

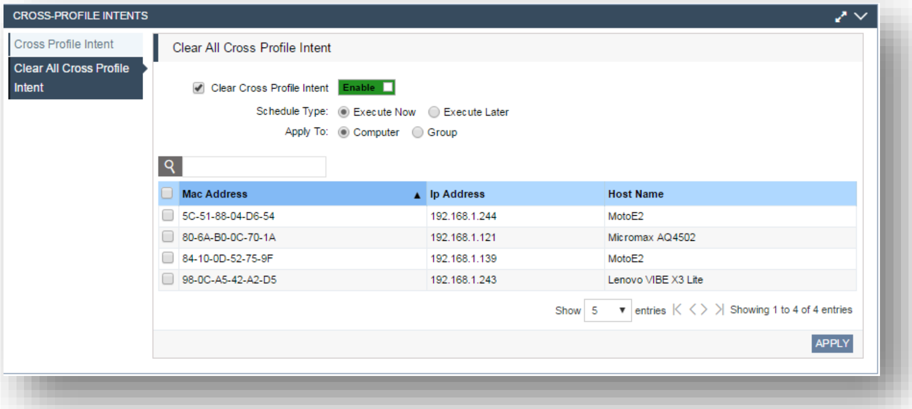
2. Expand the right menu.

3. Click **Android.**

4. Click **Manage Profile Policy.**

5. Select **Cross Profile Intents**.
6. Click on **Clear All Cross Profile Intents**.

7. Enable/Disable the value as required.



CROSS-PROFILE INTENTS

- Cross Profile Intent
- Clear All Cross Profile Intent

Clear All Cross Profile Intent

☑ Clear Cross Profile Intent Enable

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	Mac Address	Ip Address	Host Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

APPLY

8. Select the required **Schedule Type**.

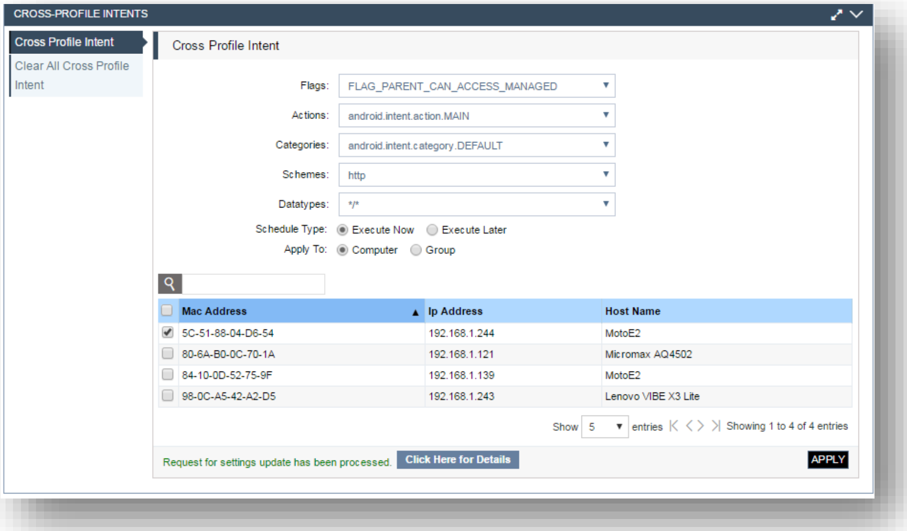
9. Under **Apply To** , select any one of the following:

   a. **Computer** – enables you to select a device and implement the settings

   b. **Group** – enables you to implement the settings to all devices in a group on the devices tree

10. Click **Apply**.

    The **Request for settings update processed** message is display.



CROSS-PROFILE INTENTS

- Cross Profile Intent
- Clear All Cross Profile Intent

Cross Profile Intent

Flags: FLAG_PARENT_CAN_ACCESS_MANAGED

Actions: android.intent.action.MAIN

Categories: android.intent.category.DEFAULT

Schemes: http

Datatypes: */*

Schedule Type: ● Execute Now ○ Execute Later

Apply To: ● Computer ○ Group

□	Mac Address	Ip Address	Host Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite

Show 5 entries Showing 1 to 4 of 4 entries

Request for settings update has been processed. Click Here for Details

APPLY

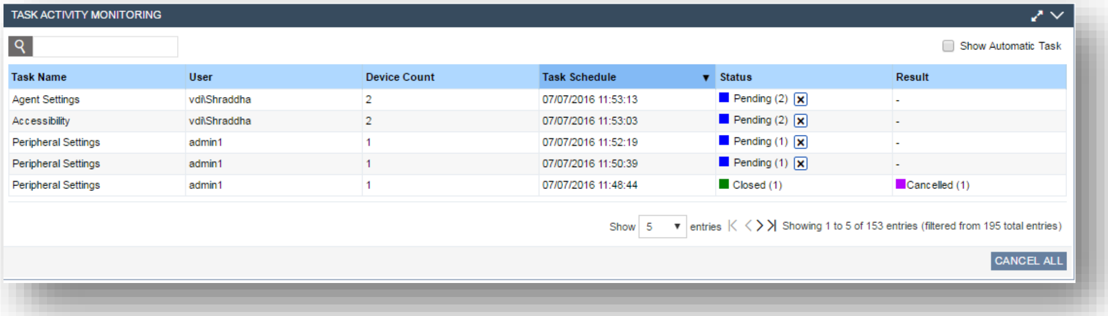
Monitoring Tasks

Fusion EMM enables you to record and archive the tasks that have been performed as a part of the management process. You can also examine the tasks on a granular basis when required to indicate why tasks may have failed.

As the name suggests, the **Task Manager** is used to monitor the status of the executed tasks. It displays the task name, the user id through which it is executed, the duration for the completion of settings, and the reason if any setting fails.

To monitor a task

1. From the toolbar, click ☰.
   The **Task Management** page is display.
2. Expand the right menu.
3. Click **Android.**
4. Click **Task Management** and click **Task Monitoring Activity**.



TASK ACTIVITY MONITORING

□ Show Automatic Task

Task Name	User	Device Count	Task Schedule ▼	Status	Result
Agent Settings	vdi\Shraddha	2	07/07/2016 11:53:13	🟦 Pending (2) ☒	-
Accessibility	vdi\Shraddha	2	07/07/2016 11:53:03	🟦 Pending (2) ☒	-
Peripheral Settings	admin1	1	07/07/2016 11:52:19	🟦 Pending (1) ☒	-
Peripheral Settings	admin1	1	07/07/2016 11:50:39	🟦 Pending (1) ☒	-
Peripheral Settings	admin1	1	07/07/2016 11:48:44	🟩 Closed (1)	🟪Cancelled (1)

Show 5 ▾ entries |< < > >| Showing 1 to 5 of 153 entries (filtered from 195 total entries)

CANCEL ALL

To view the list of automatic tasks, select the **Show Automatic Task** check box.

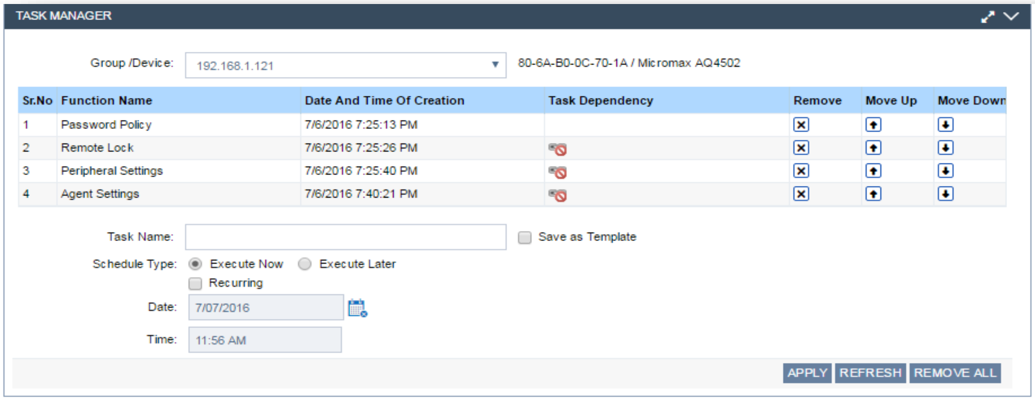
Using the Task Manager

The **Task Manager** displays all the settings that are assigned the **Schedule Type** as **Execute Later**. You can apply multiple settings to multiple devices instantly by selecting the **Schedule Type** as **Execute Later**. You can also view the list of tasks that are pending execution and execute the pending tasks.

Viewing Pending Tasks

1. From the toolbar, click ☰.
   The **Task Management** page is display.
2. Expand the right menu.
3. Click **Android**

4. Click **Task Management** and click **Task Manager**.



Group /Device: 192.168.1.121 ▾ 80-6A-B0-0C-70-1A / Micromax AQ4502

Sr.No	Function Name	Date And Time Of Creation	Task Dependency	Remove	Move Up	Move Down
1	Password Policy	7/6/2016 7:25:13 PM		☒	↑	↓
2	Remote Lock	7/6/2016 7:25:26 PM	⊘	☒	↑	↓
3	Peripheral Settings	7/6/2016 7:25:40 PM	⊘	☒	↑	↓
4	Agent Settings	7/6/2016 7:40:21 PM	⊘	☒	↑	↓

Task Name: □ Save as Template

Schedule Type: ● Execute Now ○ Execute Later

□ Recurring

Date: 7/07/2016

Time: 11:56 AM

Executing Pending Tasks

1. From the toolbar, click ☰.

   The **Task Management** page is display.

2. Expand the right menu.

3. Click **Android**

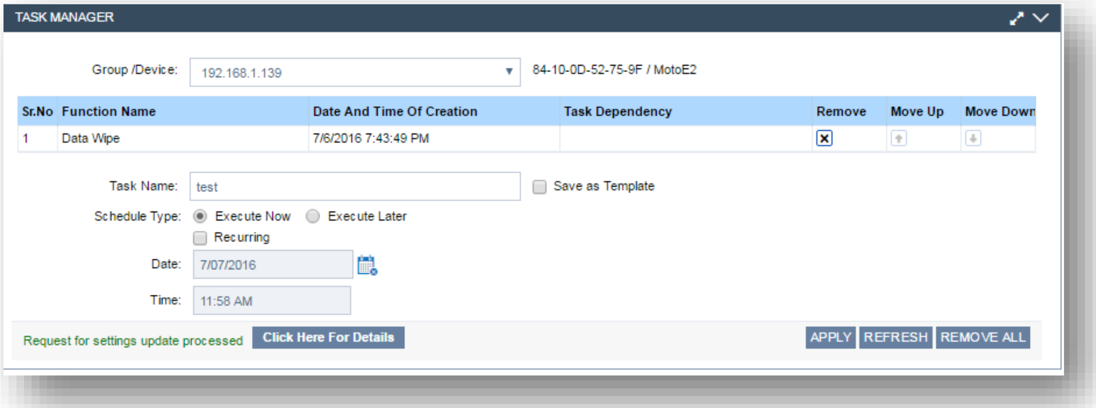
4. Click **Task Management** and click **Task Manager**.

5. In the **Task Name** box, enter the name of the task.

6. Select the required **Schedule Type**.

> The task name must be the same as the function name.

7. Click **Apply**.
   The **Request for settings update processed** message is display


TASK MANAGER

Group /Device: 192.168.1.139 ▾ 84-10-0D-52-75-9F / MotoE2

Sr.No	Function Name	Date And Time Of Creation	Task Dependency	Remove	Move Up	Move Down
1	Data Wipe	7/6/2016 7:43:49 PM		☒	↑	↓

Task Name: test □ Save as Template

Schedule Type: ● Execute Now ○ Execute Later

□ Recurring

Date: 7/07/2016

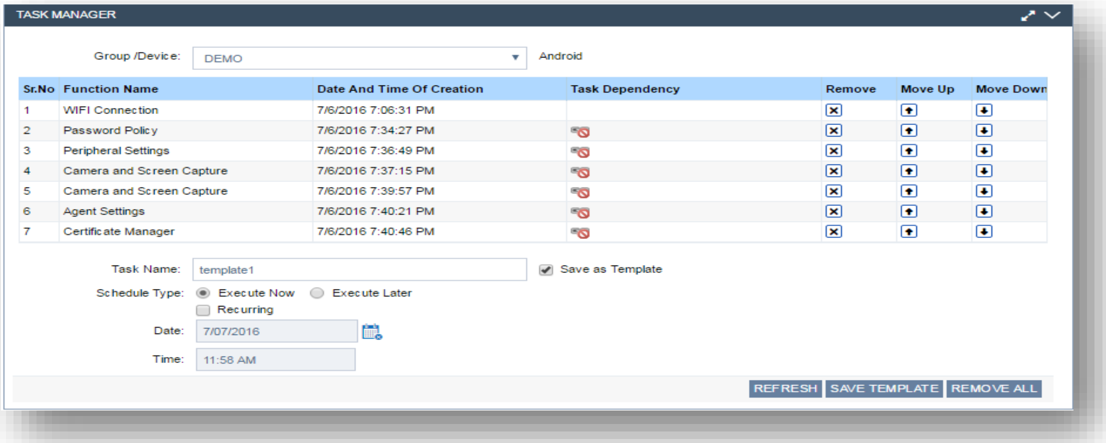
Time: 11:58 AM

Request for settings update processed

Using the Template Manager

Creating a Template

1. From the toolbar, click .
   The **Task Management** page is display.
2. Expand the right menu.
3. Click **Android**
4. Click **Task Management** and click **Task Manager**.


TASK MANAGER

Group /Device: DEMO ▾ Android

Sr.No	Function Name	Date And Time Of Creation	Task Dependency	Remove	Move Up	Move Down
1	WIFI Connection	7/6/2016 7:06:31 PM		☒	↑	↓
2	Password Policy	7/6/2016 7:34:27 PM	🔗	☒	↑	↓
3	Peripheral Settings	7/6/2016 7:36:49 PM	🔗	☒	↑	↓
4	Camera and Screen Capture	7/6/2016 7:37:15 PM	🔗	☒	↑	↓
5	Camera and Screen Capture	7/6/2016 7:39:57 PM	🔗	☒	↑	↓
6	Agent Settings	7/6/2016 7:40:21 PM	🔗	☒	↑	↓
7	Certificate Manager	7/6/2016 7:40:46 PM	🔗	☒	↑	↓

Task Name: template1 ☑ Save as Template

Schedule Type: ● Execute Now ○ Execute Later

□ Recurring

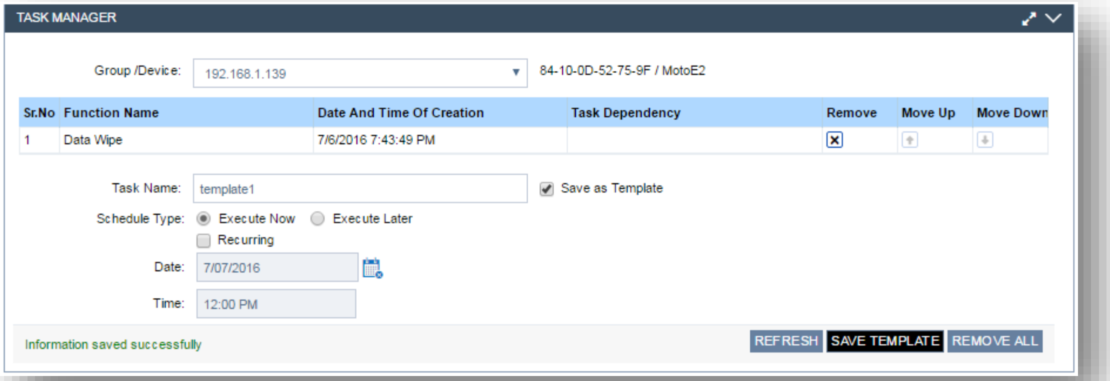
Date: 7/07/2016

Time: 11:58 AM

5. In the **Task Name** box, enter the name of the task.

The task name must be the same as the function name.

6. Select the **Save as Template** check box.
   The **Apply** button changes to **Save Template**.
7. Select the required **Schedule Type**.
8. Click **Save Template**.
   The **Information saved successfully** message is display.



TASK MANAGER

Group /Device: 192.168.1.139 ▾ 84-10-0D-52-75-9F / MotoE2

Sr.No	Function Name	Date And Time Of Creation	Task Dependency	Remove	Move Up	Move Down
1	Data Wipe	7/6/2016 7:43:49 PM		☒	↑	↓

Task Name: template1 ☑ Save as Template

Schedule Type: ● Execute Now ○ Execute Later

□ Recurring

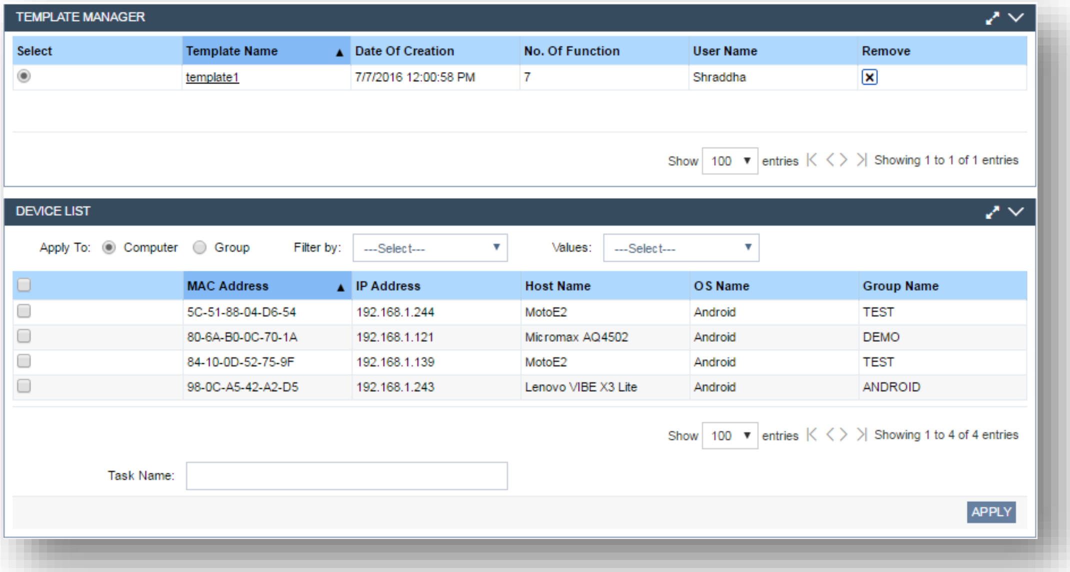
Date: 7/07/2016

Time: 12:00 PM

Information saved successfully

Applying a Template

1. From the toolbar, click ☰.
   The **Task Management** page is display.
2. Expand the right menu.
3. Click **Android.**
4. Click **Task Management** and click **Template Manager**.



TEMPLATE MANAGER

Select	Template Name ▲	Date Of Creation	No. Of Function	User Name	Remove
●	template1	7/7/2016 12:00:58 PM	7	Shraddha	☒

Show 100 ▾ entries Showing 1 to 1 of 1 entries

DEVICE LIST

Apply To: ● Computer ○ Group Filter by: ---Select--- ▾ Values: ---Select--- ▾

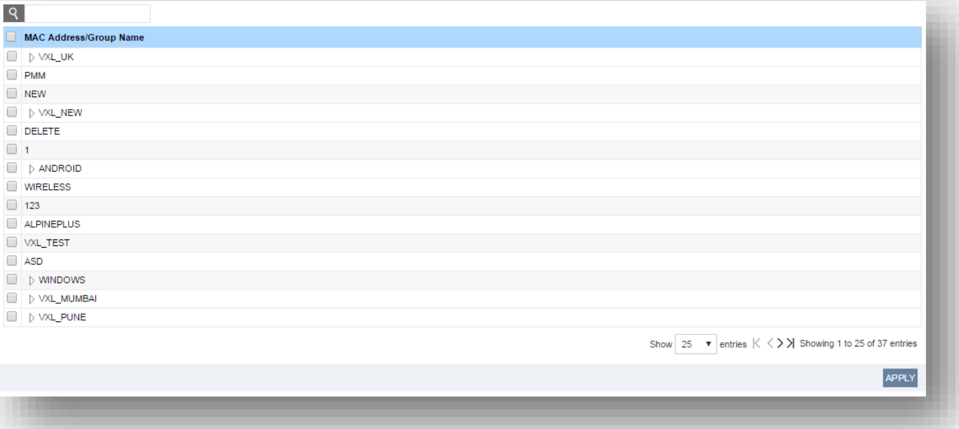
□	MAC Address ▲	IP Address	Host Name	OS Name	Group Name
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	TEST
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502	Android	DEMO
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2	Android	TEST
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite	Android	ANDROID

Show 100 ▾ entries Showing 1 to 4 of 4 entries

Task Name:

5. Select the required template.
6. Under **Apply To** , select any one of the following:
    a. **Computer** – enables you to select a device and implement the settings
    b. **Groups:** enables you to implement the settings to all devices in a group on the devices tree.

- On selecting option, Group in Apply to, groups along with hierarchy structure if present will be display.
- All subgroup present under those groups will be list out.
- If user select parent group all child group should get select.
- This Group Hierarchy feature not implemented for all modules.

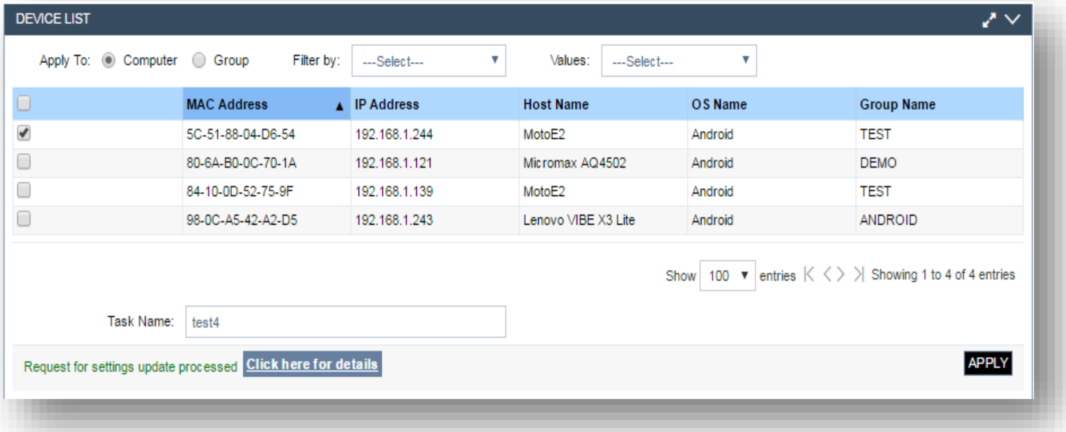


□	MAC Address/Group Name
□	▷ VXL_UK
□	PMM
□	NEW
□	▷ VXL_NEW
□	DELETE
□	1
□	▷ ANDROID
□	WIRELESS
□	123
□	ALPINEPLUS
□	VXL_TEST
□	ASD
□	▷ WINDOWS
□	▷ VXL_MUMBAI
□	▷ VXL_PUNE

Show 25 entries Showing 1 to 25 of 37 entries

b.

7. From the table, select the check box against the required device.
8. In the **Task Name** box, enter the name of the template.
9. Click **Apply**.
   The **Request for settings update processed** message is display.



DEVICE LIST

Apply To: ● Computer ○ Group Filter by: ---Select--- Values: ---Select---

□	MAC Address	IP Address	Host Name	OS Name	Group Name
☑	5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	TEST
□	80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502	Android	DEMO
□	84-10-0D-52-75-9F	192.168.1.139	MotoE2	Android	TEST
□	98-0C-A5-42-A2-D5	192.168.1.243	Lenovo VIBE X3 Lite	Android	ANDROID

Show 100 entries Showing 1 to 4 of 4 entries

Task Name: test4

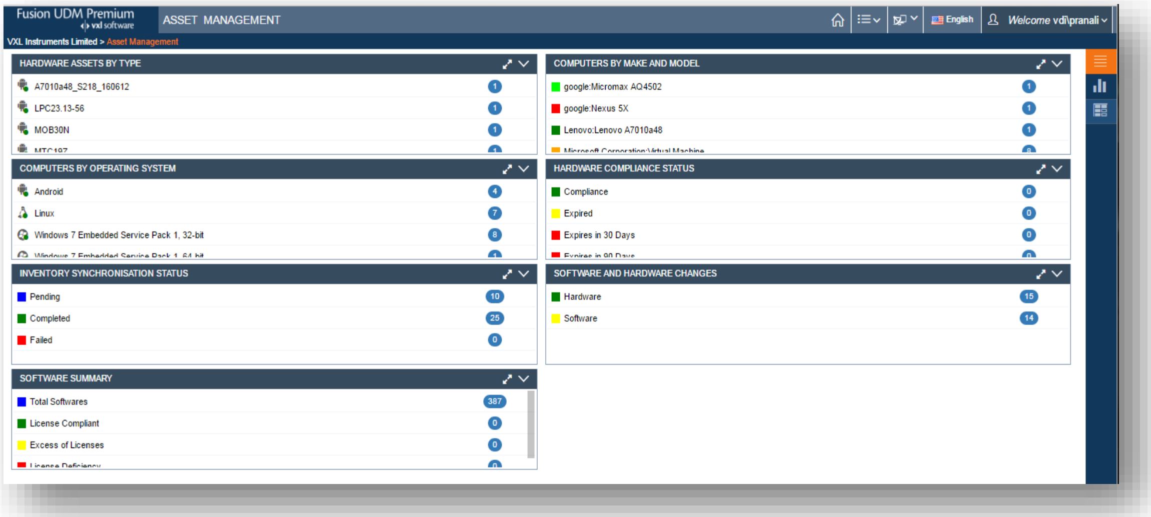
Request for settings update processed Click here for details

Asset Management

The **Asset Management** page helps you to monitor software and hardware assets for all devices, discovered and registered with Fusion EMM . It enables you to track the location of assets in the organization. User can see just the software and hardware inventory or how they are deployed.

To open the **Asset Management** page

1. Click on the toolbar.
2. The **Asset Management** page is display. By default, the page displays a dashboard with the summary of hardware and software assets in use and their status.



HARDWARE ASSETS BY TYPE	
A7010a48_S218_160612	1
LPC23.13-56	1
MOB30N	1
MTC197	1

COMPUTERS BY MAKE AND MODEL	
🟩 google:Micromax AQ4502	1
🟥 google:Nexus 5X	1
🟩 Lenovo:Lenovo A7010a48	1
🟧 Microsoft Corporation:Virtual Machine	8

COMPUTERS BY OPERATING SYSTEM	
Android	4
Linux	7
Windows 7 Embedded Service Pack 1, 32-bit	8
Windows 7 Embedded Service Pack 1, 64-bit	1

HARDWARE COMPLIANCE STATUS	
🟩 Compliance	0
🟨 Expired	0
🟥 Expires in 30 Days	0
🟥 Expires in 90 Days	0

INVENTORY SYNCHRONISATION STATUS	
🟦 Pending	10
🟩 Completed	25
🟥 Failed	0

SOFTWARE AND HARDWARE CHANGES	
🟩 Hardware	15
🟨 Software	14

SOFTWARE SUMMARY	
🟦 Total Softwares	387
🟩 License Compliant	0
🟨 Excess of Licenses	0
🟥 License Deficiency	0

3. Using the dashboard, you can check software and hardware inventory as well as any modifications made to the same, in a report format.

- **Hardware Assets by Type:** Displays the different categories of hardware assets within Fusion EMM .

  The categories are as follows:

  - iOS
  - Android

- **Computers by Operating System:** Displays devices based on their operating systems.

  Fusion EMM can manage and monitor devices with the following types of operating systems:

  - iOS
  - Android

- **Inventory Scan Status:** Displays all updates and modifications on the device side. Device inventory is scanned and updated on the Fusion EMM server on an hourly basis.

  The scanning status is as follows:

  - Pending: number of devices to be scanned
  - Complete: number of devices scanned successfully
  - Failed: number of devices where the scan failed

- **Computers by Make and Model:** Displays manufacturer details for a device.
- **Hardware Compliance Status:** Displays the warranty status of all hardware entered in the repository.

  The warranty status, classification is as follows:

  - Compliance: Hardware within warranty period
  - Expired: Hardware with expired warranty
  - Expiry in 30 Days: Hardware with 30 days' warranty remaining
  - Expiry in 90 Days: Hardware with 90 days' warranty remaining

For warranty details to display **in Hardware Compliance Status**, you must add hardware to the inventory in **Hardware Inventory** in **Inventory Settings**.

For information about adding hardware to the inventory, see "Adding a Hardware to the Inventory" in "Asset Management".

- **Software Summary:** Enables you to track client wise software usages. Using the software metering feature of Fusion EMM , you can monitor the number of licenses being used by the devices connected to Fusion EMM .

  Software metering helps to ensure the following:

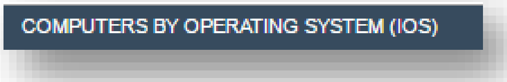
  - The client organization's usage of specific software does not go beyond the number of purchased licenses.
  - Software usage is accurately monitored and logged in so the client does not purchase more licences than required.

  Software Summary displays the following details:

  - Total Software: Total number of software installed on devices
  - License Compliant: Software with valid license
  - Excess of Licenses: Number of licenses purchased exceeds the number of licensed used
  - License Deficiency: Number of used licenses exceeds the number of purchased licensed

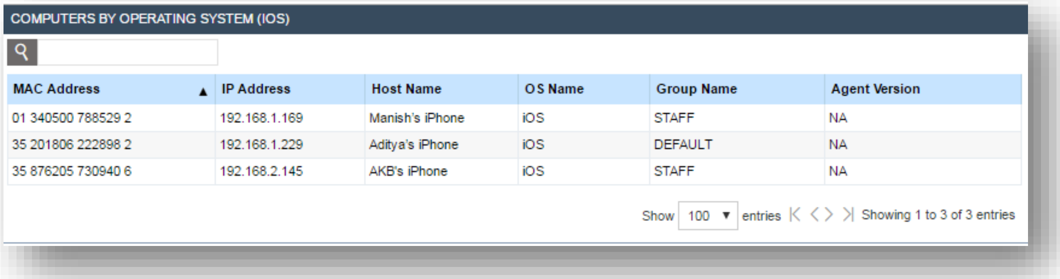
For software details to display in **Software Summary**, you must add a software to the inventory in **Software Inventory** in **Inventory Settings**.

To view details of any particular asset:



COMPUTERS BY OPERATING SYSTEM (IOS)

- On the dashboard, in the **Computers by operating system** report, click the number in bracket. A page with the details of the selected asset is display.



COMPUTERS BY OPERATING SYSTEM (IOS)

MAC Address ▲	IP Address	Host Name	OS Name	Group Name	Agent Version
01 340500 788529 2	192.168.1.169	Manish's iPhone	iOS	STAFF	NA
35 201806 222898 2	192.168.1.229	Aditya's iPhone	iOS	DEFAULT	NA
35 876205 730940 6	192.168.2.145	AKB's iPhone	iOS	STAFF	NA

Show 100 ▾ entries Showing 1 to 3 of 3 entries

Viewing Software and Hardware Details

Toolbar

📄 📊 🖨	To view or export data in PDF, Excel format or print list view
⤢	Maximize screen
⌄	Expand Screen
⤡	Minimize screen

⌃	Collapse Screen
▼	Advanced Filter
⟳	Refresh report
✉	Email report to configured mail id.
↗	Open in popup.
☰	Show / Hide column

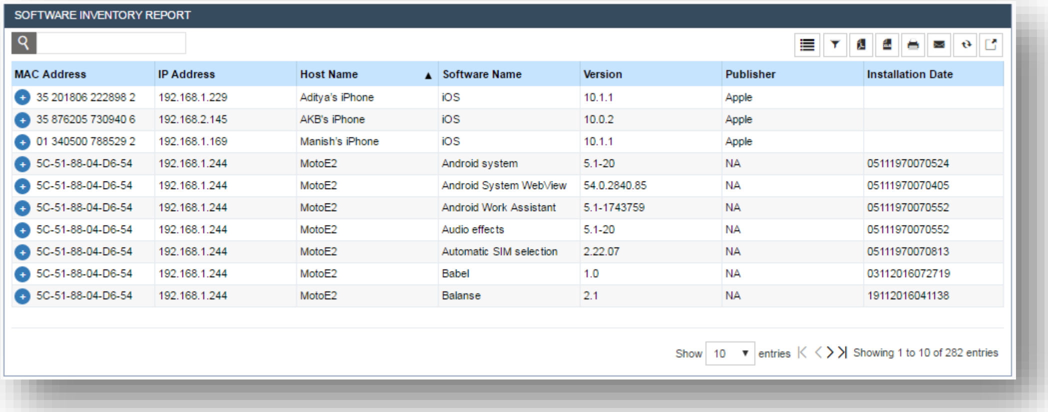
Software Inventory Report

The **Software Inventory Report** displays the details of the software installed on individual hosts and on all devices and nodes registered in the Fusion EMM server.

> *To email the report to client user ids, you need to configure the SMTP server settings.*
>
> *For information about configuring SMTP server settings , see "Working with Mailer Engine Configuration" in " Configuring Fusion EMM".*

To view the Software Inventory Report

1. Expand the right menu
2. Click **Asset Management**, then **click Software and Hardware Details**, and then click **Software Inventory Report**.



SOFTWARE INVENTORY REPORT

MAC Address	IP Address	Host Name	Software Name	Version	Publisher	Installation Date
35 201806 222898 2	192.168.1.229	Aditya's iPhone	iOS	10.1.1	Apple	
35 876205 730940 6	192.168.2.145	AKB's iPhone	iOS	10.0.2	Apple	
01 340500 788529 2	192.168.1.169	Manish's iPhone	iOS	10.1.1	Apple	
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android system	5.1-20	NA	05111970070524
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android System WebView	54.0.2840.85	NA	05111970070405
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android Work Assistant	5.1-1743759	NA	05111970070552
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Audio effects	5.1-20	NA	05111970070552
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Automatic SIM selection	2.22.07	NA	05111970070813
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Babel	1.0	NA	03112016072719
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Balanse	2.1	NA	19112016041138

Show 10 entries Showing 1 to 10 of 282 entries

3. The **Licenses** column displays the type of software, as selected when adding the software to the inventory.
4. The software type selection included the following options:

   a. Licensed (Perpetual)

   b. Licensed (Yearly/Cloud)

   c. Evaluation

   d. Open Source

   e. None

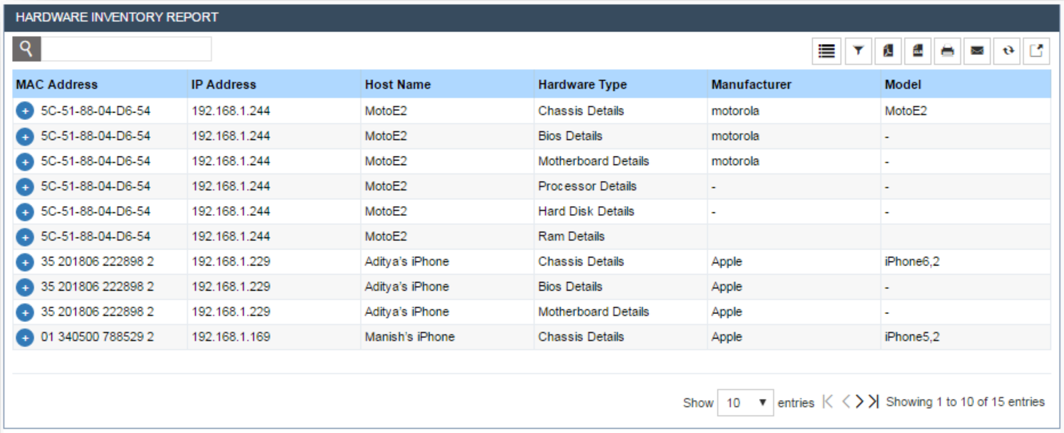
For information about adding software to the inventory, see "Adding a Software to the Inventory" in " Configuring Fusion EMM".

Hardware Inventory Report

The **Hardware Inventory Report** displays the details of the hardware available on individual hosts.

To view the Hardware Inventory Report

1. Expand the right menu
2. Click **Asset Management**, then click **Software and Hardware Details**, and then click **Hardware Inventory Report**.



HARDWARE INVENTORY REPORT

MAC Address	IP Address	Host Name	Hardware Type	Manufacturer	Model
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Chassis Details	motorola	MotoE2
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Bios Details	motorola	-
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Motherboard Details	motorola	-
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Processor Details	-	-
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Hard Disk Details	-	-
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Ram Details		
35 201806 222898 2	192.168.1.229	Aditya's iPhone	Chassis Details	Apple	iPhone6,2
35 201806 222898 2	192.168.1.229	Aditya's iPhone	Bios Details	Apple	-
35 201806 222898 2	192.168.1.229	Aditya's iPhone	Motherboard Details	Apple	-
01 340500 788529 2	192.168.1.169	Manish's iPhone	Chassis Details	Apple	iPhone5,2

Show 10 entries Showing 1 to 10 of 15 entries

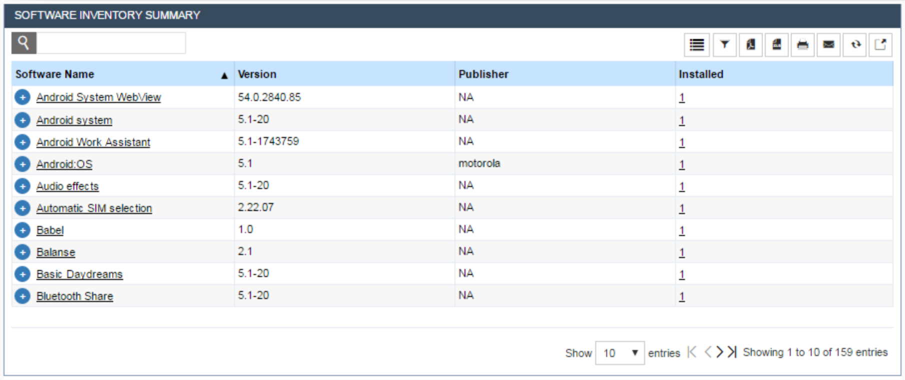
Viewing Software and Hardware Summary

Software Inventory Summary

The **Software Inventory Summary** displays licensing and installation details of the software available in the organization.

To view the Software Inventory Summary

1. Expand the right menu
2. Click **Asset Management**, and then click **Software and Hardware Summary**, and then click **Software Inventory Summary**.



SOFTWARE INVENTORY SUMMARY

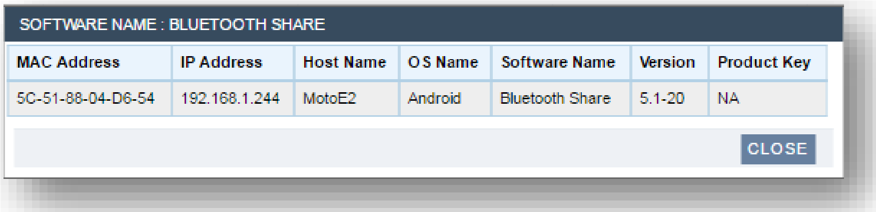
Software Name ▲	Version	Publisher	Installed
Android System WebView	54.0.2840.85	NA	1
Android system	5.1-20	NA	1
Android Work Assistant	5.1-1743759	NA	1
Android:OS	5.1	motorola	1
Audio effects	5.1-20	NA	1
Automatic SIM selection	2.22.07	NA	1
Babel	1.0	NA	1
Balanse	2.1	NA	1
Basic Daydreams	5.1-20	NA	1
Bluetooth Share	5.1-20	NA	1

Show 10 entries Showing 1 to 10 of 159 entries

License Details

To view the details of the licenses

1. In the **Purchased** column, click the displayed number.
2. The details of the licenses purchased for that software are displayed.



SOFTWARE NAME : BLUETOOTH SHARE

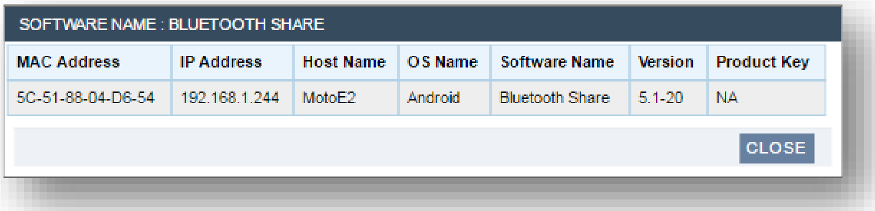
MAC Address	IP Address	Host Name	OS Name	Software Name	Version	Product Key
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	Bluetooth Share	5.1-20	NA

3. Click **Close**.

Installation Details

To view details of the system where the software is installed

1. In the **Installed** column, click the number for the software.
   A pop-up displays the license details.



SOFTWARE NAME : BLUETOOTH SHARE

MAC Address	IP Address	Host Name	OS Name	Software Name	Version	Product Key
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	Bluetooth Share	5.1-20	NA

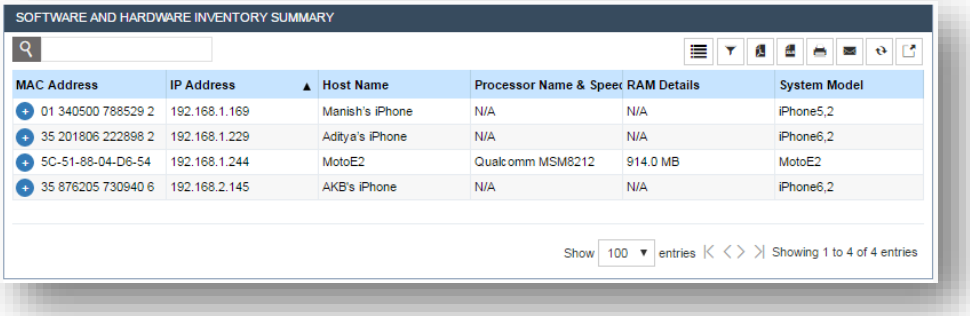
2. Click **Close**.

Software and Hardware Inventory Summary

The Software and Hardware Inventory Summary displays the hardware available on each host as well as details of the operating system, anti-virus and Microsoft Office installations.

To view the Software Inventory Summary

1. Expand the right menu
2. Click **Asset Management**, and then click **Software and Hardware Inventory Summary**.

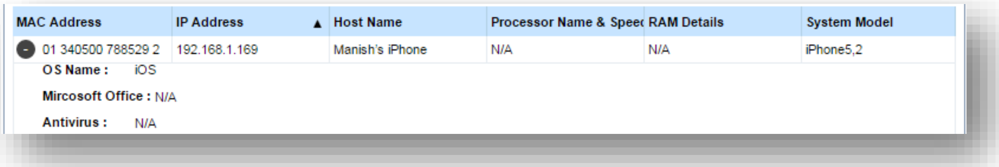

SOFTWARE AND HARDWARE INVENTORY SUMMARY

MAC Address	IP Address ▲	Host Name	Processor Name & Speed	RAM Details	System Model
⊕ 01 340500 788529 2	192.168.1.169	Manish's iPhone	N/A	N/A	iPhone5,2
⊕ 35 201806 222898 2	192.168.1.229	Aditya's iPhone	N/A	N/A	iPhone6,2
⊕ 5C-51-88-04-D6-54	192.168.1.244	MotoE2	Qualcomm MSM8212	914.0 MB	MotoE2
⊕ 35 876205 730940 6	192.168.2.145	AKB's iPhone	N/A	N/A	iPhone6,2

Show 100 ▾ entries
Showing 1 to 4 of 4 entries

By default, only the hardware details are displayed in the **Software and Hardware Inventory Summary**.

3. Click ⊕ next to the **MAC Address** to see more details from the columns not displayed in the table.



MAC Address	IP Address ▲	Host Name	Processor Name & Speed	RAM Details	System Model
⊖ 01 340500 788529 2	192.168.1.169	Manish's iPhone	N/A	N/A	iPhone5,2

OS Name : iOS

Mircosoft Office : N/A

Antivirus : N/A

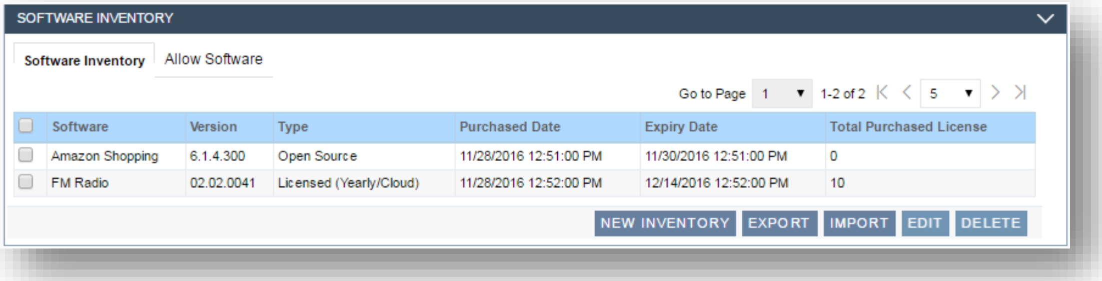
Inventory Settings

Working with Software Inventory

The **Software Inventory** settings enable you to add and select the software to monitor.

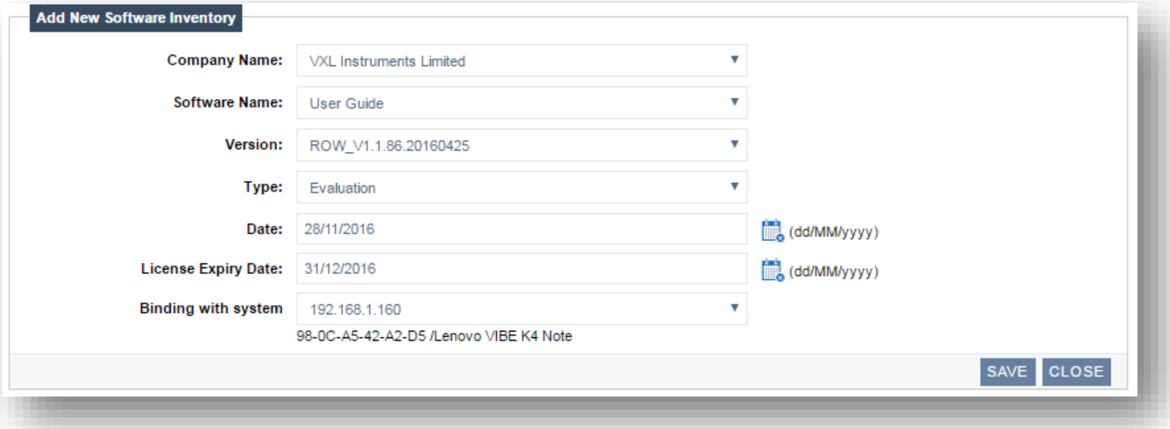
Adding a Software to the Inventory

1. Expand the right menu.
2. Click **Asset Management**, then click **Inventory Settings** and then click **Software Inventory**.



☐	Software	Version	Type	Purchased Date	Expiry Date	Total Purchased License
☐	Amazon Shopping	6.1.4.300	Open Source	11/28/2016 12:51:00 PM	11/30/2016 12:51:00 PM	0
☐	FM Radio	02.02.0041	Licensed (Yearly/Cloud)	11/28/2016 12:52:00 PM	12/14/2016 12:52:00 PM	10

3. On the **Software Inventory** tab, click **New Inventory**.



Add New Software Inventory

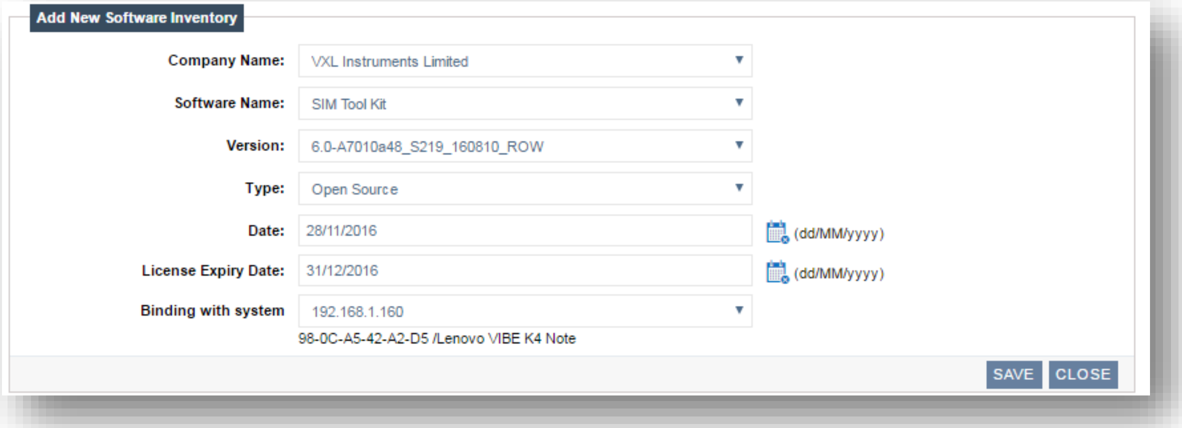
Company Name:	VXL Instruments Limited ▼
Software Name:	User Guide ▼
Version:	ROW_V1.1.86.20160425 ▼
Type:	Evaluation ▼
Date:	28/11/2016 (dd/MM/yyyy)
License Expiry Date:	31/12/2016 (dd/MM/yyyy)
Binding with system	192.168.1.160 ▼ 98-0C-A5-42-A2-D5 /Lenovo VIBE K4 Note

4. In **Add New Software Inventory**, enter the customer name and applicable software details.
5. In **Binding with system**, select the IP address of device where the applicable software has been installed.
6. Click **Save**.

The **Software Inventory added successfully** message is display.

Editing a Software from the Inventory

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Software Inventory**.
3. On the **Software Inventory** tab, in the **Select** column, select the software inventory to edit.



Add New Software Inventory

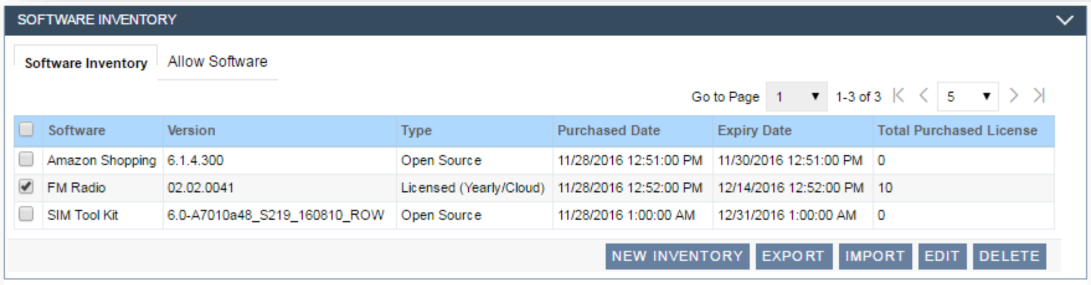
Company Name:	VXL Instruments Limited ▼
Software Name:	SIM Tool Kit ▼
Version:	6.0-A7010a48_S219_160810_ROW ▼
Type:	Open Source ▼
Date:	28/11/2016 (dd/MM/yyyy)
License Expiry Date:	31/12/2016 (dd/MM/yyyy)
Binding with system	192.168.1.160 ▼ 98-0C-A5-42-A2-D5 /Lenovo VIBE K4 Note

4. Click **Edit**.
5. In **Edit Software Inventory**, edit the details as required.
6. Click **Update**.

The **Software Inventory updated successfully** message is display.

Deleting a Software from the Inventory

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Software Inventory**.



□	Software	Version	Type	Purchased Date	Expiry Date	Total Purchased License
□	Amazon Shopping	6.1.4.300	Open Source	11/28/2016 12:51:00 PM	11/30/2016 12:51:00 PM	0
☑	FM Radio	02.02.0041	Licensed (Yearly/Cloud)	11/28/2016 12:52:00 PM	12/14/2016 12:52:00 PM	10
□	SIM Tool Kit	6.0-A7010a48_S219_160810_ROW	Open Source	11/28/2016 1:00:00 AM	12/31/2016 1:00:00 AM	0

3. On the **Software Inventory** tab, in the **Select** column, select the software to delete.
4. Click **Delete.**

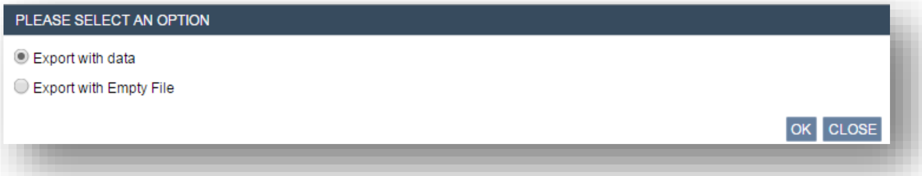
The **Software Inventory deleted successfully** message is display.

Export Inventory Data

User can Export data/format to .CSV file format by clicking on Export button with two options:

- Export with data
- Export with Empty .CSV file.

User can add data in empty .CSV file.

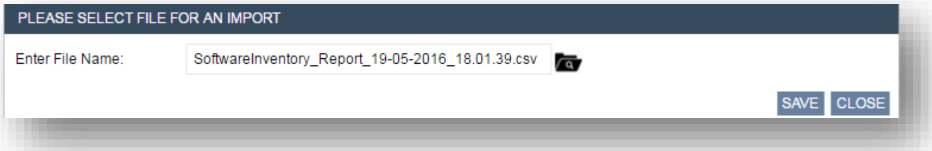


● Export with data

○ Export with Empty File

Import Inventory Data

1. User can import software inventory data only in .csv file format.
2. Specify the.CSV file consisting of software inventory data to be imported, press save button to import data into the database, once imported the data will get listed into data table.
3. The imported inventory data will also reflect into dashboard data.

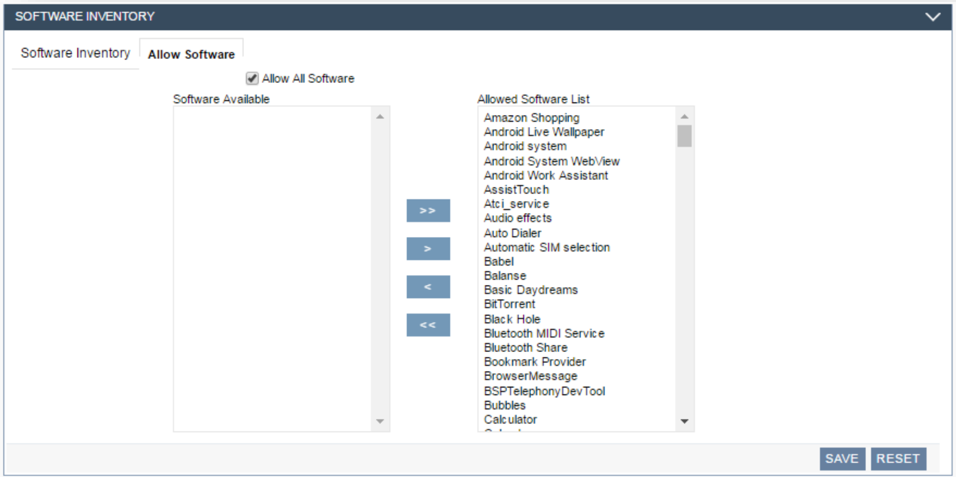


PLEASE SELECT FILE FOR AN IMPORT

Enter File Name: SoftwareInventory_Report_19-05-2016_18.01.39.csv

Selecting the Software for Monitoring

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Software Inventory**.



SOFTWARE INVENTORY

☑ Allow All Software

Software Available

Allowed Software List

Amazon Shopping
Android Live Wallpaper
Android system
Android System WebView
Android Work Assistant
AssistTouch
Atci_service
Audio effects
Auto Dialer
Automatic SIM selection
Babel
Balanse
Basic Daydreams
BitTorrent
Black Hole
Bluetooth MIDI Service
Bluetooth Share
Bookmark Provider
BrowserMessage
BSPTelephonyDevTool
Bubbles
Calculator

   a. The **Software Available** column displays all available software. The **Allowed Software List** column displays monitored software.
   b. On the **Software Settings** tab, in the **Software Available** column, select the software to monitor.

3. Move the selected software to the **Allowed Software List**.

> Select the **Allow All Software** check box to enable monitoring of all software. Bydefault settings is Enabled.

4. Click **Save**.

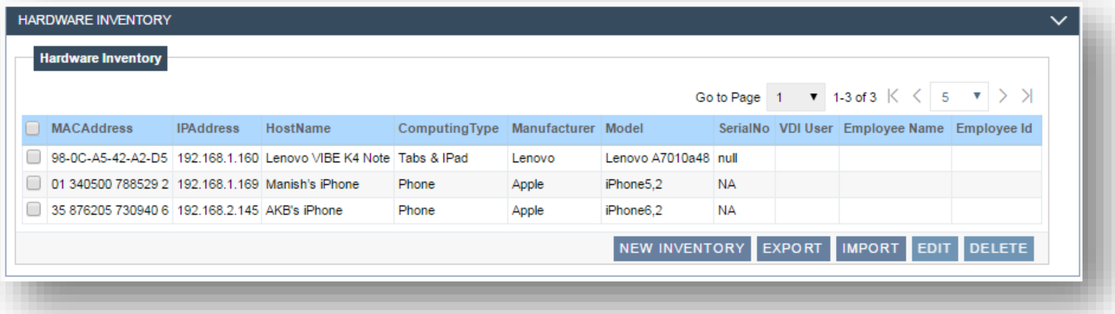
The Software settings updated successfully message is display.

Working with Hardware Inventory

The **Hardware Inventory** settings enable you to add and select the hardware to monitor.

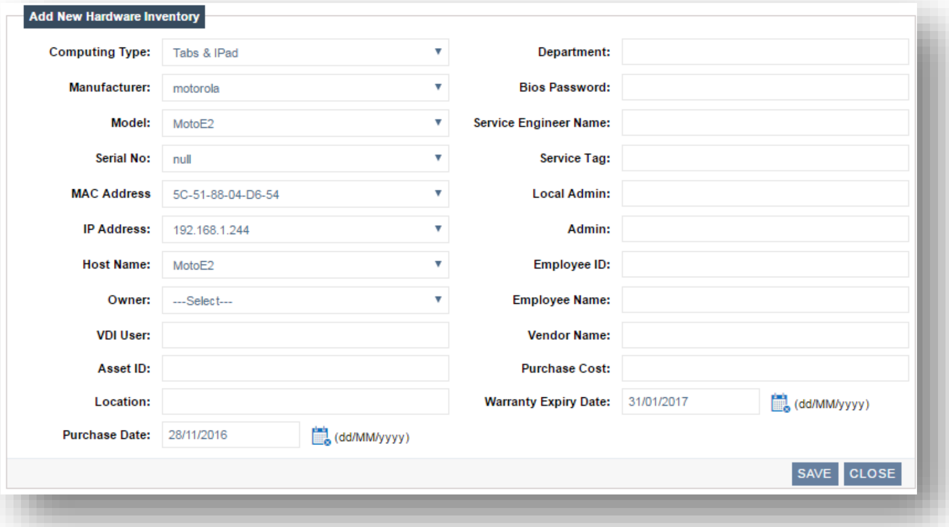
Adding a Hardware to the Inventory

1. Expand the right menu.
2. Click **Asset Management**, then click **Configuration Settings**, and then click **Hardware Inventory.**



☐	MACAddress	IPAddress	HostName	ComputingType	Manufacturer	Model	SerialNo	VDI User	Employee Name	Employee Id
☐	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	Tabs & IPad	Lenovo	Lenovo A7010a48	null			
☐	01 340500 788529 2	192.168.1.169	Manish's iPhone	Phone	Apple	iPhone5,2	NA			
☐	35 876205 730940 6	192.168.2.145	AKB's iPhone	Phone	Apple	iPhone6,2	NA			

3. In **Hardware Inventory**, click **New Inventory**.
4. In **Add New Hardware Inventory**, enter the hardware purchase and other required details.



Add New Hardware Inventory

Computing Type:	Tabs & IPad ▾	Department:	
Manufacturer:	motorola ▾	Bios Password:	
Model:	MotoE2 ▾	Service Engineer Name:	
Serial No:	null ▾	Service Tag:	
MAC Address	5C-51-88-04-D6-54 ▾	Local Admin:	
IP Address:	192.168.1.244 ▾	Admin:	
Host Name:	MotoE2 ▾	Employee ID:	
Owner:	---Select--- ▾	Employee Name:	
VDI User:		Vendor Name:	
Asset ID:		Purchase Cost:	
Location:		Warranty Expiry Date:	31/01/2017 (dd/MM/yyyy)
Purchase Date:	28/11/2016 (dd/MM/yyyy)		

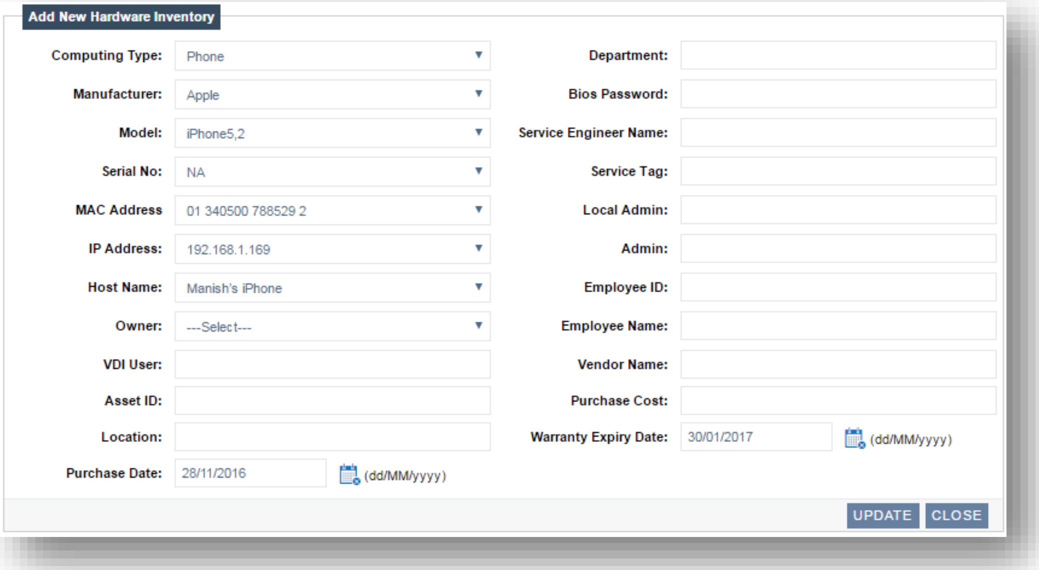
5. Click **Save**.

The **Hardware Inventory added successfully** message is display.

Editing a Hardware from the Inventory

1. Expand the right menu.
2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Hardware Inventory**.
3. In **Hardware Inventory**, in the **Select** column, select the hardware to edit.

4. Click **Edit**.

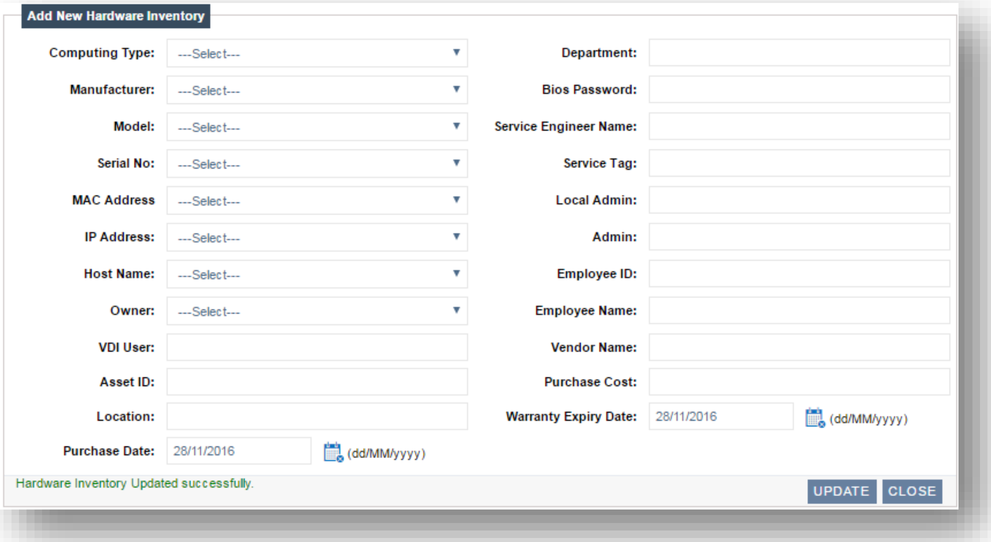


Add New Hardware Inventory

Computing Type:	Phone	Department:	
Manufacturer:	Apple	Bios Password:	
Model:	iPhone5,2	Service Engineer Name:	
Serial No:	NA	Service Tag:	
MAC Address	01 340500 788529 2	Local Admin:	
IP Address:	192.168.1.169	Admin:	
Host Name:	Manish's iPhone	Employee ID:	
Owner:	---Select---	Employee Name:	
VDI User:		Vendor Name:	
Asset ID:		Purchase Cost:	
Location:		Warranty Expiry Date:	30/01/2017 (dd/MM/yyyy)
Purchase Date:	28/11/2016 (dd/MM/yyyy)		

5. In **Add New Hardware Inventory**, edit the hardware details.
6. Click **Update**.

The **Hardware Inventory Updated successfully** message is display.



Add New Hardware Inventory

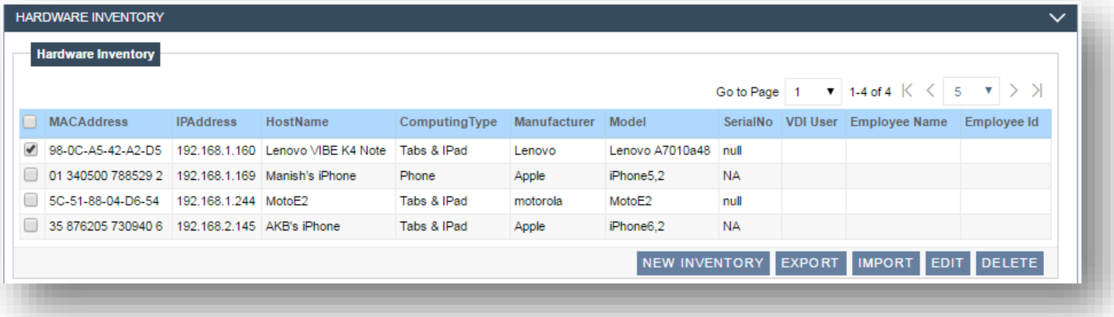
Computing Type:	---Select---	Department:	
Manufacturer:	---Select---	Bios Password:	
Model:	---Select---	Service Engineer Name:	
Serial No:	---Select---	Service Tag:	
MAC Address	---Select---	Local Admin:	
IP Address:	---Select---	Admin:	
Host Name:	---Select---	Employee ID:	
Owner:	---Select---	Employee Name:	
VDI User:		Vendor Name:	
Asset ID:		Purchase Cost:	
Location:		Warranty Expiry Date:	28/11/2016 (dd/MM/yyyy)
Purchase Date:	28/11/2016 (dd/MM/yyyy)		

Hardware Inventory Updated successfully.

Deleting a Hardware from the Inventory

1. Expand the right menu.

2. Click **Configuration Setup**, then click **Configuration Settings**, and then click **Hardware Inventory**.



□	MACAddress	IPAddress	HostName	ComputingType	Manufacturer	Model	SerialNo	VDI User	Employee Name	Employee Id
☑	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	Tabs & IPad	Lenovo	Lenovo A7010a48	null			
□	01 340500 788529 2	192.168.1.169	Manish's iPhone	Phone	Apple	iPhone5,2	NA			
□	5C-51-88-04-D6-54	192.168.1.244	MotoE2	Tabs & IPad	motorola	MotoE2	null			
□	35 876205 730940 6	192.168.2.145	AKB's iPhone	Tabs & IPad	Apple	iPhone6,2	NA			

3. In **Hardware Inventory**, in the **Selec**t column, select the hardware to delete.
4. Click **Delete**

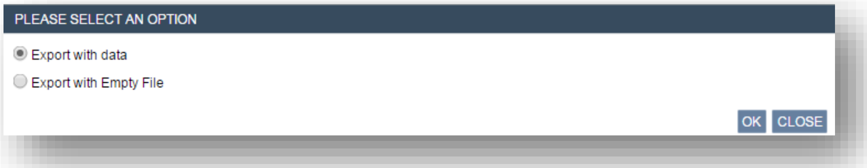
The **Hardware Inventory deleted successfully** message is display.

Export Inventory Data

User can Export data/format to .CSV file format by clicking on Export button with two options:

- Export with data
- Export with Empty .CSV file.

User can add data in empty .CSV file.

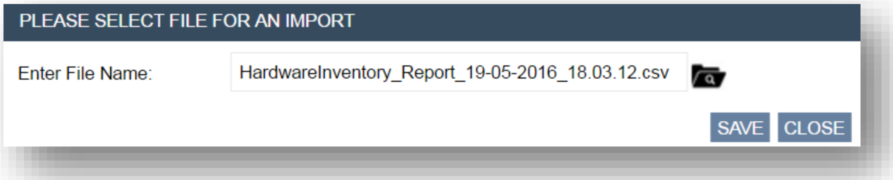


● Export with data

○ Export with Empty File

Import Inventory Data

1. User can import Hardware inventory data only in .csv file format.
2. Specify the.CSV file consisting of Hardware inventory data to be imported, press save button to import data into the database, once imported the data will get listed into data table.
3. The imported inventory data will also reflect into dashboard data.



PLEASE SELECT FILE FOR AN IMPORT

Enter File Name: HardwareInventory_Report_19-05-2016_18.03.12.csv

Performing Common Operations

You can perform the following common operations across the reports viewed in **Asset Management**.

- Show or hide the columns to display in reports and logs.
- Export the data to Excel
- Export the data to PDF
- Print displayed details
- Email the data to clients
- View the data in a pop-up window

For information about the common operations , see “Understanding Common Operations” in “Getting Started”.

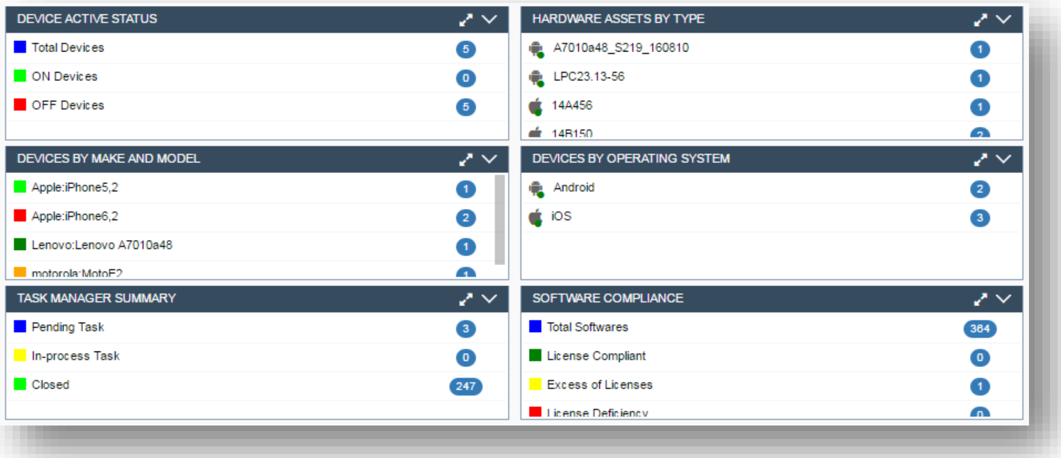
You can email or export only the filtered records .

Reports and Audit Logs

The **Reports and Audit Logs** contain comprehensive and detailed information of various useful data points that can be used for accurate auditing and exhaustive reporting.

To open the **Reports and Audit Logs** page.

- On the toolbar, click 📋.
  The **Reports and Audit Logs** page is display. By default, the page displays a dashboard with the summary of all reports and logs.



DEVICE ACTIVE STATUS

🟦 Total Devices	5
🟩 ON Devices	0
🟥 OFF Devices	5

HARDWARE ASSETS BY TYPE

A7010a48_S219_160810	1
LPC23.13-56	1
14A456	1
14B150	

DEVICES BY MAKE AND MODEL

🟩 Apple:iPhone5,2	1
🟥 Apple:iPhone6,2	2
🟩 Lenovo:Lenovo A7010a48	1
🟧 motorola:MotoE2	

DEVICES BY OPERATING SYSTEM

Android	2
iOS	3

TASK MANAGER SUMMARY

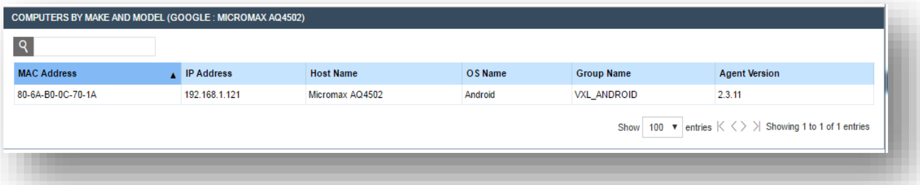
🟦 Pending Task	3
🟨 In-process Task	0
🟩 Closed	247

SOFTWARE COMPLIANCE

🟦 Total Softwares	364
🟩 License Compliant	0
🟨 Excess of Licenses	1
🟥 License Deficiency	

To view details of any particular report

- Click the number in bracket.
  A page with the details of the selected report is display.



COMPUTERS BY MAKE AND MODEL (GOOGLE : MICROMAX AQ4502)

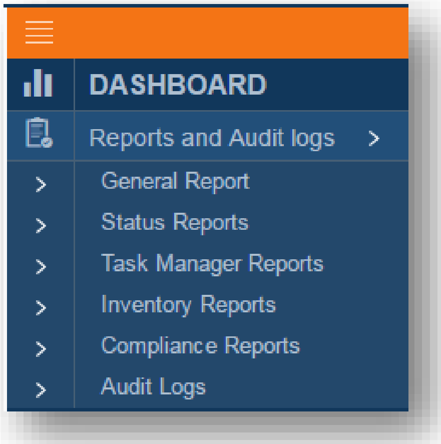
MAC Address	IP Address	Host Name	OS Name	Group Name	Agent Version
80-6A-B0-0C-70-1A	192.168.1.121	Micromax AQ4502	Android	VXL_ANDROID	2.3.11

Show 100 entries Showing 1 to 1 of 1 entries

To view the list of available reports and audit logs

1. Expand the right menu.
2. Click **Reports and Audit logs**.

   A list of available report categories is display



Viewing the General Reports

Performing Common Operations

You can perform the following common operations across the reports and logs viewed in **Reports and Audit**

> For information about the common operations, see “Understanding Common Operations” in “Getting Started”.

Toolbar

📄 📊 🖶	To view or export data in PDF, Excel format or print list view
⤢	Maximize screen
⌄	Expand Screen
⤡	Minimize screen
⌃	Collapse Screen

▼	Advanced Filter
↻	Refresh report
✉	Email report to configured mail id.
↗	Open in popup.
☰	Show / Hide column

Reports & Audit Logs search filter are now saved user wise.

Emailing Reports, Logs and Alerts

You can email all reports, audit logs, and alert messages to client devices.

Prerequisites:

Mailer Engine Configuration

In order to email data to clients, you have to set up the Mailer Engine Configuration in Fusion EMM Configuration View.

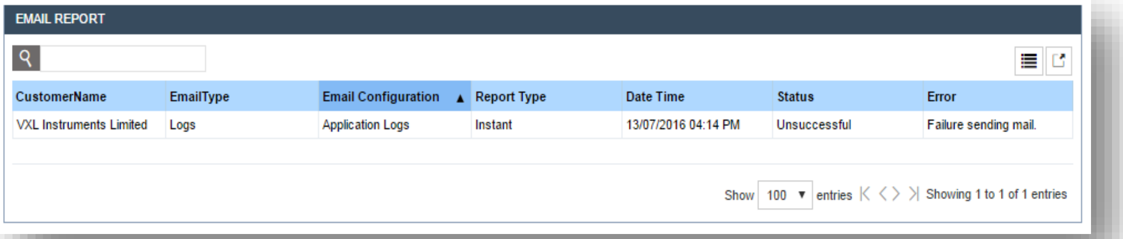
For information about Mailer Engine Configuration, see “Working with Mailer Engine Configuration in, “Configuring Fusion EMM”.

- To email the report, log or alert, in the area above the table, click ✉.

Email Report

The **Email Report** displays the status of the configured auto email services; whether the emails were sent successfully or not. If the emails are unsuccessful, it also displays the error type and indicates the reason for failure.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **General Report**, and then click **Email Report**.



EMAIL REPORT

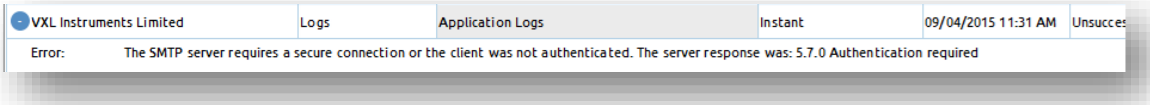
CustomerName	EmailType	Email Configuration ▲	Report Type	Date Time	Status	Error
VXL Instruments Limited	Logs	Application Logs	Instant	13/07/2016 04:14 PM	Unsuccessful	Failure sending mail.

Show 100 ▾ entries Showing 1 to 1 of 1 entries

Determining the Error for an Unsuccessful Email

1. For an email alert whose status is unsuccessful, click ⊕

   The error details are displayed.



⊖ VXL Instruments Limited	Logs	Application Logs	Instant	09/04/2015 11:31 AM	Unsucces

Error: The SMTP server requires a secure connection or the client was not authenticated. The server response was: 5.7.0 Authentication required

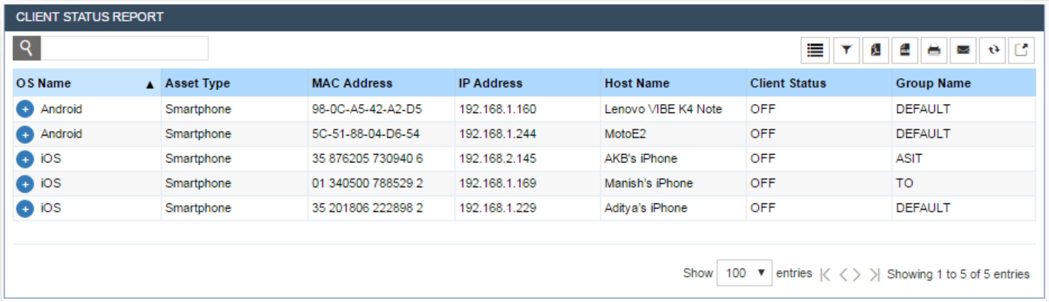
2. Click ⊖ to hide the details.

Viewing Status Reports

Client Status Report

The **Client Status Report** displays details about the status of a client.

1. Expand the right menu.
2. Click **Reports and Audit logs,** then click **Status Report** and, then click **Client Status Report.**



CLIENT STATUS REPORT

OS Name ▲	Asset Type	MAC Address	IP Address	Host Name	Client Status	Group Name
Android	Smartphone	98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	OFF	DEFAULT
Android	Smartphone	5C-51-88-04-D6-54	192.168.1.244	MotoE2	OFF	DEFAULT
iOS	Smartphone	35 876205 730940 6	192.168.2.145	AKB's iPhone	OFF	ASIT
iOS	Smartphone	01 340500 788529 2	192.168.1.169	Manish's iPhone	OFF	TO
iOS	Smartphone	35 201806 222898 2	192.168.1.229	Aditya's iPhone	OFF	DEFAULT

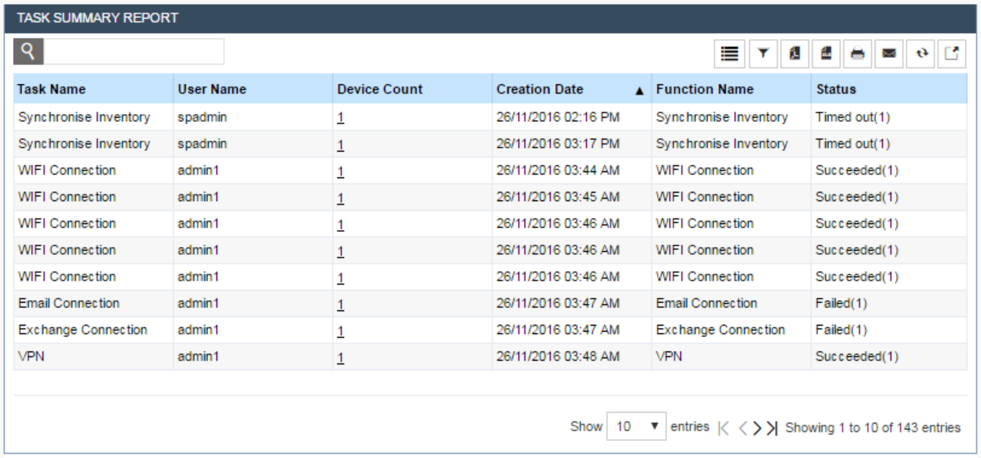
Show 100 entries Showing 1 to 5 of 5 entries

Viewing the Task Manager Reports

Task Summary Report

The **Task Summary Report** displays the summary of the tasks run on various devices including the user who ran the task, the number of devices affected, and whether the task succeeded.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Task Manager Report**, and then click **Task Summary Report**.



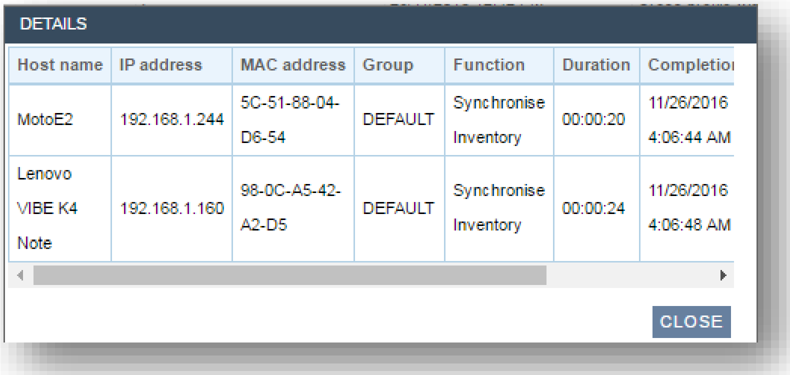
TASK SUMMARY REPORT

Task Name	User Name	Device Count	Creation Date ▲	Function Name	Status
Synchronise Inventory	spadmin	1	26/11/2016 02:16 PM	Synchronise Inventory	Timed out(1)
Synchronise Inventory	spadmin	1	26/11/2016 03:17 PM	Synchronise Inventory	Timed out(1)
WIFI Connection	admin1	1	26/11/2016 03:44 AM	WIFI Connection	Succeeded(1)
WIFI Connection	admin1	1	26/11/2016 03:45 AM	WIFI Connection	Succeeded(1)
WIFI Connection	admin1	1	26/11/2016 03:46 AM	WIFI Connection	Succeeded(1)
WIFI Connection	admin1	1	26/11/2016 03:46 AM	WIFI Connection	Succeeded(1)
WIFI Connection	admin1	1	26/11/2016 03:46 AM	WIFI Connection	Succeeded(1)
Email Connection	admin1	1	26/11/2016 03:47 AM	Email Connection	Failed(1)
Exchange Connection	admin1	1	26/11/2016 03:47 AM	Exchange Connection	Failed(1)
VPN	admin1	1	26/11/2016 03:48 AM	VPN	Succeeded(1)

Show 10 entries Showing 1 to 10 of 143 entries

To view details of the devices on which the task was run,

- In the **Device Count** column, click the number displayed.
  A page with the details of the selected asset is display.



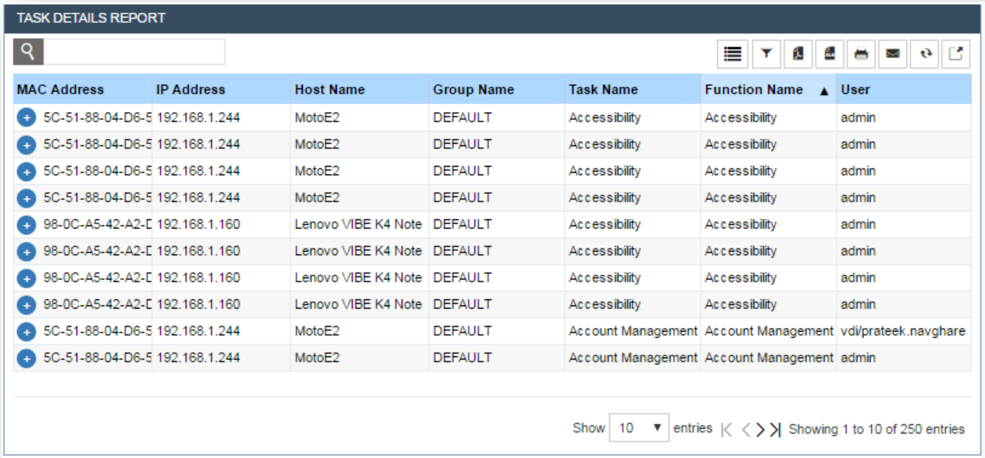
DETAILS

Host name	IP address	MAC address	Group	Function	Duration	Completio
MotoE2	192.168.1.244	5C-51-88-04-D6-54	DEFAULT	Synchronise Inventory	00:00:20	11/26/2016 4:06:44 AM
Lenovo VIBE K4 Note	192.168.1.160	98-0C-A5-42-A2-D5	DEFAULT	Synchronise Inventory	00:00:24	11/26/2016 4:06:48 AM

Task Details Report

The **Task Details Report** displays details about the various tasks run on each host including the user who initiated the task, the start and completion times of the task, and whether it succeeded.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Task Manager Report**, and then click **Task Details Report**.



TASK DETAILS REPORT

MAC Address	IP Address	Host Name	Group Name	Task Name	Function Name ▲	User
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Accessibility	Accessibility	admin
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Accessibility	Accessibility	admin
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Accessibility	Accessibility	admin
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Accessibility	Accessibility	admin
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	Accessibility	Accessibility	admin
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	Accessibility	Accessibility	admin
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	Accessibility	Accessibility	admin
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	Accessibility	Accessibility	admin
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Account Management	Account Management	vdi/prateek.navghare
5C-51-88-04-D6-5	192.168.1.244	MotoE2	DEFAULT	Account Management	Account Management	admin

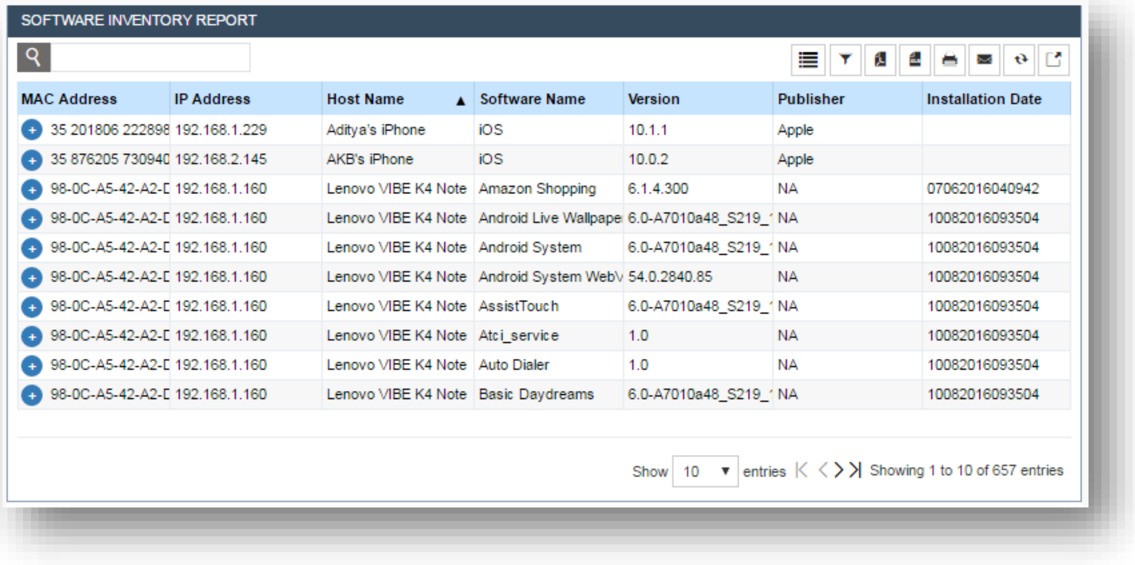
Show 10 entries Showing 1 to 10 of 250 entries

Viewing the Inventory Reports

Software Inventory Report

The **Software Inventory Report** displays an inventory of software used by the client. It also provides the product key for software installed on each system.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Inventory Report**, and then click **Software Inventory Report**.



SOFTWARE INVENTORY REPORT

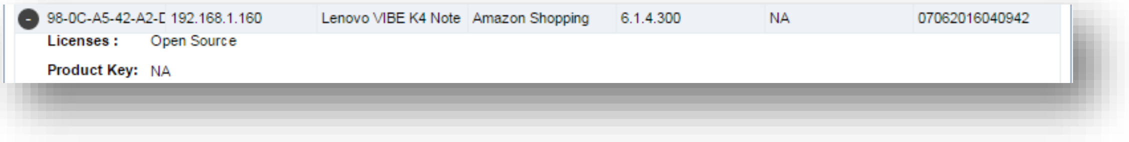
MAC Address	IP Address	Host Name ▲	Software Name	Version	Publisher	Installation Date
35 201806 222898	192.168.1.229	Aditya's iPhone	iOS	10.1.1	Apple	
35 876205 730940	192.168.2.145	AKB's iPhone	iOS	10.0.2	Apple	
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Amazon Shopping	6.1.4.300	NA	07062016040942
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Android Live Wallpape	6.0-A7010a48_S219_	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Android System	6.0-A7010a48_S219_	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Android System WebV	54.0.2840.85	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	AssistTouch	6.0-A7010a48_S219_	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Atci_service	1.0	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Auto Dialer	1.0	NA	10082016093504
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Basic Daydreams	6.0-A7010a48_S219_	NA	10082016093504

Show 10 ▼ entries |< < > >| Showing 1 to 10 of 657 entries

Viewing the Product Key

1. For a particular MAC address, click ⊕.

   The product key, if any, is display.



MAC Address	IP Address	Host Name	Software Name	Version	Publisher	Installation Date
98-0C-A5-42-A2-D	192.168.1.160	Lenovo VIBE K4 Note	Amazon Shopping	6.1.4.300	NA	07062016040942

Licenses : Open Source

Product Key: NA

2. The product key is stored in Fusion EMM when new software is installed or added to inventory.

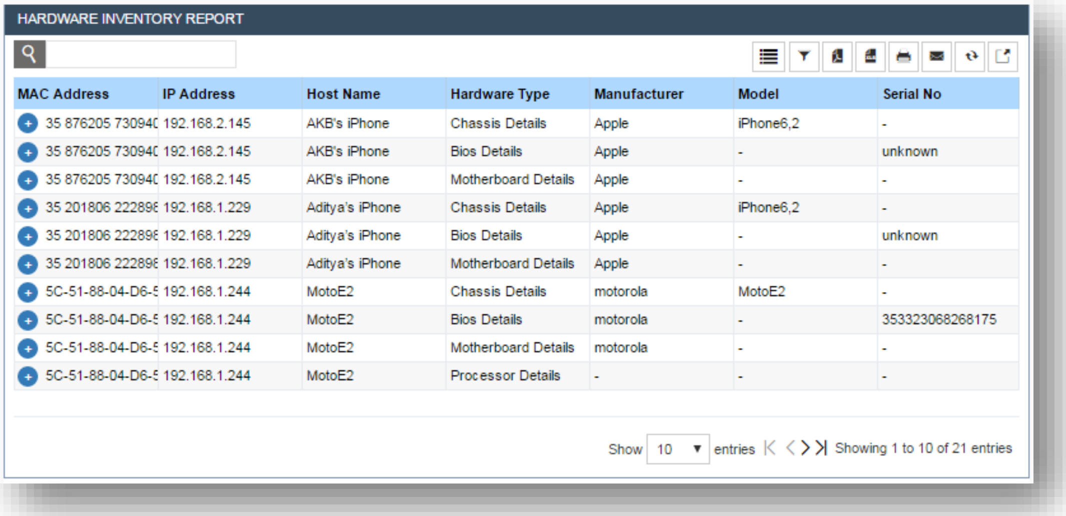
For information about adding new software to inventory, see “Inventory Settings” in “Asset Management”.

3. Click ⊖ to hide the details.

Hardware Inventory Report

The **Hardware Inventory Report** displays an inventory of hardware used by the client.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Inventory Report**, and then click **Hardware Inventory Report**.



HARDWARE INVENTORY REPORT

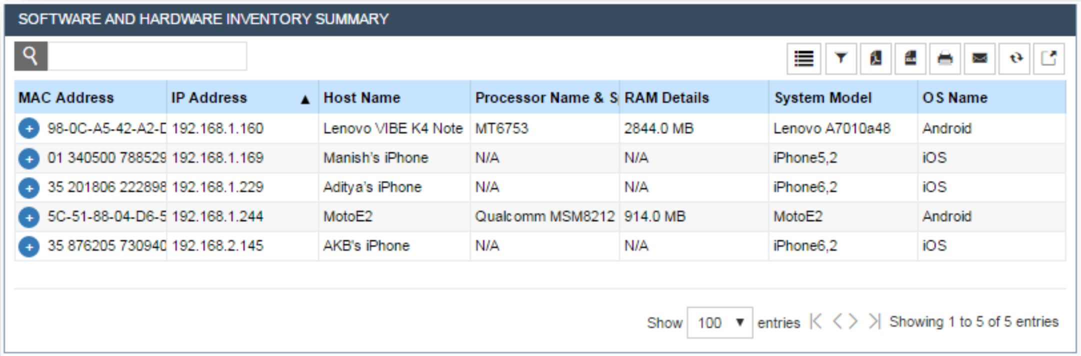
MAC Address	IP Address	Host Name	Hardware Type	Manufacturer	Model	Serial No
35 876205 73094	192.168.2.145	AKB's iPhone	Chassis Details	Apple	iPhone6,2	-
35 876205 73094	192.168.2.145	AKB's iPhone	Bios Details	Apple	-	unknown
35 876205 73094	192.168.2.145	AKB's iPhone	Motherboard Details	Apple	-	-
35 201806 22289	192.168.1.229	Aditya's iPhone	Chassis Details	Apple	iPhone6,2	-
35 201806 22289	192.168.1.229	Aditya's iPhone	Bios Details	Apple	-	unknown
35 201806 22289	192.168.1.229	Aditya's iPhone	Motherboard Details	Apple	-	-
5C-51-88-04-D6-	192.168.1.244	MotoE2	Chassis Details	motorola	MotoE2	-
5C-51-88-04-D6-	192.168.1.244	MotoE2	Bios Details	motorola	-	353323068268175
5C-51-88-04-D6-	192.168.1.244	MotoE2	Motherboard Details	motorola	-	-
5C-51-88-04-D6-	192.168.1.244	MotoE2	Processor Details	-	-	-

Show 10 entries Showing 1 to 10 of 21 entries

Software and Hardware Inventory Summary

The **Software and Hardware Inventory Summary** provides an inventory of the hardware of a system and the corresponding software pertaining to that hardware.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Inventory Report**, and then click **Software and Hardware Inventory Summary**.

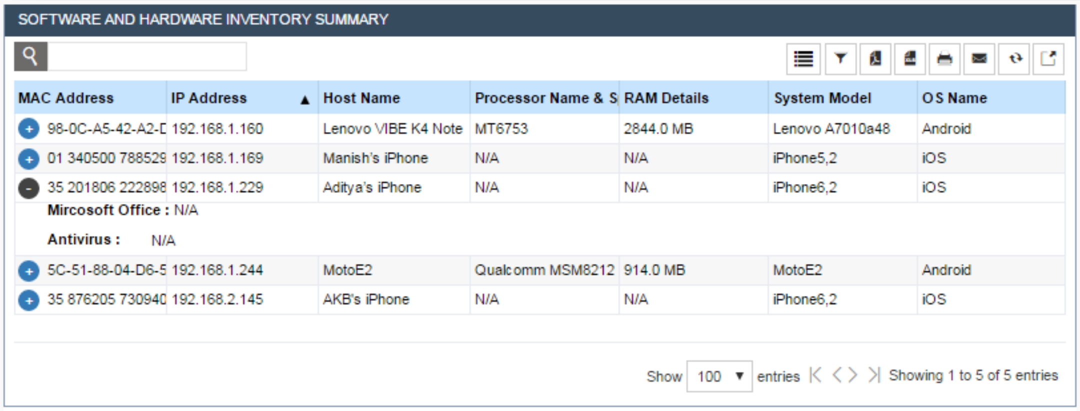


SOFTWARE AND HARDWARE INVENTORY SUMMARY

MAC Address	IP Address ▲	Host Name	Processor Name & S	RAM Details	System Model	OS Name
98-0C-A5-42-A2-	192.168.1.160	Lenovo VIBE K4 Note	MT6753	2844.0 MB	Lenovo A7010a48	Android
01 340500 78852	192.168.1.169	Manish's iPhone	N/A	N/A	iPhone5,2	iOS
35 201806 222898	192.168.1.229	Aditya's iPhone	N/A	N/A	iPhone6,2	iOS
5C-51-88-04-D6-5	192.168.1.244	MotoE2	Qualcomm MSM8212	914.0 MB	MotoE2	Android
35 876205 730940	192.168.2.145	AKB's iPhone	N/A	N/A	iPhone6,2	iOS

Show 100 entries Showing 1 to 5 of 5 entries

3. For a particular MAC address, click ⊕.
   The software inventory report of the system is display.



SOFTWARE AND HARDWARE INVENTORY SUMMARY

MAC Address	IP Address ▲	Host Name	Processor Name & S	RAM Details	System Model	OS Name
+ 98-0C-A5-42-A2-[	192.168.1.160	Lenovo VIBE K4 Note	MT6753	2844.0 MB	Lenovo A7010a48	Android
+ 01 340500 788529	192.168.1.169	Manish's iPhone	N/A	N/A	iPhone5,2	iOS
- 35 201806 222898	192.168.1.229	Aditya's iPhone	N/A	N/A	iPhone6,2	iOS
Mircosoft Office : N/A						
Antivirus : N/A						
+ 5C-51-88-04-D6-5	192.168.1.244	MotoE2	Qualcomm MSM8212	914.0 MB	MotoE2	Android
+ 35 876205 730940	192.168.2.145	AKB's iPhone	N/A	N/A	iPhone6,2	iOS

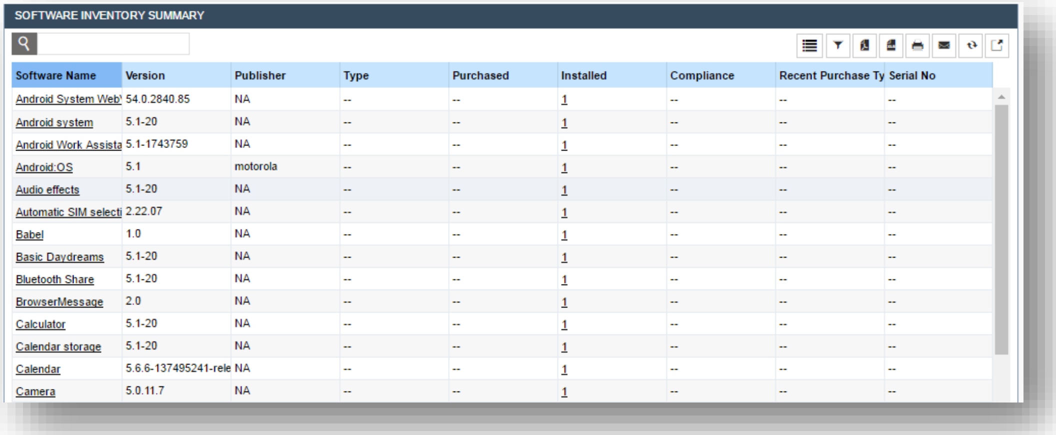
Show 100 ▼ entries |< < > >| Showing 1 to 5 of 5 entries

4. Click ⊖ to hide the details.

Software Inventory Summary

The **Software Inventory Summary** displays information about the number of purchased software and the number of installed software. It thus indicates the level of compliance.

1. Expand the right menu.
2. Click **Reports and Audit logs,** then click **Compliance Report,** and then click **Software Inventory Summary**.



SOFTWARE INVENTORY SUMMARY

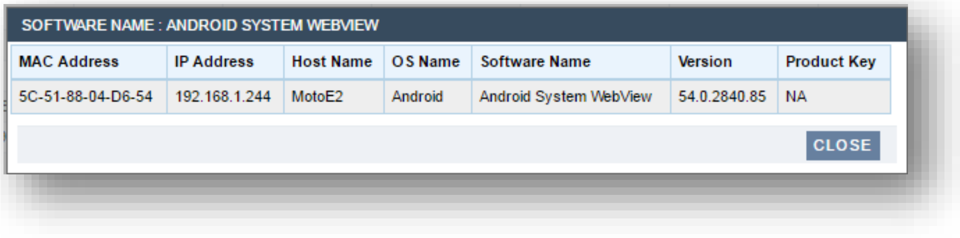
Software Name	Version	Publisher	Type	Purchased	Installed	Compliance	Recent Purchase Ty	Serial No
Android System Web\	54.0.2840.85	NA	--	--	1	--	--	--
Android system	5.1-20	NA	--	--	1	--	--	--
Android Work Assista	5.1-1743759	NA	--	--	1	--	--	--
Android:OS	5.1	motorola	--	--	1	--	--	--
Audio effects	5.1-20	NA	--	--	1	--	--	--
Automatic SIM selecti	2.22.07	NA	--	--	1	--	--	--
Babel	1.0	NA	--	--	1	--	--	--
Basic Daydreams	5.1-20	NA	--	--	1	--	--	--
Bluetooth Share	5.1-20	NA	--	--	1	--	--	--
BrowserMessage	2.0	NA	--	--	1	--	--	--
Calculator	5.1-20	NA	--	--	1	--	--	--
Calendar storage	5.1-20	NA	--	--	1	--	--	--
Calendar	5.6.6-137495241-rele	NA	--	--	1	--	--	--
Camera	5.0.11.7	NA	--	--	1	--	--	--

License Details

To view the details of the licenses

1. In the **Purchased** column, click the displayed number.

   A pop-up with the license details is display.



SOFTWARE NAME : ANDROID SYSTEM WEBVIEW

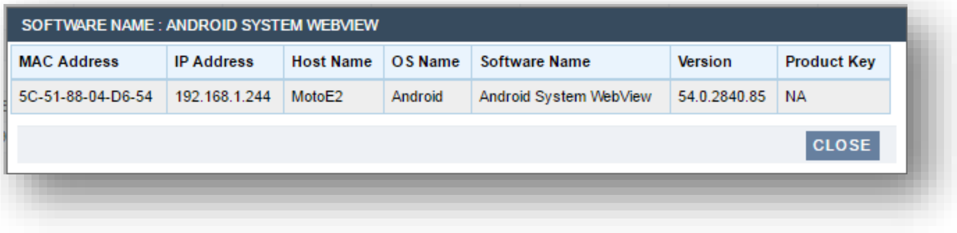
MAC Address	IP Address	Host Name	OS Name	Software Name	Version	Product Key
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	Android System WebView	54.0.2840.85	NA

2. Click **Close**.

Installation Details

To view details of the system where the software is installed

1. In the **Installed** column, click the number for the software.
   A pop-up displays the license details.



SOFTWARE NAME : ANDROID SYSTEM WEBVIEW

MAC Address	IP Address	Host Name	OS Name	Software Name	Version	Product Key
5C-51-88-04-D6-54	192.168.1.244	MotoE2	Android	Android System WebView	54.0.2840.85	NA

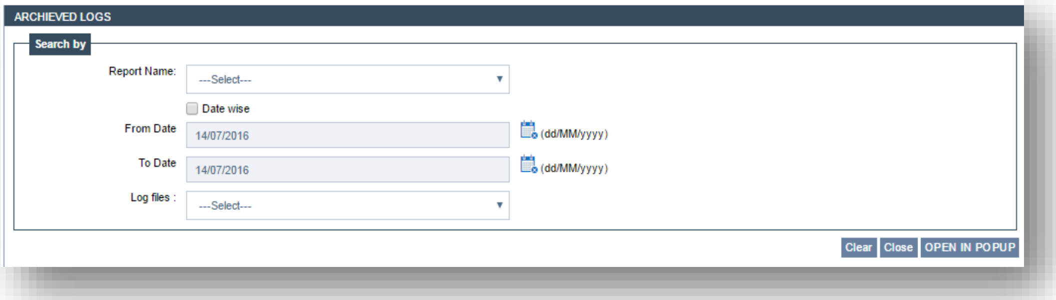
2. Click **Close**.

Viewing the Audit Logs

Archived Logs

The **Archived Logs** allows you to retrieve older logs that have been archived.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Audit Logs**, and then click **Archived Logs**.



Report Name: ---Select---

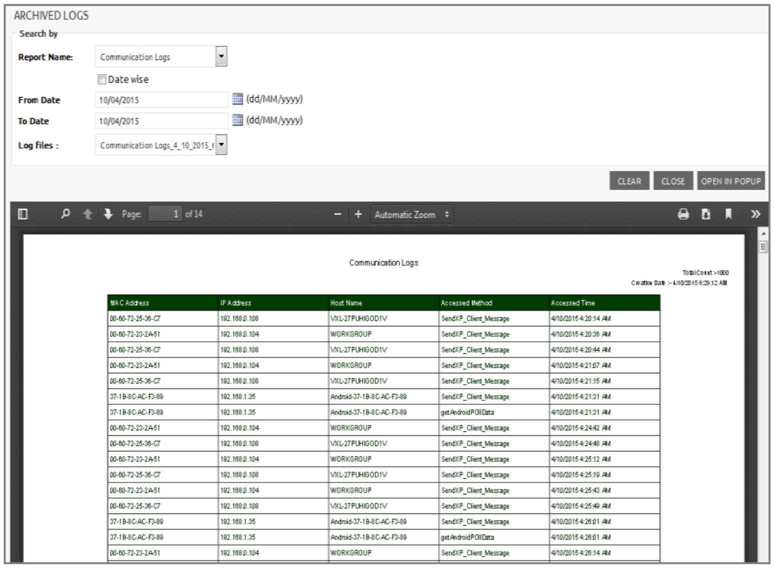
□ Date wise

From Date 14/07/2016 (dd/MM/yyyy)

To Date 14/07/2016 (dd/MM/yyyy)

Log files : ---Select---

2. In the **Report Name** list, select one of the following report names:
   - Application Logs
   - Communication Logs
   - Disk Drive Logs
   - Internet Access Logs
   - Task Detail Report
3. In the **Log File** list, select a date specific log file.
   The report is display.



Report Name: Communication Logs

□ Date wise

From Date 10/04/2015 (dd/MM/yyyy)

To Date 10/04/2015 (dd/MM/yyyy)

Log files : Communication Logs_4_10_2015_6

Communication Logs

TotalCount :-1000
Creation Date :- 4/10/2015 6:29:12 AM

MAC Address	IP Address	Host Name	Accessed Method	Accessed Time
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:20:14 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:20:36 AM
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:20:44 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:21:07 AM
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:21:15 AM
37-1B-8C-AC-F3-89	192.168.1.35	Android-37-1B-8C-AC-F3-89	SendXP_Client_Message	4/10/2015 4:21:31 AM
37-1B-8C-AC-F3-89	192.168.1.35	Android-37-1B-8C-AC-F3-89	getAndroidPOIIData	4/10/2015 4:21:31 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:24:42 AM
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:24:48 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:25:12 AM
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:25:19 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:25:43 AM
00-60-72-25-36-C7	192.168.0.108	VXL-27PUHIGOD1V	SendXP_Client_Message	4/10/2015 4:25:49 AM
37-1B-8C-AC-F3-89	192.168.1.35	Android-37-1B-8C-AC-F3-89	SendXP_Client_Message	4/10/2015 4:26:01 AM
37-1B-8C-AC-F3-89	192.168.1.35	Android-37-1B-8C-AC-F3-89	getAndroidPOIIData	4/10/2015 4:26:01 AM
00-60-72-23-2A-51	192.168.0.104	WORKGROUP	SendXP_Client_Message	4/10/2015 4:26:14 AM

Filtering by Date

The archived logs can also be filtered for a specific date range.

To access logs for a specific date range

1. In the **Report Name** list, select one of the following report names:
   - Application Logs

- Communication Logs
- Disk Drive Logs
- Internet Access Logs
- Task Detail Report

2. Select the **Date-wise** check box.

3. In the **From Date** box, click 📅 , and then select the required start date.

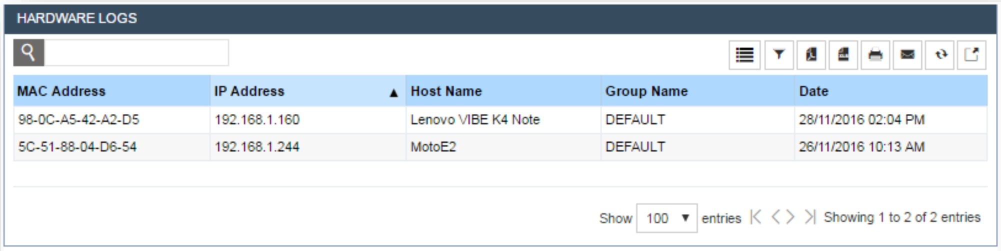
4. In the **To Date** box, click 📅 , and then select the required end date.

5. In the **Log File** list, select the required log file.
Date specific archived report is display.

Hardware Logs

The **Hardware Logs** display information about the hardware connected to a system. It provides the status of hardware like keyboard, mouse and display.

1. Click **Reports and Audit logs**, then click **Audit Logs,** and then click **Hardware Logs.**



HARDWARE LOGS

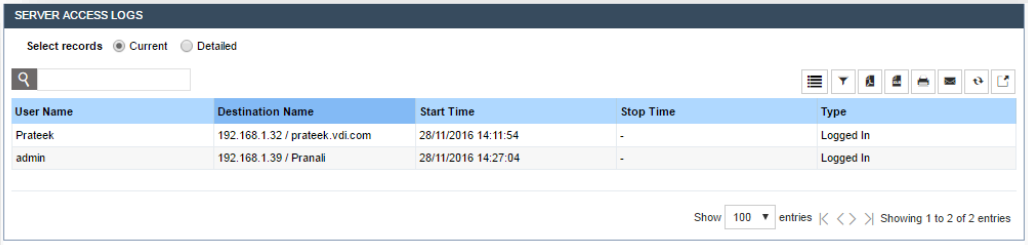
MAC Address	IP Address ▲	Host Name	Group Name	Date
98-0C-A5-42-A2-D5	192.168.1.160	Lenovo VIBE K4 Note	DEFAULT	28/11/2016 02:04 PM
5C-51-88-04-D6-54	192.168.1.244	MotoE2	DEFAULT	26/11/2016 10:13 AM

Show 100 ▾ entries Showing 1 to 2 of 2 entries

Server Access Logs

These logs provide information about the Fusion EMM administrator's username, and log-in time and log-out time processed by the server.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Audit Logs**, and then click **Server Access Logs**.



SERVER ACCESS LOGS

Select records ● Current ○ Detailed

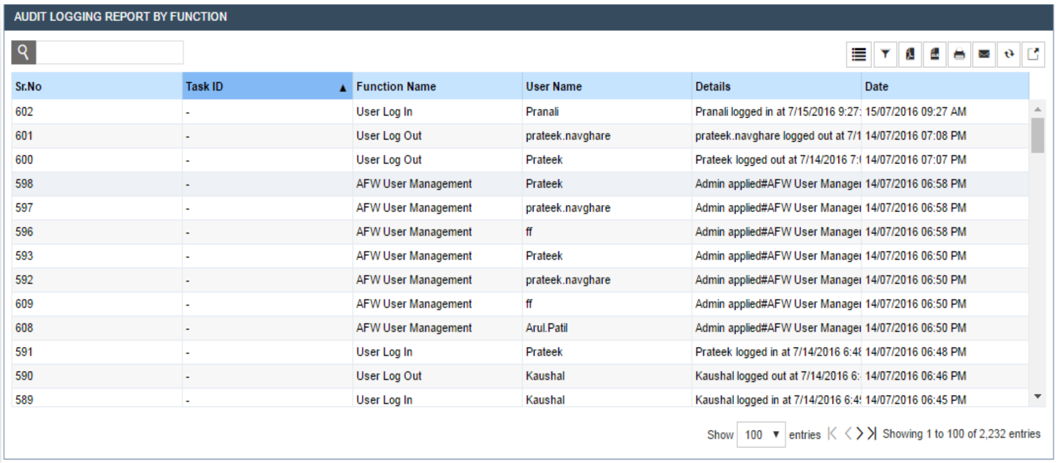
User Name	Destination Name	Start Time	Stop Time	Type
Prateek	192.168.1.32 / prateek.vdi.com	28/11/2016 14:11:54	-	Logged In
admin	192.168.1.39 / Pranali	28/11/2016 14:27:04	-	Logged In

Show 100 ▾ entries Showing 1 to 2 of 2 entries

Audit Logging Report

The **Audit Logging Report** captures each and every activity of all users.

1. Expand the right menu.
2. Click **Reports and Audit logs**, then click **Audit Logs**, and then click **Audit Logging Report.**



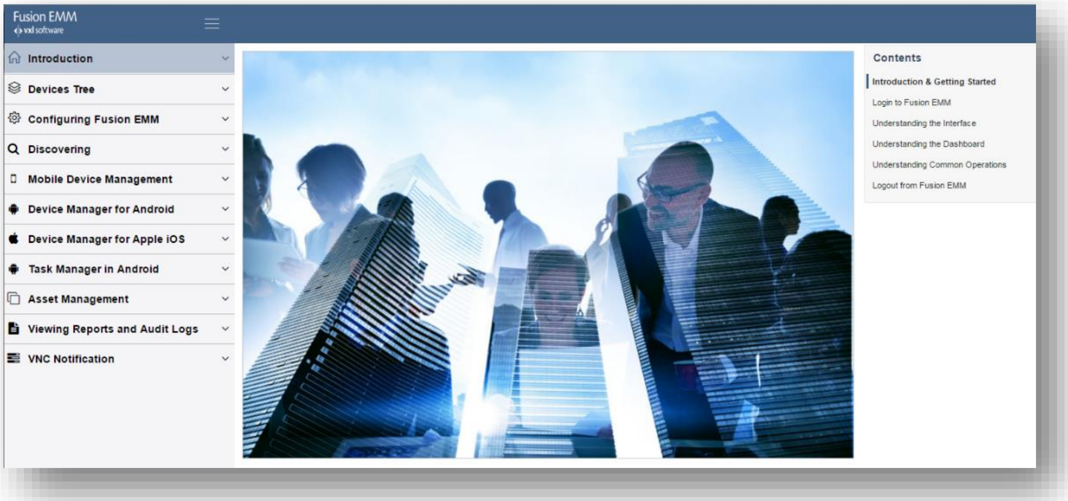
AUDIT LOGGING REPORT BY FUNCTION

Sr.No	Task ID	Function Name	User Name	Details	Date
602	-	User Log In	Pranali	Pranali logged in at 7/15/2016 9:27:	15/07/2016 09:27 AM
601	-	User Log Out	prateek.navghare	prateek.navghare logged out at 7/1	14/07/2016 07:08 PM
600	-	User Log Out	Prateek	Prateek logged out at 7/14/2016 7:	14/07/2016 07:07 PM
598	-	AFW User Management	Prateek	Admin applied#AFW User Manage	14/07/2016 06:58 PM
597	-	AFW User Management	prateek.navghare	Admin applied#AFW User Manage	14/07/2016 06:58 PM
596	-	AFW User Management	ff	Admin applied#AFW User Manage	14/07/2016 06:58 PM
593	-	AFW User Management	Prateek	Admin applied#AFW User Manage	14/07/2016 06:50 PM
592	-	AFW User Management	prateek.navghare	Admin applied#AFW User Manage	14/07/2016 06:50 PM
609	-	AFW User Management	ff	Admin applied#AFW User Manage	14/07/2016 06:50 PM
608	-	AFW User Management	Arul.Patil	Admin applied#AFW User Manage	14/07/2016 06:50 PM
591	-	User Log In	Prateek	Prateek logged in at 7/14/2016 6:4	14/07/2016 06:48 PM
590	-	User Log Out	Kaushal	Kaushal logged out at 7/14/2016 6:	14/07/2016 06:46 PM
589	-	User Log In	Kaushal	Kaushal logged in at 7/14/2016 6:4	14/07/2016 06:45 PM

Show 100 ▾ entries Showing 1 to 100 of 2,232 entries

HELP

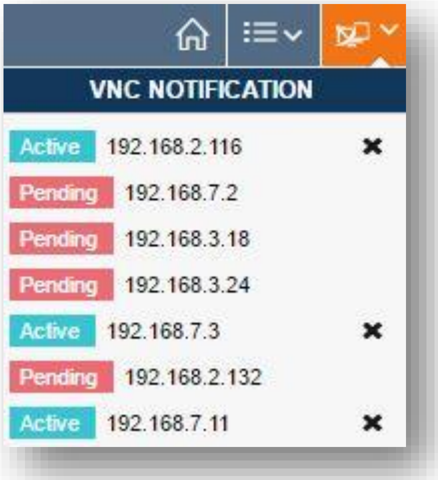
HTML User guide is available from toolbar using tool button for Help. User can refer help information for all modules and views from this tab.



VNC Notification

VNC notification widget provides a list of devices with VNC connection status.

1. To apply task for VNC settings go to Context menu -> select shadowing click on Apply.
2. In notification view user can see following type of connection status:
    - Active
    - Pending



VNC NOTIFICATION

Active	192.168.2.116	✖
Pending	192.168.7.2	
Pending	192.168.3.18	
Pending	192.168.3.24	
Active	192.168.7.3	✖
Pending	192.168.2.132	
Active	192.168.7.11	✖

Active: Based upon successful authentication, status will have updated from Pending to Active.

Pending: When user will request / apply task for shadowing the request will remain in pending status until completion of connection process.

After click on active IP link, user can obtain remote VNC session of selected end point device.

User may get interactive message asking for authorising VNC connection request with display of select options "YES" or "No". If yes option is selected then the VNC connection wiil be established and status in VNC noification panel will be updated from pending to Active.

Default password should be configured in General Settings.