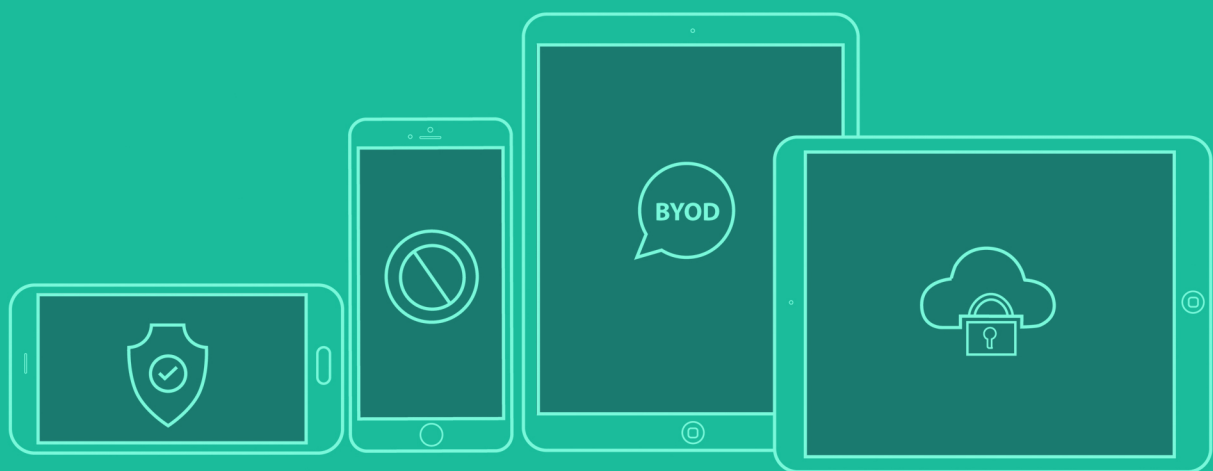


Hexnode MDM

Admin Guide



Contents

Hexnode Mobile Device Management solution.....	7
MDM Key features	7
Supported Operating Systems.....	7
Supported Devices	7
Hexnode MDM - Architecture	8
Hexnode MDM server	8
Firewall	8
APNs	8
Mobile Devices	9
Architecture of Hexnode MDM:.....	9
MDM Getting configured	10
Admin tab.....	10
NAT settings.....	10
APNs settings.....	11
Renewing APNs certificate	13
Proxy Settings	14
Configuring Email Server Settings	14
Server Settings	15
Server HTTP port.....	15
Server SSL port	15
LOG level.....	15
MDM settings	16
Scheduled scan settings.....	16
Home Tab - Mobile Device Management Dashboard.....	17
Ribbon that shows the summary of mobile devices.....	17
BYOD (Bring Your Own Device) Summary Graph	17
Compliance statistics widget.....	18
Recently enrolled mobile devices	18
Inactive devices.....	19
Non-Compliant devices.....	19
Activity Feed Widget	20
Instant “Enroll “button	21
Instant “Add policy” button	21
Enrollment Tab.....	22
Ribbon panel of enrollment status	22

Enrolling devices.....	22
How to enroll iOS devices	23
How to enroll Android devices	26
Send Enrollment Request.....	26
Install App and complete Enrollment process.....	26
Cancel Pending request.....	29
Send New request.....	30
Enrollment request status	31
Self Enrollment	31
CSV import	31
DEP Management	33
Dep Settings	33
Renew a DEP Token	34
DEP Devices	34
To associate a device with a profile	34
DEP Policies.....	35
VPP settings	37
Policy Management.....	39
Password policy	39
Restrictions.....	40
WIFI.....	42
VPN.....	43
Email	44
Active Sync	45
LDAP	46
CalDav	46
CardDav	47
Subscribed Calendars	47
Web Clip.....	48
Configure Access Point.....	48
Configure credentials	49
Steps to configure policy.....	49
Steps to remove policy from the devices/user or from groups	49
Management.....	50
Devices.....	50
Scanning the device	50

Viewing the details of devices	50
Ribbon that shows status of device scan summary	51
Device Summary	51
Device information	51
Security details	52
Applications	52
Associated policies	53
Action feed	54
.....	55
Filters	55
Remote Device Management	56
Clear passcodes	56
Remote Lock	56
Wipe device	56
Disenroll Device	56
Associate policy	56
User	56
Adding a user	56
Viewing user details	57
Sort	57
Search	57
Filter	58
Management	58
Clear passcodes	58
Remote Lock	58
Wipe device	58
Disenroll Device	58
Associate policy	58
Device Groups	59
Static grouping	59
Dynamic grouping	60
User group	62
Group Management Functions	63
Clear passcodes	63
Remote Lock	63
Wipe device	63

Disenroll Device	63
Associate policy	63
MDM Reporting Module	64
MDM Device reports	66
Non-Compliant.....	66
iOS devices	66
Camera Enabled	66
Password present.....	66
Missing mandatory apps	66
Non-encrypted.....	66
Enrolled devices	66
Unenrolled devices.....	66
Jailbroken devices	66
All devices.....	66
Enrollment Pending.....	66
MDM User reports	67
All users	67
Unenrolled user	67
Non-Compliant user.....	67
Users without passcode.....	67
Users with inactive device	67
Camera enabled users.....	67
Enrolled users.....	67
Users with unencrypted devices.....	67
Compliance reports	68
Compliant Devices	68
Profile Compliant.....	68
Passcode Compliant	68
Non-Compliant.....	68
Profile Non-compliant.....	68
No Passcode	68
Inactive.....	68
Mobile Application Management (MAM)	69
Getting started with Mobile Application management	69
Apps (App inventory)	69
App groups.....	70

Enterprise App catalogs	70
Deploying apps via Enterprise app catalog.....	71
App installation	72
App Blacklisting/Whitelisting.....	72
Push Enterprise Apps	73
Mandatory Apps	74
Active Directory settings	75
Applying polices on an AD group.....	76
Active Directory based Remote Device Management	77
App lock	78
Location Tracking	78
To enable and configure Location on devices.....	79
To view the current location of the device	79
Location History	80
To view the device location history:	80
Contacting Hexnode support.....	81
Contact information	81
Technical support	81

Hexnode Mobile Device Management solution

Hexnode delivers a simple, easy-to-configure enterprise mobility management solution to manage the entire fleet of mobile devices in your organization. Hexnode MDM allows you to enable Bring Your Own Device (BYOD) and Enterprise Mobility (EMM) in your business without compromising security. It can be deployed on-premises or in the cloud.

MDM Key features

- ✓ Extensive set of policy controls for managing devices efficiently.
- ✓ Reports and analytics to keep you well informed of your security and compliance status at all times
- ✓ Instant notifications to help you quickly detect and respond to policy violations.
- ✓ Take control of the apps with mobile app deployment, update and removal capabilities
- ✓ App inventory to monitor the applications, track the currently trending apps and identify outdated and potentially risky applications in the network
- ✓ Remotely view and manage devices, and execute a host of remote actions from the MDM portal.

Supported Operating Systems

- iOS version 5 and above.
- Android 2.3 and up

Supported Devices

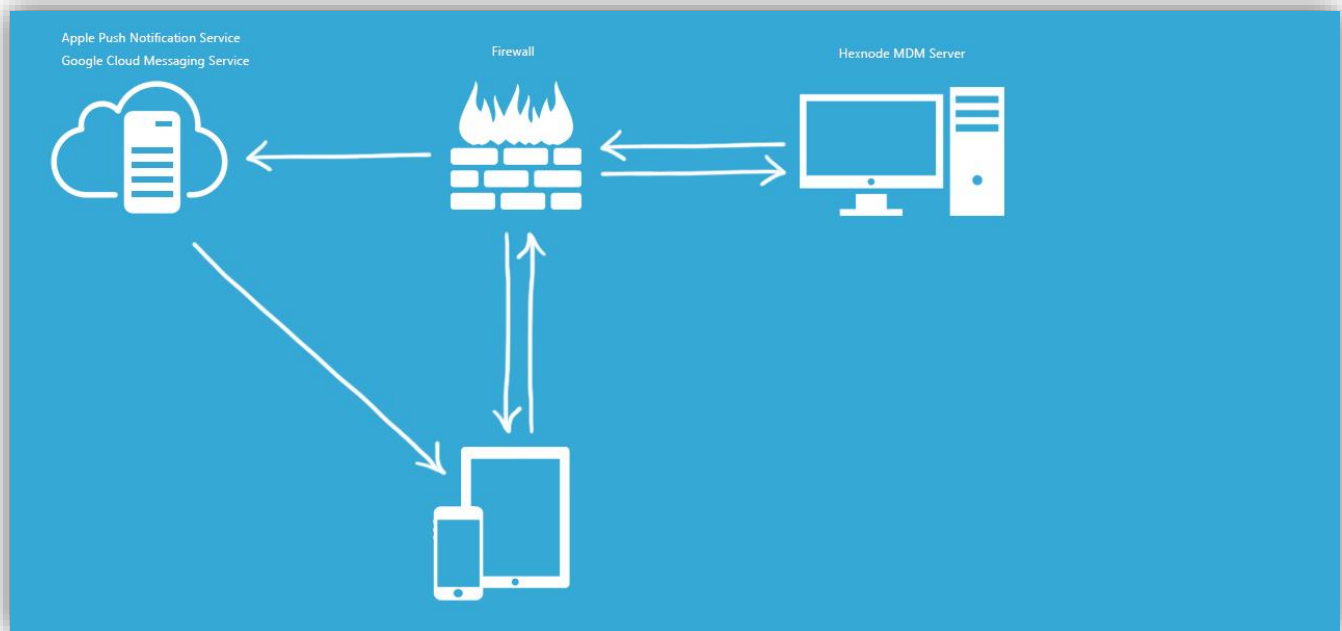
- iPhones
- iPads
- Android devices

Hexnode MDM - Architecture

Hexnode MDM lets you securely manage both personal and corporate mobile devices in your business.

Using Hexnode MDM, an IT manager can easily enroll devices over-the-air, impose settings / policies, manage apps and check compliance with enterprise's standards. Unified web console simplifies EMM by letting you centrally manage and secure the entire fleet of devices.

The diagram below represents the MDM architecture in Hexnode Mobile Device Management Solution.



The main infrastructure entities involved in the architecture are

Hexnode MDM server

The Server which hosts Hexnode Mobile Device Management software. The server must be accessible via public IP address as many users will be out of office network.

Firewall

A firewall establishes a barrier between a trusted, secure internal network of an enterprise and internet. It controls incoming and outgoing network traffic based on predefined set of rules.

APNs

Apple Push Notification Service is a highly efficient service created by Apple, to enable communication from a third party to iOS devices.

APNs certificate installed in Hexnode MDM server ensures that the managed mobile devices

communicate through a secure channel using Apple Push Notification Service

Mobile Devices

Personal or corporate owned devices of employees which need to be managed in an organization.

Architecture of Hexnode MDM:

1. Hexnode MDM initiates the communication by sending a notification to APNs server, to wake up the managed mobile device (via TCP port 2195).
2. A live TCP connection is maintained by all iOS devices to APNs, via port 5223.
3. The device listens for the commands, policy settings and configurations sent by Hexnode MDM.
4. The device will execute the commands, apply the configurations/policies and report the data back to the Hexnode MDM server.

Ports

- Port 80: The default application port used during the installation of Hexnode MDM.
- Port 443: Used for secured and encrypted connection between mobile devices and Hexnode MDM.
- Port 2195 (outbound): This port must be open for the Hexnode MDM server to communicate with APNs (Host Address is gateway.push.apple.com).
- Port 5223(outbound): If the mobile devices are connected to the internet through Wi-Fi, this port should be open.

MDM Getting configured

Admin tab

You need to configure all the admin settings before you can get the MDM up and running. Admin settings include configurations for the MDM to interact with Apple push notification service; the global settings for MDM and web server; the firewall, email and proxy settings.

For accessing admin configuration section, you need to

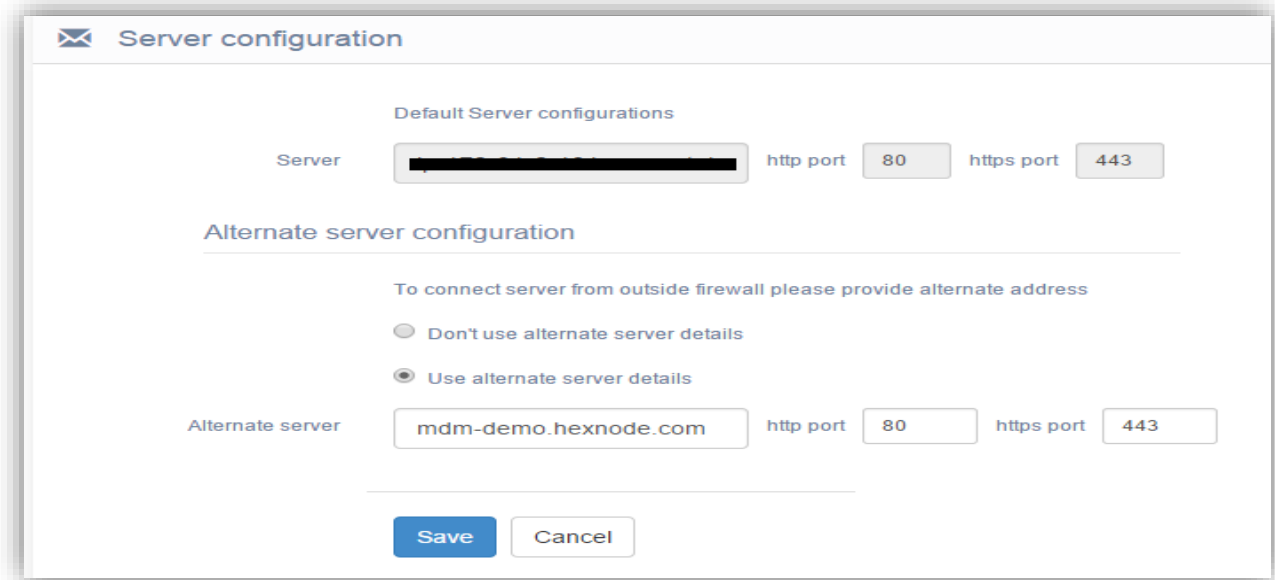
1. Log in to Hexnode MDM using the administrator credentials
2. Click on the Admin tab in the header section

Admin tab consists of the below sections below.

1. NAT settings
2. APNs settings
3. Proxy settings
4. Email Server settings
5. MDM settings
6. Server settings

NAT settings

NAT settings are necessary as we are managing all the mobile devices using one centralized system and the server should be reachable via public IP address. This helps Hexnode MDM to connect to mobile devices across the world through internet.



The screenshot shows a 'Server configuration' dialog box with the following sections:

- Default Server configurations:** Includes a 'Server' field with a redacted IP address, an 'http port' of 80, and an 'https port' of 443.
- Alternate server configuration:** Includes a heading 'To connect server from outside firewall please provide alternate address' and two radio buttons: 'Don't use alternate server details' (unselected) and 'Use alternate server details' (selected).
- Alternate server:** Includes an 'Alternate server' field with the value 'mdm-demo.hexnode.com', an 'http port' of 80, and an 'https port' of 443.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Default server configurations

Displays the details of configured server, communication port number and SSL port, which you have configured while installing the product.

Alternate server configurations

You can provide the details of the alias URL which will be available to the external users.

APNs settings

Apple Push Notification service (APNs) is a service created by Apple Inc. to handle the communication to apple devices from third parties.

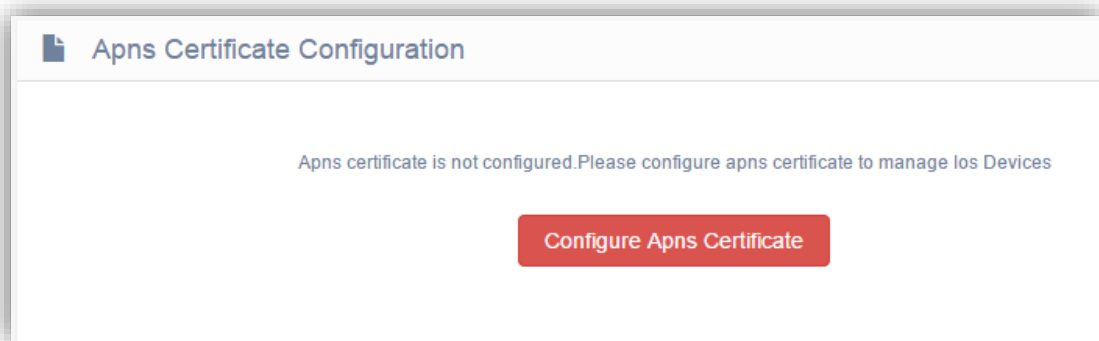
To communicate with an iOS device, Hexnode MDM server will first send a notification to APNS server and then the server will in-turn communicate with the device. The APNS server will act as a gateway of communication to all iOS devices. Hence we need the APNS certificate to authorize this communication from Hexnode MDM to iOS device.

APNS certificate is valid for one year from the date of creation. You need to renew the certificate after every 365 days. This process of renewing the certificate is same as creating a new one.

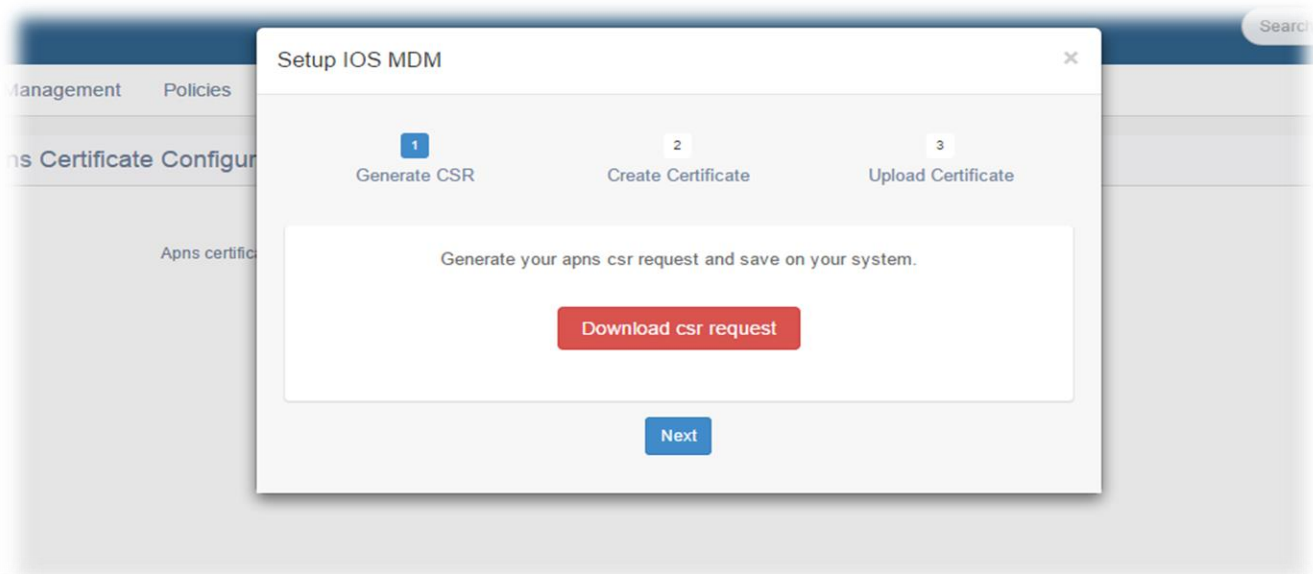
APNS configuration can be done in 3 simple steps.

Step 1: Create a CSR request

1. Go to Admin tab, click on APNs settings
2. Click on configure APNS certificate

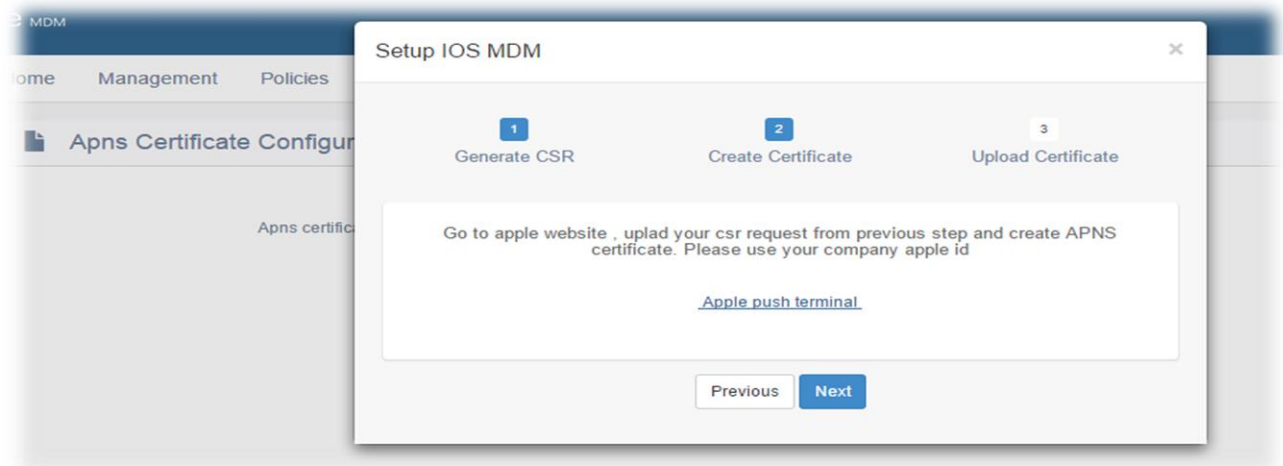


3. Download the self-signed-certificate from hexnode by clicking on download CSR request.

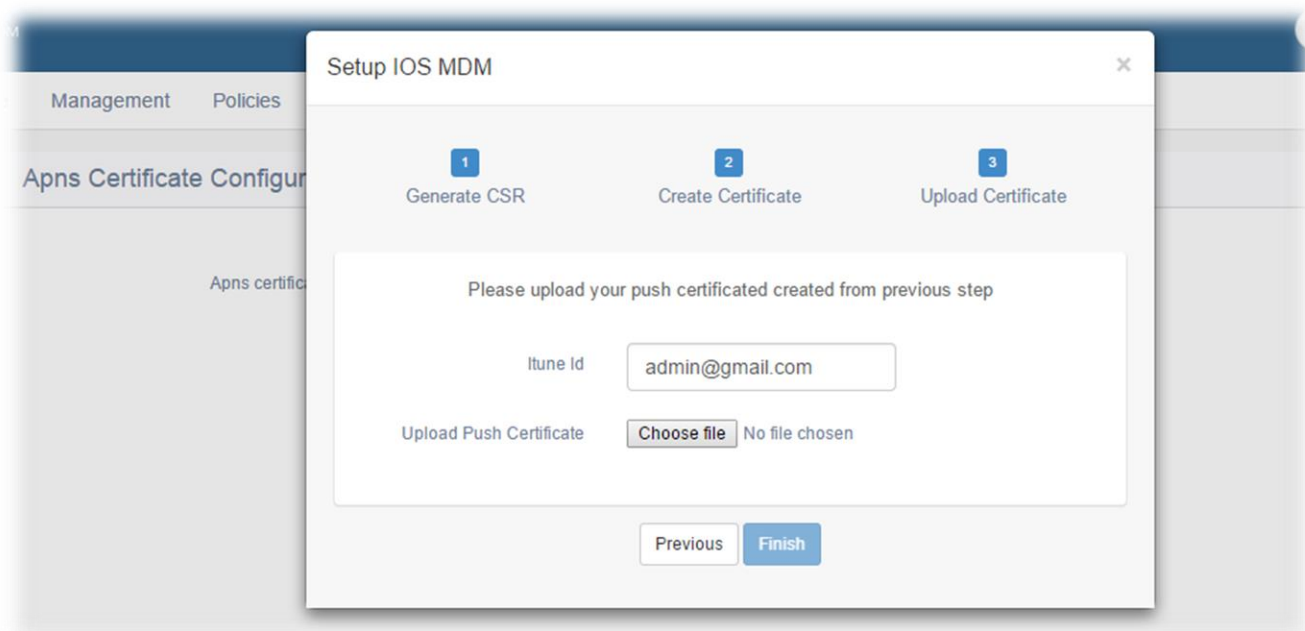


Step 2: Create Self Signed certificate and upload in the Apple Server

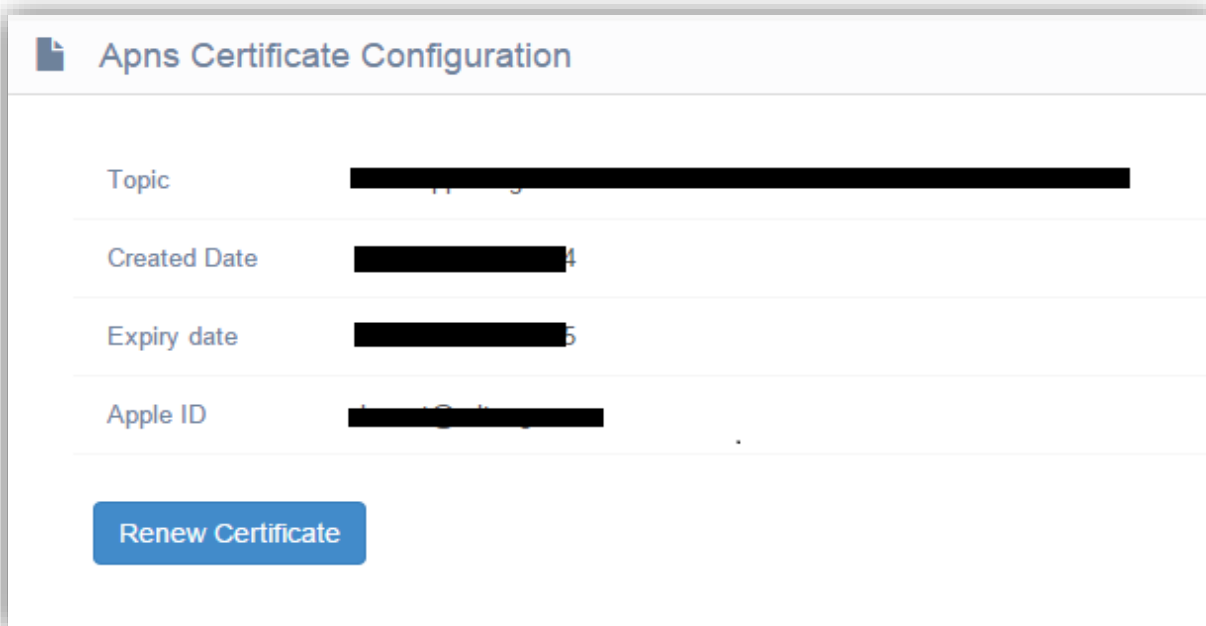
1. Once the certificate is created, go to the Apple website, then upload our self-signed-certificate
2. Create APNs certificate Here you need use your own company Apple id.
3. Apple's certificate push terminal link is provided in the product itself.



Step 3: Upload the APNs certificate back to the application by clicking on upload push certificate.



After applying the certificate, you will have the following details displayed under admin tab, APNs certificate.



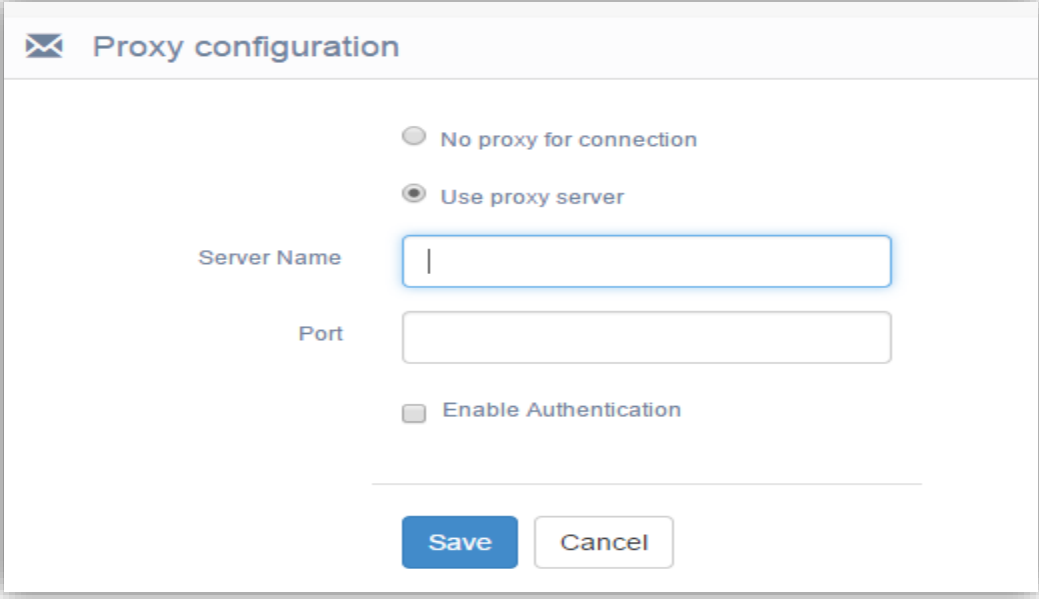
Renewing APNs certificate

ANPS certificate will have one year of validity from the date of creation, after which you need to renew the certificate. This can be done by clicking the option renew certificate, under the admin tab, APNS settings. Then you need to follow the same process of APNs certificate configuration.

Proxy Settings

You can configure proxy setting for MDM server, if required. While configuring/During configuration you need to provide the proxy server name (FQDN) or IP address and port number for the proxy.

If authentication is required for proxy settings, check the field Enable Authentication and provide username and password.



The image shows a 'Proxy configuration' dialog box with a title bar containing an envelope icon and the text 'Proxy configuration'. Inside the dialog, there are two radio buttons: 'No proxy for connection' (unselected) and 'Use proxy server' (selected). Below the radio buttons, there are three input fields: 'Server Name' (with a cursor), 'Port', and 'Enable Authentication' (a checkbox). At the bottom, there are two buttons: 'Save' (blue) and 'Cancel' (white with a blue border).

Configuring Email Server Settings

Hexnode MDM allows you to send email notifications to the end-users. The configurations for the Outgoing Email Server settings can be set up from admin tab, email server settings.



The image shows an 'Email server configuration' dialog box with a title bar containing an envelope icon and the text 'Email server configuration'. Inside the dialog, there are six input fields: 'Server Name', 'Port' (with the value '587'), 'Sender Email', 'User Name', and 'Password' (masked with dots). There are also three checkboxes: 'Enable TLS', 'Enable SSL', and 'Enable Authentication', all of which are checked. At the bottom, there are two buttons: 'Save' (blue) and 'Cancel' (white with a blue border).

You need to mention the following mandatory fields for outgoing emails to work.

Server name: Outgoing email server name or IP address of the email service provider

Port number: Communication port number of the email server

Sender's email address: The email address used for sending emails

Enable TLS: Select this option, if Transport Layer Security is enabled in the mail server.

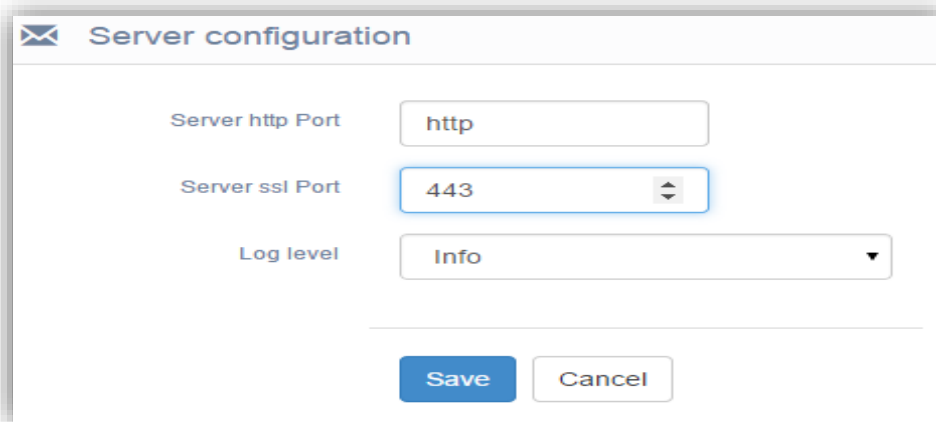
Enable SSL: Check this option, if SSL (Secure Socket layer) is enabled.

Enable Authentication: If outgoing email authentication is required in the email server, choose this option and provide the credentials required for authenticating the outgoing emails.

Once all the configurations are entered, Save the settings.

Server Settings

The basic server settings such as changing the application web server port, SSL port and logging level can be configured from here.



The screenshot shows a 'Server configuration' window with a light blue header and a white body. It contains three configuration items: 'Server http Port' with a text input field containing 'http', 'Server ssl Port' with a spinner box containing '443', and 'Log level' with a dropdown menu showing 'Info'. At the bottom are 'Save' and 'Cancel' buttons.

Server HTTP port

You can change the default web port assigned for the application's communication from here. The port should be opened from the Hexnode MDM server.

Server SSL port

If you wish to change the default SSL port assigned, you can configure it from this section. The port should be opened from the Hexnode MDM server.

LOG level

Option to set up the level of logs that need to be captured according to the severity of the issue occurred.

Info: This log level traces the normal operations happening in the application.

Debug: Provides detailed information about the failure occurred which will be useful for the developers

Error: Traces non-urgent failures, these should be relayed to developers or admins.

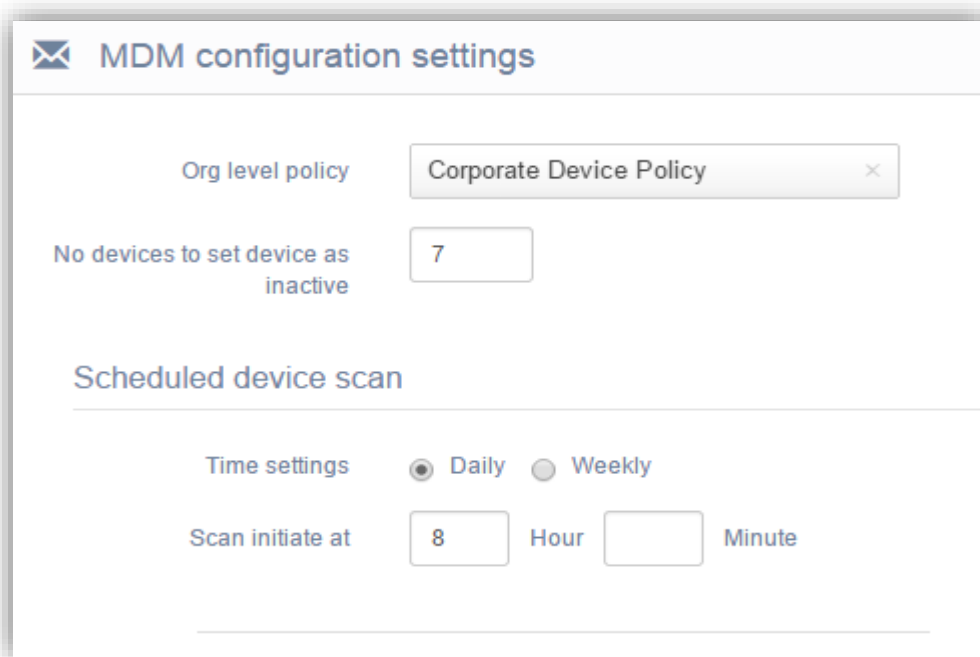
Critical: Captures fatal errors which need to be fixed immediately.

MDM settings

The default settings of mobile device scan, default organization policy and the scan schedule can be configured from this section.

Org Level Policy

This section allows you to choose the default policy which will be applicable for all employees in the Organization.



The screenshot shows the 'MDM configuration settings' window. It has a title bar with an envelope icon and the text 'MDM configuration settings'. Below the title bar, there are three main sections. The first section is 'Org level policy' with a dropdown menu showing 'Corporate Device Policy'. The second section is 'No devices to set device as inactive' with a text input field containing the number '7'. The third section is 'Scheduled device scan' with a sub-section 'Time settings' containing two radio buttons: 'Daily' (selected) and 'Weekly'. Below this, there is a 'Scan initiate at' section with a text input field containing '8', followed by 'Hour' and 'Minute' labels, and another empty text input field for minutes.

Number of days to set Scan as inactive

You can set the number of days at which the device will be set as inactive, if not scanned.

Scheduled scan settings

The Schedule scan of the mobile devices can be configured here. The scan fetches the data of enrolled devices into the application and update the details periodically. You can set the schedule of the scan daily or weekly according your business needs.

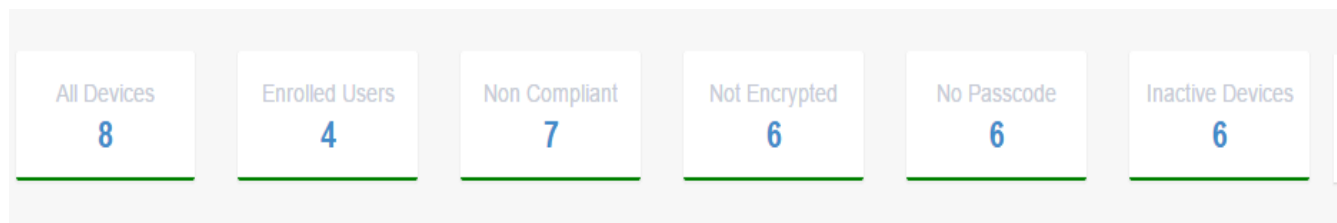
Home Tab - Mobile Device Management Dashboard

The home page gives a quick overview of your entire mobile ecosystem. The integrated dashboard simplifies management, streamlines the monitoring process and helps in quicker resolution of compliance issues. The centralized console model ensures consistency among the devices in case of configuration profiles and policies applied. Admins can either have a quick glance of activity summary or invoke detailed information about individual devices.

Home page displays the below sections below.

1. Ribbon that shows the summary of mobile devices
2. BYOD statistics widget
3. Compliance graph
4. List of Recently enrolled devices
5. List of inactive devices
6. List of Non-Compliant devices
7. Activity Feed

Ribbon that shows the summary of mobile devices



Total Devices: Shows the total number of mobile devices

Enrolled Users: Displays the number of users enrolled with one or more devices

Non-Compliant: Displays the number of enrolled devices, meeting all compliance criteria specified under device summary

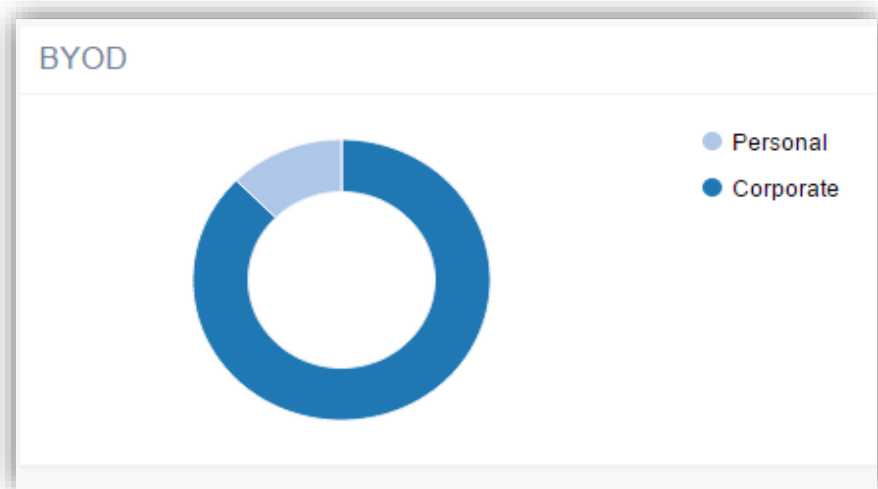
Non-encrypted: Represents the total number of enrolled devices that have data protection enabled.

No Passcode: Shows the count of devices without configuring screen passcode.

Inactive Devices: Devices which are not scanned into the application for a particular number of days. The number of days here, is a configurable option under admin tab > MDM settings.

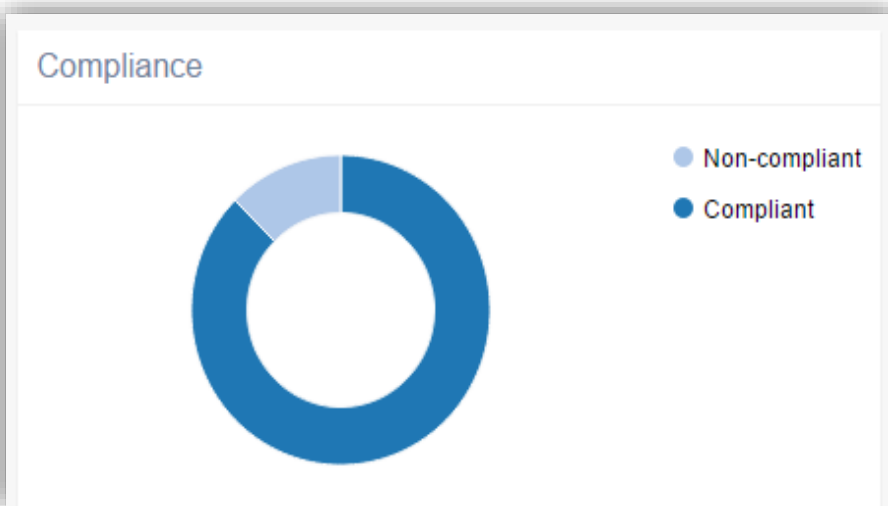
BYOD (Bring Your Own Device) Summary Graph

The widget displays a ring chart, which showcase the count of personal and corporate devices of the employees.








Compliance statistics widget

This ring chart displays the statistics of compliant and non-compliant devices.








Recently enrolled mobile devices

This section provides the details of newly enrolled device names, its ownership and time since enrollment has done.

Recently Enrolled Devices		
Sahad	 suhanna	2 hrs
Mitsogo I	 Rachana	2 ds
Sahad	 sahad mitz	10 ds
John's Ipad	 Rachana	11 ds
IPhone	 Grace Williams	14 ds






Inactive devices

This section shows the details of the enrolled devices which are not scanned into the application for a particular number of days. The number of days here, is a configurable option under Admin tab > MDM settings > Number of days to set the device as inactive.

Inactive Devices		
Sahad	 suhanna	2 hrs
Sahad	 sahad mitz	10 ds
John's Ipad	 Rachana	11 ds
Sahad	 Sahad	16 ds
John's Ipad	 John Doe	20 ds






Non-Compliant devices

This section gives the description of enrolled devices, which meet all the compliance criteria given under device summary section.

Non compliant		
Sahad		
 suhanna		2 hrs
Mitsogo I		
 Rachana		2 ds
Sahad		
 sahad mitz		10 ds
John's Ipad		
 Rachana		11 ds
Sahad		
 Sahad		16 ds

Activity Feed Widget

This event based timeline shows the device name, user name, type of action and days passed after the activity has done. This provides the IT managers with better insights on the application status.

Activity feed		
	John Doe IOS De...	20 ds
	Device apns details updated	
	Martin Lewis IOS ...	20 ds
	Device Enrolled	
	Martin Lewis IOS ...	20 ds
	Device apns details updated	
	Fhh IOS Device	16 ds
	Device Enrolled	
	Fhh IOS Device	16 ds
	Device apns details updated	

Instant “Enroll “button

There is a quick enrollment option available on dashboard home, to enroll the users instantly. Follow the below steps to enroll a device into the application.

- 1.Go to Enrollment tab, click on New Enrollment Option
2. Select the user or add a new user.
- 3.Select the type of the device, whether it is corporate, personal or allow user to choose.
- 4.Click on Send enrollment request.

Instant “Add policy” button

Follow the steps to configure new policy

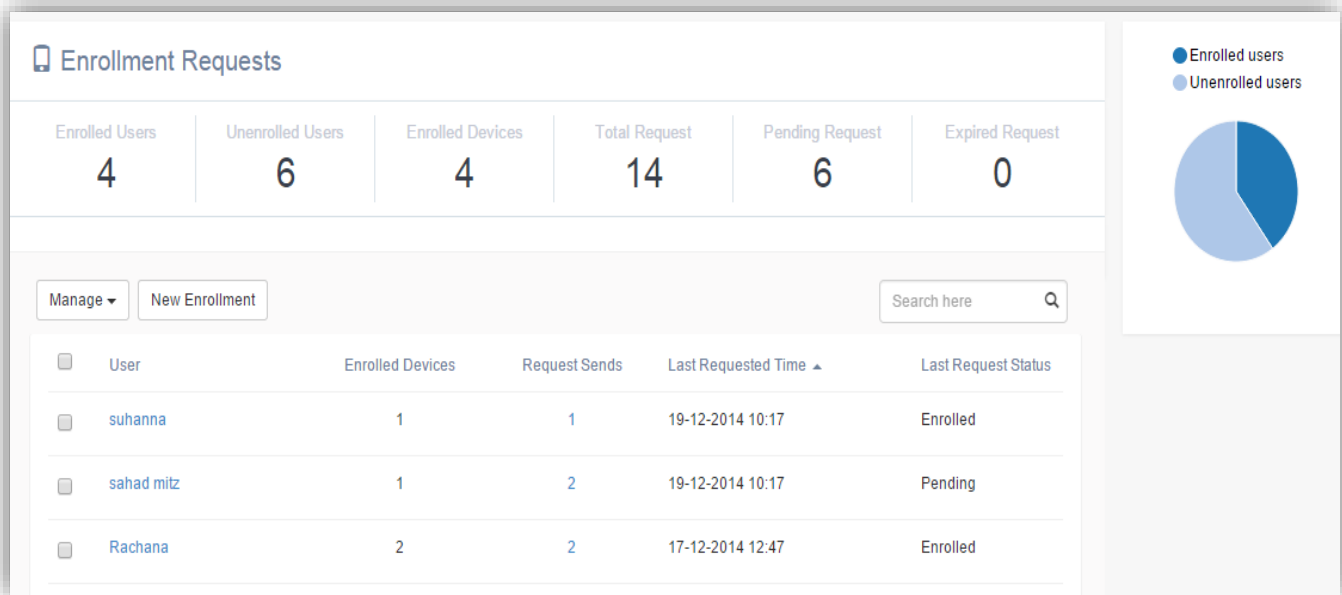
- 1.Go to Policy tab, Click on new policy
2. Add the policy name and description of the policy
- 3.Go to iOS policy setting and choose the required settings.
- 4.Add the policy target, under which you need to associate the user/devices/groups.

Enrollment Tab

Enrollment module handles the enrollment of devices over-the-air or through LAN/Wi-Fi. This is the first step of managing mobile devices in an organization. Hexnode provides quick and easy enrollment process to get the devices managed effectively.

Ribbon panel of enrollment status

This indicates the current enrollment status and the state of requests sent:



The graph on the right-top-panel shows the statistics of enrolled and unenrolled users.

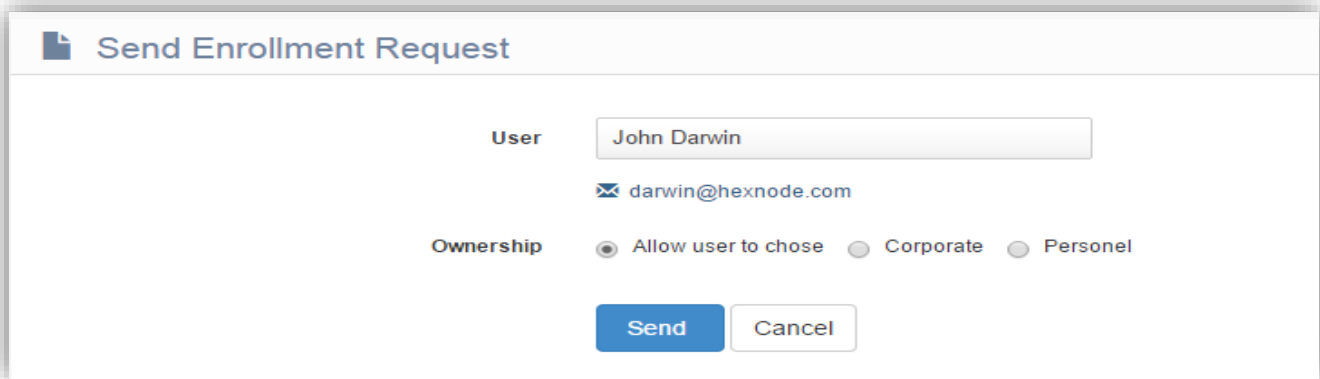
Search Allows you to search for a particular device.

Enrolling devices

Follow steps below to enroll a device into the application.

1. Under Enrollment tab, click on New Enrollment Option
2. Select the user or add the new user.

3. Select the type of the device, whether it is corporate, personal or allow user to choose.



The image shows a web form titled "Send Enrollment Request". It has a "User" section with a text input field containing "John Darwin" and an email icon with the address "darwin@hexnode.com". Below this is an "Ownership" section with three radio buttons: "Allow user to chose" (which is selected), "Corporate", and "Personal". At the bottom are two buttons: "Send" and "Cancel".

4. Click on Send enrollment request.

Make sure that you have configured the email server settings under admin tab, so that users will receive the enrollment email without fail.

How to enroll iOS devices

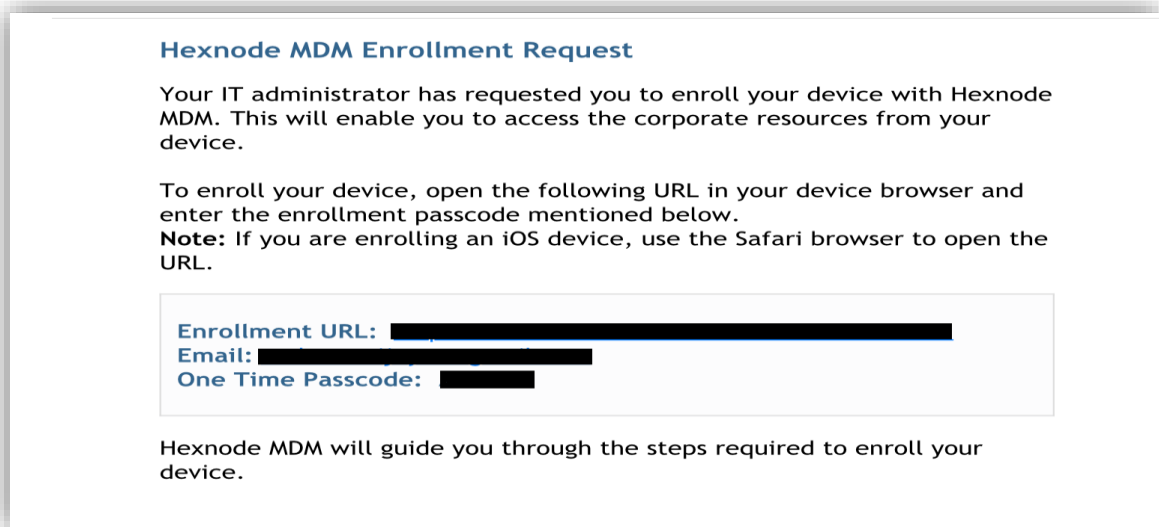
We have made the enrollment process very quick and easy for the end users.

The administrator sends the end user, an email containing the enrollment link. User needs to

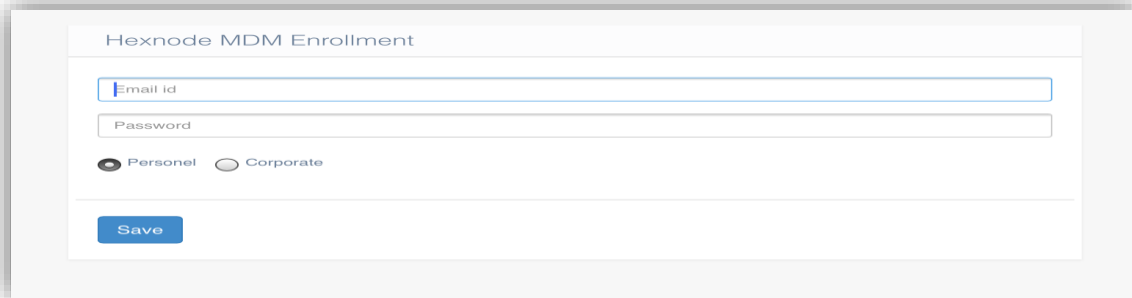
1. Tap on the link and type the one-time passcode provided in the email.
2. Tap on the install button to install the Hexnode MDM profile

Once the profile is successfully installed, the enrollment process is complete

Here is a sample enrollment process. The enrollment email is sent to the end user:

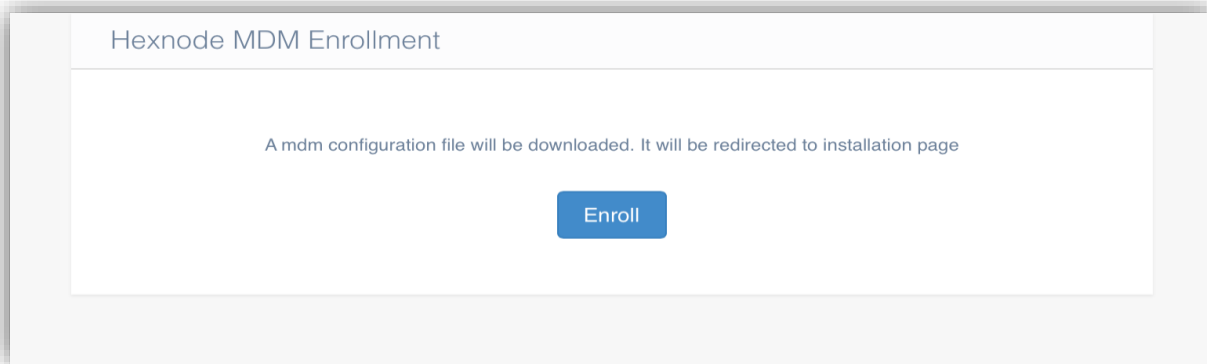


The image shows a sample email content for a "Hexnode MDM Enrollment Request". It starts with a heading "Hexnode MDM Enrollment Request". The body text says: "Your IT administrator has requested you to enroll your device with Hexnode MDM. This will enable you to access the corporate resources from your device." It then says: "To enroll your device, open the following URL in your device browser and enter the enrollment passcode mentioned below." A note follows: "Note: If you are enrolling an iOS device, use the Safari browser to open the URL." Below this is a box containing three lines of text: "Enrollment URL: [redacted]", "Email: [redacted]", and "One Time Passcode: [redacted]". At the bottom, it says: "Hexnode MDM will guide you through the steps required to enroll your device."

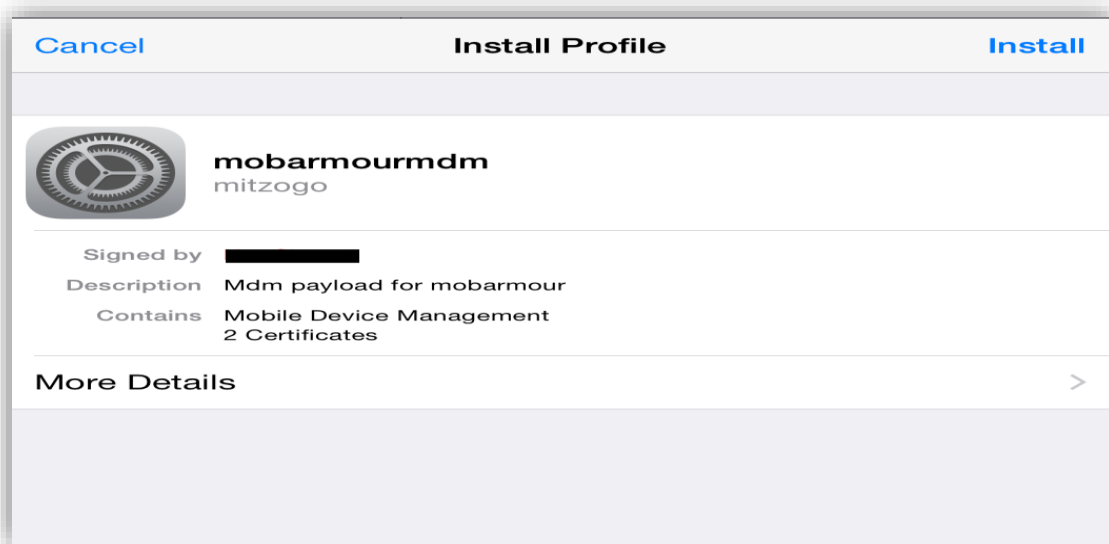
A screenshot of a web form titled "Hexnode MDM Enrollment". It contains two input fields: "Email id" and "Password". Below these fields are two radio buttons labeled "Personel" (with a typo) and "Corporate". At the bottom of the form is a blue button labeled "Save".

The user need to enter the email address and passcode here.

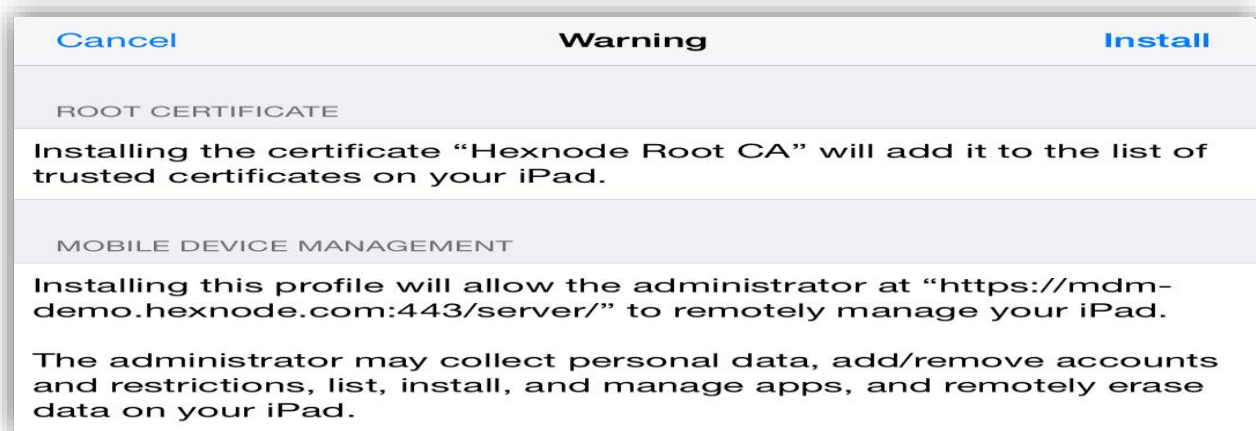
The MDM configuration file will be downloaded and the user needs to tap on enroll button.

A screenshot of a web page titled "Hexnode MDM Enrollment". It displays a message: "A mdm configuration file will be downloaded. It will be redirected to installation page". Below the message is a blue button labeled "Enroll".

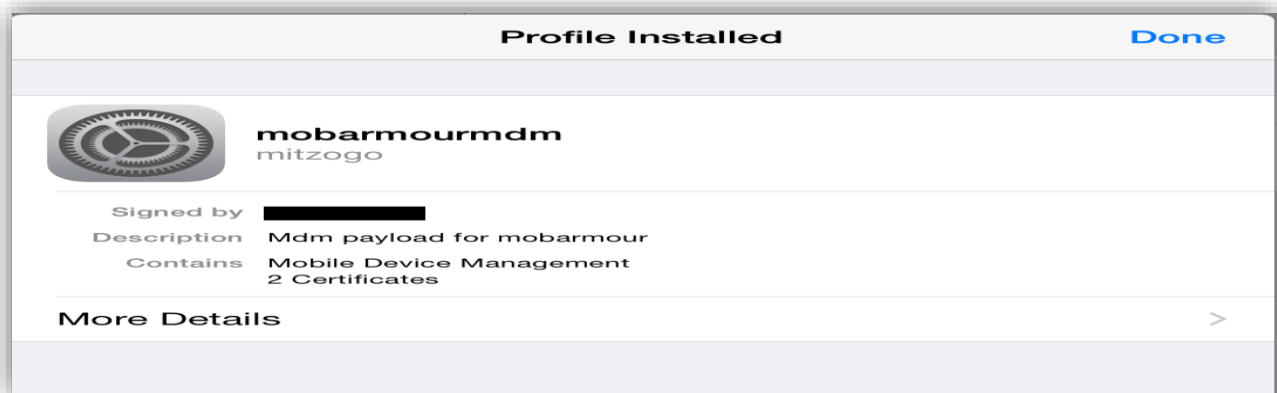
Tap on "install" button to install the profile.

A screenshot of an iOS "Install Profile" dialog. The title bar has "Cancel" on the left, "Install Profile" in the center, and "Install" on the right. The main content area shows a profile icon (a gear with a stylized 'M') and the name "mobarmourmdm" by "mitsogo". Below this, it lists details: "Signed by" (redacted), "Description" "Mdm payload for mobarmour", and "Contains" "Mobile Device Management" and "2 Certificates". At the bottom, there is a "More Details" link with a right-pointing chevron.

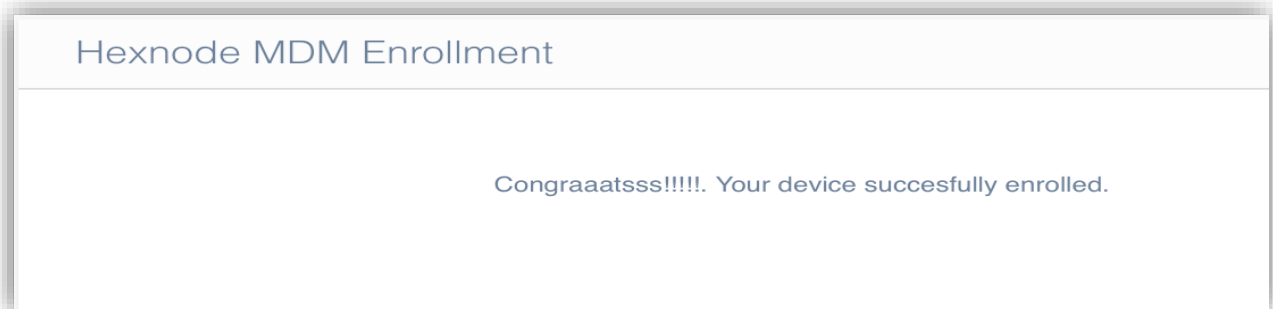
It takes the user to the terms and conditions page. He has to click on install button to proceed installation.



User will get the message below, when the profile installation is over.



The below message will be displayed when the device is successfully installed.

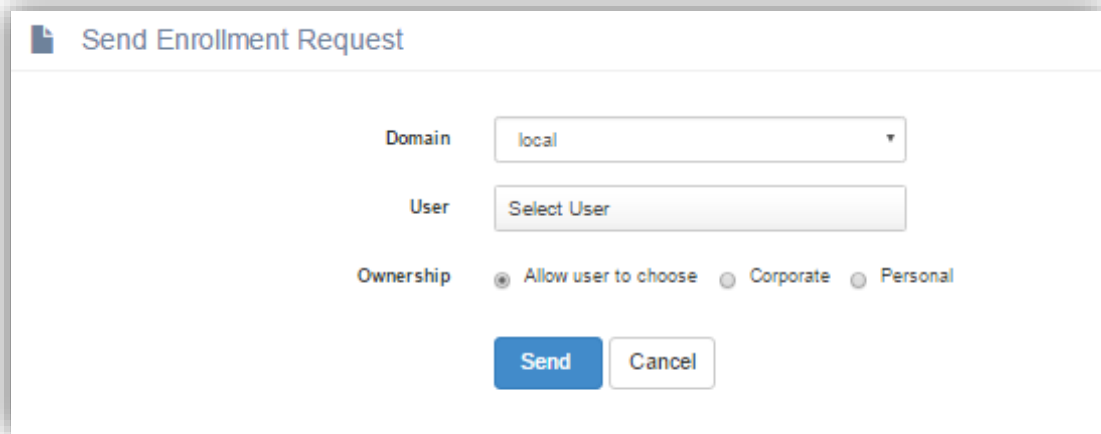


How to enroll Android devices

The enrollment process for an android device is a little different from that of an iOS device. It is a two-step process. First step is to send an enrollment request from Hexnode MDM and second step is to install the Hexnode app on the device and complete enrollment. The initial step to send an enrollment request is similar to that of an iOS device but is listed here again for ease.

Send Enrollment Request

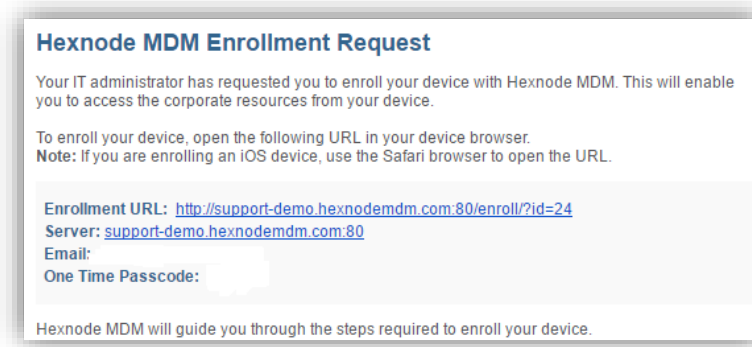
1. Go to Enrollment tab, click on New Enrollment button.



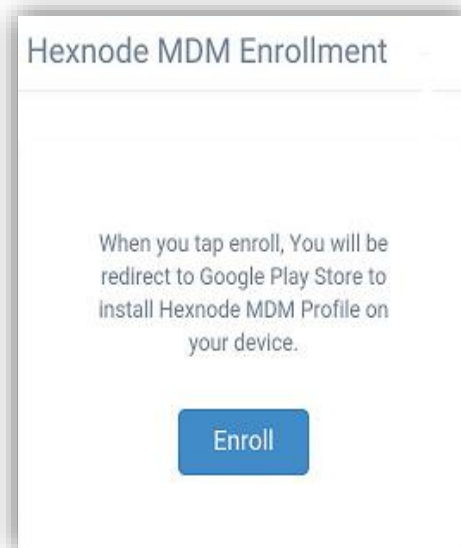
2. Following screen appears
3. Enter information like domain, user to which the enrollment is to be sent. If the user doesn't exist, create a new user first from Management > Users > New User.
4. Enter ownership information
 - a. Allow user to choose – if the user needs to provide this information at the time of installation on the device.
 - b. Corporate – if the device being used is a corporate device
 - c. Personal – If the user is bringing his own personal device.
5. Click on send button to send an invite to the user. This sends an invite mail to the user.

Install App and complete Enrollment process

1. Once the enrollment request is sent to user, user receives an email with details.
2. A sample email is shown below:



3. Open the enrollment URL in the same device which needs to be enrolled. It shows the following screen.

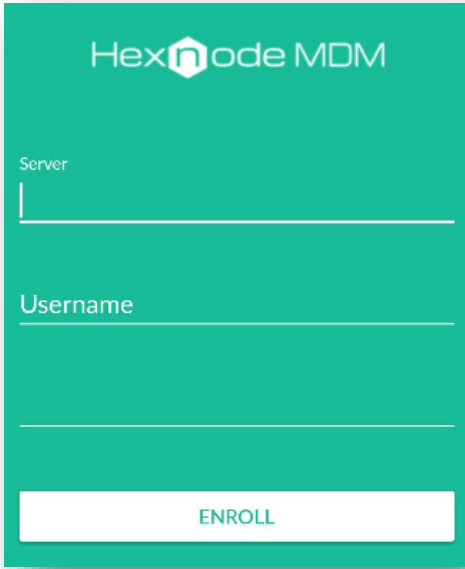


4. Click on Enroll button.

It will redirect you to google play store to download and install Hexnode MDM Profile.

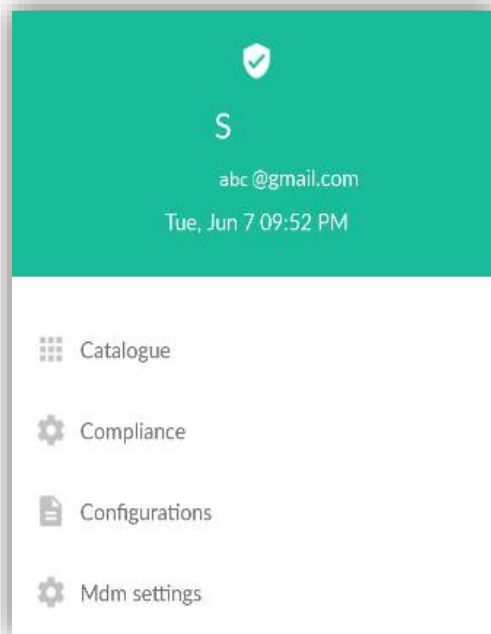


5. Click on Install and once installed, open the application in the device. It will show a page as shown below.

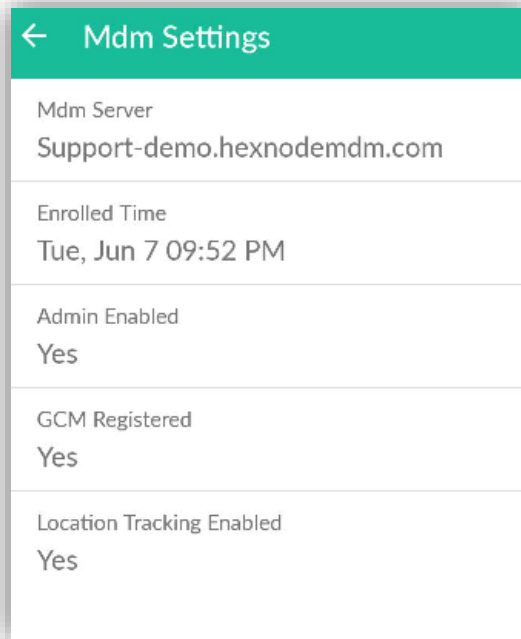
The image shows the Hexnode MDM enrollment screen. It has a teal background. At the top, the 'Hexnode MDM' logo is displayed in white. Below the logo, there are two input fields: 'Server' and 'Username', both with white text labels and white input lines. At the bottom, there is a white button with the word 'ENROLL' in teal capital letters.

Enter the Server details, username and password information as received in the initial enrollment email. Click on Enroll.

6. Once the authentication is done, the device is successfully enrolled with Hexnode MDM. Following screens will activate device administration through Hexnode MDM. Once activated, the app shows the policies and compliance status of the device, catalogues attached to the device and MDM settings for the device.

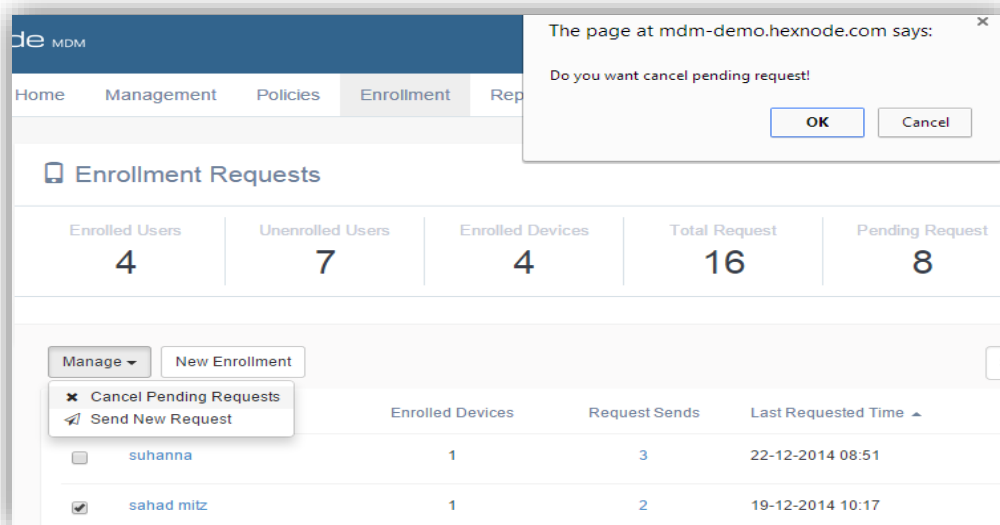


- Catalogue lists the app catalogues assigned to the device.
- Compliance lists the compliance status of the device
- Configurations lists the policies related stats of the device.
- MDM settings has information related to various device properties as shown below.



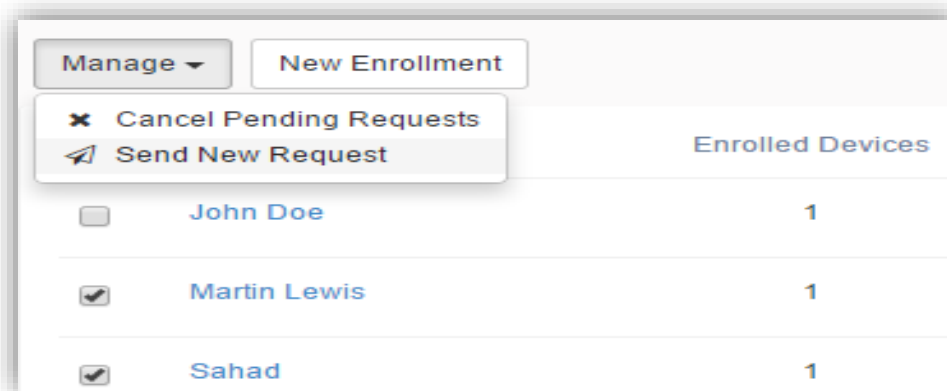
Cancel Pending request

You can cancel the request sent for enrollment under enrollment tab > go to enrollment list view > select the request(s) > cancel request. Once this is done, the enrollment link will no longer be active.

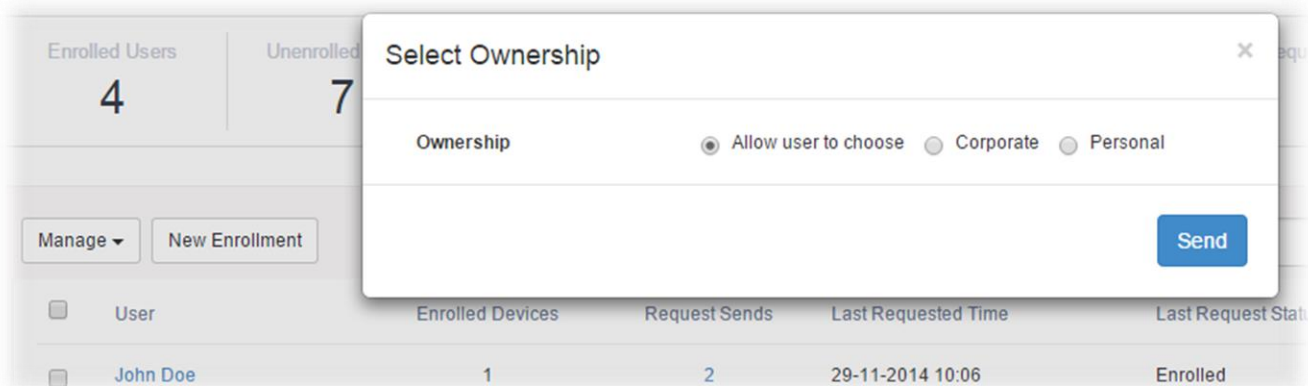


Send New request

You have the option to resend the enrollment request to a device or to multiple devices. Go to enrollment tab > choose the user(s) > click on manage > send new request.



You need choose the type of ownership of the devices before sending the request.



Sorting the enrollment list view

Sorting can be done just by clicking on the column name. It sorts and groups in ascending or descending order. e.g.: sorted by user name

<input type="checkbox"/>	User	Enrolled Devices	Request Sends	Last Requested Time	Last Request Status
<input type="checkbox"/>	John Doe	1	2	29-11-2014 10:06	Enrolled
<input type="checkbox"/>	Martin Lewis	1	2	05-12-2014 10:24	Pending
<input type="checkbox"/>	Sahad	1	1	03-12-2014 12:17	Enrolled

Enrollment request status

Enrollment status can be viewed by clicking on the “request send “in the enrollment request list view.

Enrollment request of Martin Lewis			
Time	Status	Device	Remarks
5/12/2014 15:12	Pending		
29/11/2014 15:11	Enrolled	Martin	Successfully Enrolled

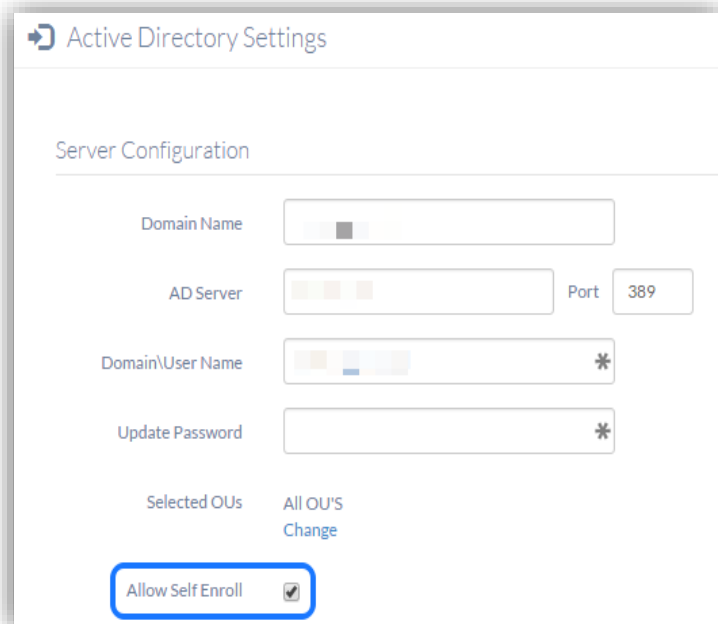
Self Enrollment

Self Enrollment spares you the hassle of sending enrollment requests to every user. When self enrollment is turned on users can directly enroll their devices from the portal.

Self enrollment makes use of the users' AD credentials for authentication. Hence AD users alone can be enrolled likewise. Self enrollment is not a global option; you can selectively enable it for different domains.

To enable self-enroll,

Select Admin > AD Settings



Active Directory Settings

Server Configuration

Domain Name

AD Server Port

Domain\User Name *

Update Password *

Selected OUs All OU'S Change

Allow Self Enroll ☒

Click on any of the AD slots to edit settings. Select the Allow Self Enroll checkbox to turn on self enrollment for the users in this particular domain. If it is deselected, authentication fails and users won't be able to enroll their device.

CSV import

Hexnode MDM allows you to send out enrollment requests in bulk by importing users from a CSV file. CSV import comes in quite handy while having to send out enrollment requests to a large number of users in your AD.

For CSV import,

Select Home > Enrollment

Click on Bulk Enrollment. First, let's send requests to local users. For Domain, choose local. If you have a CSV file in the prescribed format, you can upload it. Else download a sample CSV file by clicking on the Sample CSV at the top right corner. You can use this file as format reference.

Send Bulk Enrollment Request

Sample CSV

1 Upload CSV 2 Verify CSV 3 Summary

Domain local

Select CSV File Choose file No file chosen

Next Cancel

Now click choose file and select the sample_csv file. Click next. Here you can verify the entries. Keep the required ones selected and click next. You'll receive a confirmation. Click send and the enrollment requests will be sent to the selected users. For sending requests to AD users, at the bulk enrollment request screen, select the CSV file, choose an AD domain and click next. Hexnode MDM shows the list of matching domain users in the CSV file. You can select the required users and send them requests likewise.

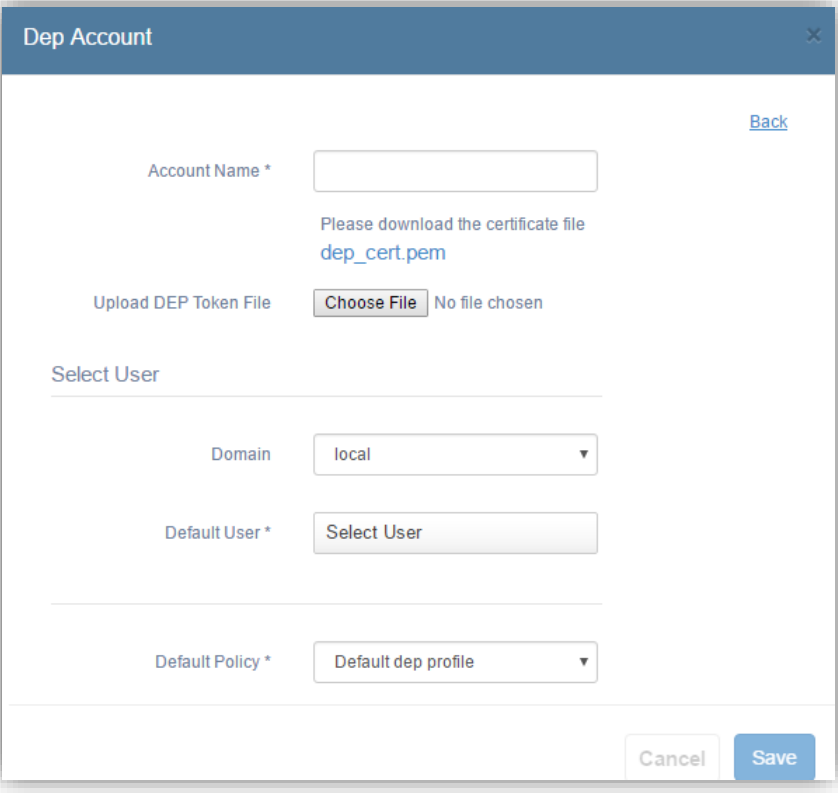
DEP Management

Device Enrollment Program or DEP enables automatic deployment of your corporate Apple devices. Once a device is activated, it is immediately configured without the need for IT to physically do it. Following documentation will explain how to use Apple DEP with Hexnode MDM.

Dep Settings

To integrate Hexnode MDM to Apple DEP, admin must do the following settings

- Go to Admin
- Click DEP
- Click DEP Settings button on the top.



The screenshot shows a web form titled "Dep Account" with a close button (X) in the top right corner. The form contains the following fields and elements:

- Account Name ***: A text input field.
- Back**: A blue link in the top right corner.
- Please download the certificate file**: A text label.
- dep_cert.pem**: A blue link for downloading the certificate file.
- Upload DEP Token File**: A section containing a **Choose File** button and the text "No file chosen".
- Select User**: A section header.
- Domain**: A dropdown menu with "local" selected.
- Default User ***: A dropdown menu with "Select User" selected.
- Default Policy ***: A dropdown menu with "Default dep profile" selected.
- Cancel** and **Save** buttons: Located at the bottom right of the form.

Apart from information like Account name, default user and policy, it needs a DEP token file to be uploaded. Here are the steps to generate this token.

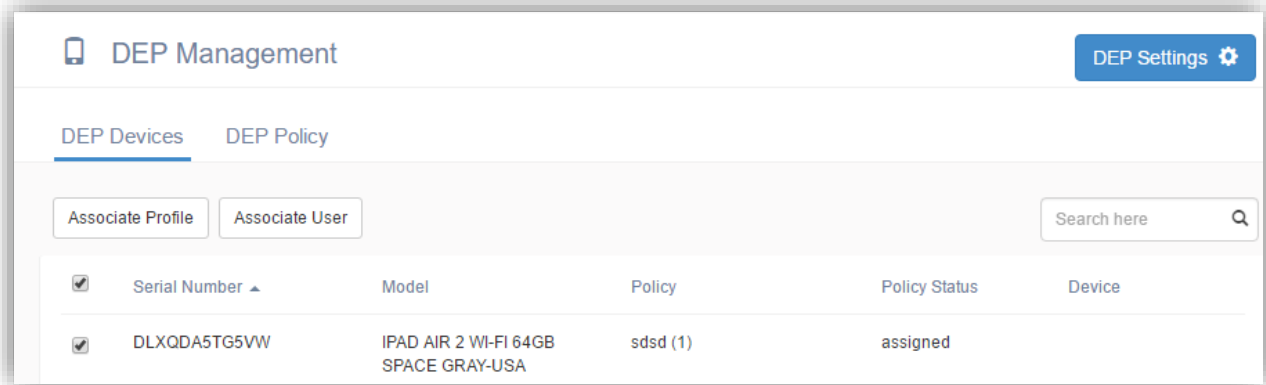
1. Download the certificate file dep_cert.pem
2. Go to <https://deploy.apple.com/> and login with your apple ID
3. Navigate to Device Enrollment Program and add MDM server.
4. Choose a suitable name and upload the certificate file downloaded in step 1.
5. Download the server token file provided.

Renew a DEP Token

Apple DEP tokens need to be renewed every year. Follow the above steps and upload new token before your previous token expires.

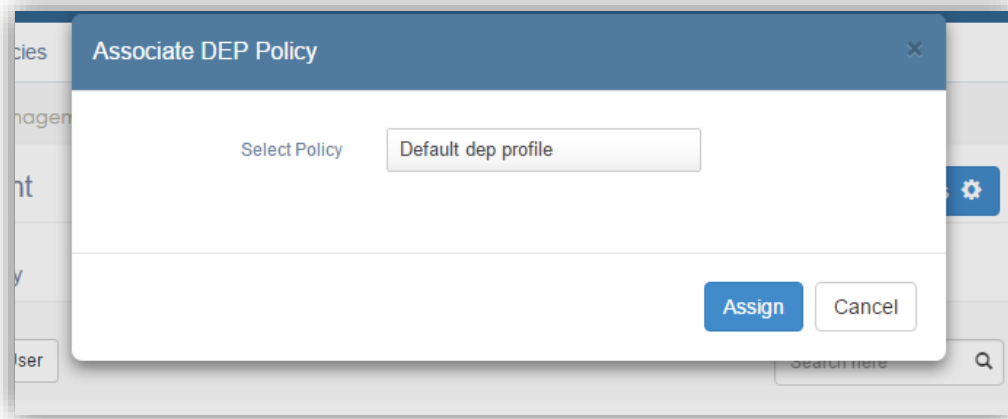
DEP Devices

By default, this page lists the devices enrolled under this program. It shows the device serial number and model along with the DEP policies assigned, if any to the device.



To associate a device with a profile

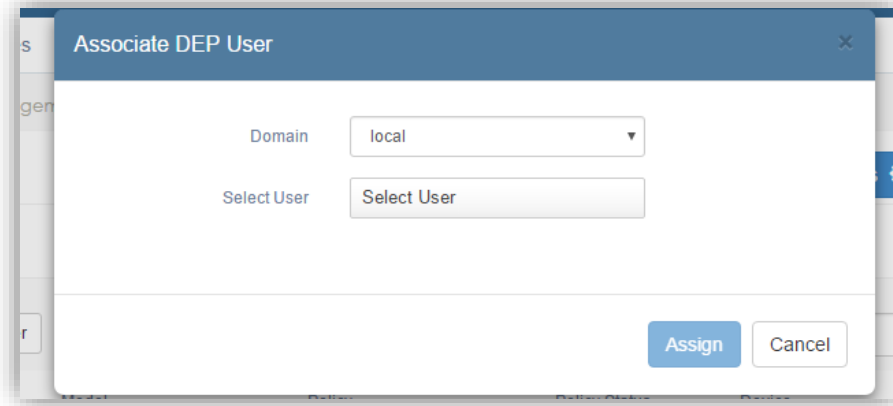
1. Select the device.
2. Click Associate Profile button on the top. The following window pops up.



3. Select the profile to be assigned and click 'Assign'.

To associate a device to a user

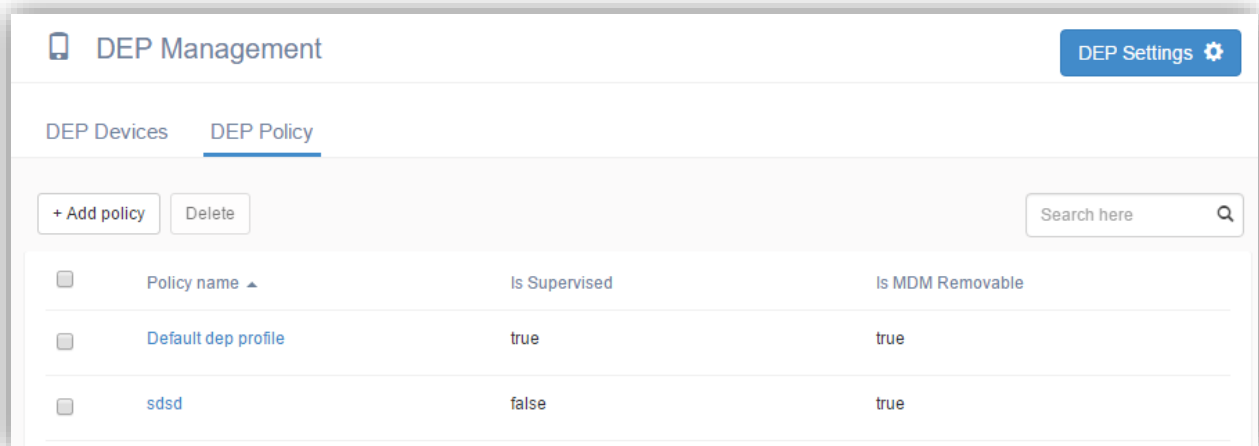
1. Select the device
2. Click 'Associate User' button. Following window pops up.



3. Select the domain and user and click Assign button.

DEP Policies

By default, this page lists all the existing DEP policies.



To see the details of any policy

1. Click on its name
2. The following screen pops up with detailed information about the policy.

Dep Policy

Display Name: Default dep profile

Department:

Support Phone Number:

Mandatory: ☒

Supervised: ☒

Allow Pairing: ☒

Removable: ☒

Is Multi user: ☒

Skip Steps: ☒ Location ☒ Restore
☒ Apple ID ☒ TOS
☒ Diagnostics ☒ Siri
☐ Passcode ☒ Registration
☒ Biometric ☒ Payment
☒ Zoom ☒ FileVault

You can also edit the policy on this page and save it again.

To add a new policy

1. Click the '+Add Policy' button. It pops up a blank policy page.

Dep Policy

Display Name:

Department:

Support Phone Number:

Mandatory: ☐

Supervised: ☐

Allow Pairing: ☒

Removable: ☒

Is Multi user: ☐

Skip Steps: ☐ Location ☐ Restore
☐ Apple ID ☐ TOS
☐ Diagnostics ☐ Siri
☐ Passcode ☐ Registration
☐ Biometric ☐ Payment
☐ Zoom ☐ FileVault

Cancel Save

2. Configure your policy settings and click save.

Here is the description of the configuration parameters for a policy.

- **Display name** - A friendly name of the policy
- **Department** - Department name to which the devices are assigned
- **Support Phone Number** – Contact number for users if they need help during setup
- **Mandatory** - Check this, if it is mandatory for users to complete enrollment during setup
- **Supervised** - Check this, if the devices under this policy are supervised upon enrollment
- **Allow pairing** - Check this, if the devices can be paired with a computer
- **Removable** - Check this, if this profile is removable
- **Is multi user** - Check this, if a device can have multiple users
- **Skip steps** - Hexnode MDM DEP allows for a customized setup Experience. Check the options which are allowed to be skipped during setup.

VPP settings

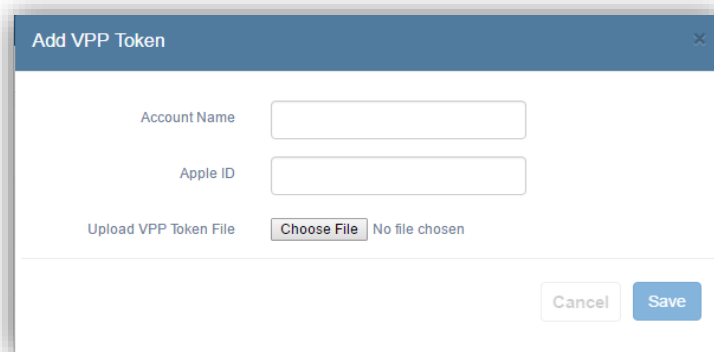
VPP refers to Apple Volume Purchase Plan which allows you to buy and distribute applications in bulk and then assign them to specific devices/users in the organization. This is a three-step process – creating an apple VPP account and configuring Hexnode MDM for distribution and sending invites to the users.

To create an apple account:

Refer to the link <http://www.apple.com/business/vpp/> and create an account for your business.

To configure VPP settings in Hexnode MDM:

1. Click on Admin tab > VPP settings.
2. To do the following settings, you need a VPP token. This token can be downloaded from the Apple site.
 - a. Go to <https://vpp.itunes.apple.com>.
 - b. Login with your Apple VPP account credentials.
 - c. Go to Account summary
 - d. Download token and save it. This file is a .vpptoken type.
3. Hexnode MDM VPP settings page, click the button labelled 'Add VPP token'. This opens a new form as shown below.
4. Enter your account name, Apple ID and upload the VPP token file downloaded in step 2 above and click 'Save' button. MDM server is now linked to your Apple VPP account.



The screenshot shows a web form titled "Add VPP Token". It contains three input fields: "Account Name", "Apple ID", and "Upload VPP Token File". The "Upload VPP Token File" field includes a "Choose File" button and the text "No file chosen". At the bottom right, there are "Cancel" and "Save" buttons.

To invite users

1. After the MDM server has established link to the VPP account, go to Management tab.
2. Click on Users.
3. Select one or more users whom you want to send the invite and click on Manage button.
4. Select 'Send VPP invitation' from the list.
5. This will send the invite to all the selected users.

The VPP Settings page also lists the accounts already added to the Hexnode MDM server as shown below.



For every account, it gives additional options to sync and manage.

Sync button, when pressed fetches the updated information about the total assets or users currently being used under this account.

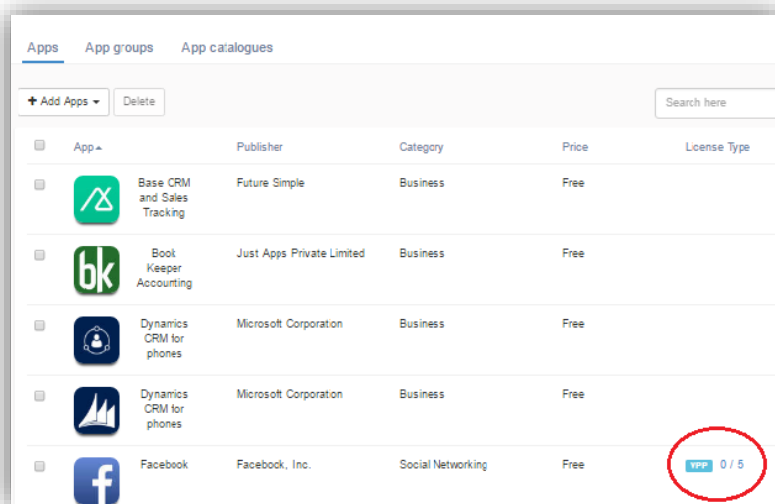
Manage button gives an option to delete any existing account.

App License information

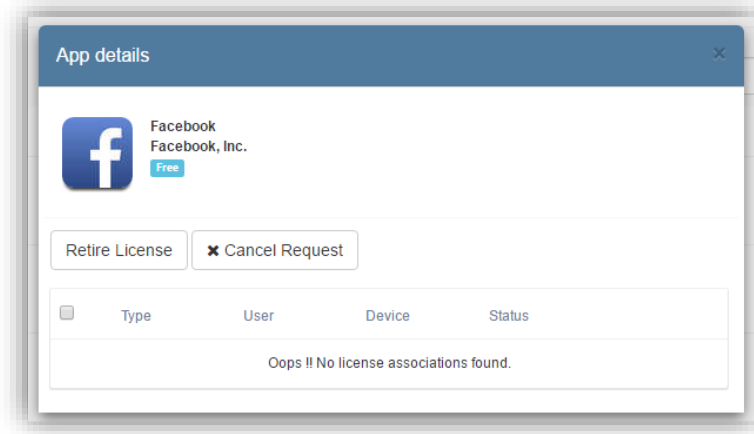
On devices with iOS 9 and above, whenever a VPP app installation is initiated, the license will be automatically assigned to the device.

To retire this license:

3. Go to Admin tab
4. Click App Settings
5. Go to Apps
6. The list of apps is shown.



7. For apps, which are VPP type, License Type column shows VPP.
8. Click on VPP, it opens another window which gives option to Retire License.



9. Select the device and click 'Retire License' button.

Policy Management

The enrolled devices can be managed and controlled through automated policy enforcement. Policy Management helps in assigning profiles to the device(s)/user(s)/group(s) over-the-air.

When a policy is associated to a device/user/groups, it will get immediately applied as soon as the device is reachable. Similarly, in case of profile removal, the restrictions will be taken off as soon as the profile has been removed from the entity.

Hexnode MDM provides an extensive set of policy controls for effective device management. From passcode policies and group policies to configurations and restrictions: you get ample control over the devices in your network.

- ✓ **Passcode policies:** Secure your content and network by enforcing strong passcode policies on the devices.
- ✓ **Device configuration:** Configure corporate email accounts, ActiveSync, CalDav, CardDav and calendar and setup Wi-Fi, VPN and network configuration settings easily.
- ✓ **Device restrictions:** Enforce restrictions on the use of YouTube, camera, Siri etc.
- ✓ **Group based policies:** Create virtual groups based on the organization structure or import from corporate directories. Separate BYOD and Enterprise devices. Seamlessly associate policies to groups or individuals.

Password policy

Users require a passcode to enter into the device, which is the basic protection level of mobile devices from information theft. Use this section to configure how the passcode related security restrictions need to be maintained for the users.

Allow simple value: Allows users to use sequential/repeated characters as their passcodes.

Require alphanumeric value: Mandatory that passcode must contain at least one letter character.

Minimum passcode length: Represents the smallest number of characters that the passcode should contain.

Minimum complex characters: Represents the minimum number of alphanumeric values that should be present in the password

Maximum passcode age (in days): The number of days after which a user password expires.

Password Policy	
Allow simple value	<input checked="" type="checkbox"/>
Require alpha numeric value	<input type="checkbox"/>
Minimum Passcode Length	--
Minimum complex character	--
Maximum passcode age in days (1 - 730 days or none)	
Auto lock	Never
Passcode History (1 - 50 passcodes or none)	
Grace period for device lock	None
Failed attempt	--

Auto-Lock: When the device is not used for this specified period of time, it will get locked automatically.

Passcode History: The new password shouldn't match the old passwords used. You can mention the number of old passwords it should remember, while entering a new password.

Grace period for device lock: Determines the number of failed passcode attempts can be made before the device is locked.

Failed attempts: Shows the number of failed passcode attempts can be made before the device is wiped and factory settings restored.

Restrictions

The permissions or restrictions on the device functionality and applications can be configured from this section. You can select the check box near each function to enable or disable it.

Device functionality

Allow installing apps: You can select this option to permit the user to install apps from the iTunes Store on the device.

Allow use of camera: Select this option to allow users to use camera on their device

Allow facetime: Face time can be allowed to users by selecting this option

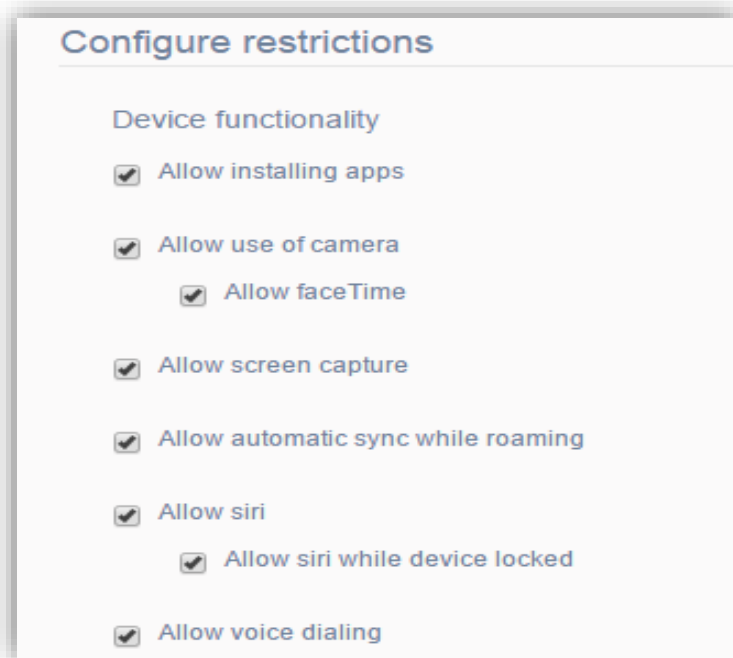
Allow screen capture: Check this check box to allow user to take screenshot in the mobile device

Allow automatic sync while roaming: Select this option to enable the device to automatically sync data while the device is roaming.

Allow Siri: Check this box to allow user to use Siri.

Allow Siri while device locked: Select the check box to allow user to use Siri, while device is locked.

Allow voice dialing: Select the check box to allow user to use voice dialing, which helps in making calls through voice commands.



Allow Passbook while device locked: Passbook is an app for keeping your tickets, passes, and membership cards in a single place. Select the check box to allow user to passbook, while device is locked.

Allow In-App Purchase: App purchase can be restricted using this option.

Force user to enter iTunes store password for all purchase: By selecting this option you can force user to enter iTunes store password for all purchases.

Allow multi-player gaming: Select the check box to allow user access to multi-player games.

Allow adding Game Center friends: Select this option to allow the user to add friends in the Game Center application.

Applications: You can restrict or allow the following applications and its features for devices assigned to the profile using this section.

Allow use of YouTube: Select the check box to permit user to use YouTube.

Allow use of iTunes Store: Select the check box to permit user to use iTunes.

Allow Safari: Select the check box to permit user to use safari browser. The browser features such as Enable auto-fill, Force fraud warning, Enable JavaScript, Block pop-ups, Accept Cookies etc. can also be chosen according to the user's requirement.

iCloud: iCloud stores apps, contacts, calendars, photos, music, books and lets you to access them on your devices. iCloud services can be enabled or disabled in this section.

Allow backup: Choose this option to allow users to backup data and save in iCloud.

Allow document sync: Choose this option to allow users to save documents to iCloud.

Allow Photo Stream (disallowing can cause data loss): Choose this option to allow users to use Photo Stream to share photos with other iOS devices.

Allow Shared Photo Streams: When you select this option, users can share the photo stream with others and can also view the photos shared by other users.

Security and Privacy

Allow diagnostic data to be sent to Apple: Enabling this option will send diagnostic data to the apple server.

Allow user to accept untrusted TLS certificate: Choose this option to use untrusted Transport Layer Security certificates.

Force encrypted backup: Select this option to encrypt the data during backup process

Content ratings

Allow explicit music, podcasts, & iTunes U: Select the check box to permit user to use music, podcast etc.

Allow iBooks Store erotica: Select the check box to permit user to use i Books Store erotica.

Rating region: Allows you to choose ratings by region

Allowed content rating: Allows to access movies TV shows and Apps according to the rating chosen.

Networks

WIFI

The profile specifications for configuring Wi-Fi are given below.

Service Set Identifier: Provide the wireless network identification

Auto join: Choose the option to automatically join the network

Hidden Network: Select this option if target network is not broadcasting its SSID

Security Type: Choose the security protocol to secure the Wi-Fi

Password: Provide the password for authenticate to the network

Proxy: Choose the type of proxy, if it is manual or automatic

The 'Configure Wifi' window contains the following fields:

- Service Set Identifier:** A text box containing 'default'.
- Auto join:** A checked checkbox.
- Hidden Network:** An unchecked checkbox.
- Security Type:** A dropdown menu showing 'Any (Personal)'.
- Password:** An empty text box.
- Proxy:** A dropdown menu showing 'None'.

VPN

The profile specifications for configuring VPN are given below.

Connection Name: Provide the VPN connection name

Connection Type: Choose the type of protocol that need to be used for VPN

Server: Provide the server name or IP address

Account: Provide the user account name for authentication

User Authentication: Mention user authentication type as password / RSA securID

Shared Secret: Provide the shared secret for VPN connection to get established

Send All Traffic: By enabling this option, it routes all network traffic through VPN connection

Proxy: Provide proxy setting for VPN connection, if required

The 'Configure Vpn' window contains the following fields:

- Connection Name:** A text box containing 'VPN Configuration'.
- Connection Type:** A dropdown menu showing 'L2TP'.
- Server:** A text box containing 'scrver'.
- Account:** An empty text box.
- User Authentication:** Two radio buttons: 'Password' (unselected) and 'RSA SecureID' (selected).
- Shared Secret:** An empty text box.
- Send All Traffic:** An unchecked checkbox.
- Proxy:** A dropdown menu showing 'None'.

Email

The profile specifications for configuring email are given below.

Account Description: Provide account name of the mail

Account Type: Choose the type of email protocol used, if it is IMAP or POP

User Display Name: Provide the user display name

Email Address: Provide the email address of the account

Allow Move: Turn on this option to allow user to move messages received on the exchange account using a different mail account.

Incoming Mail Server: Provide the name of incoming email server

Incoming Server Port: Provide the name of incoming email server port for communication.

User Name: Provide the name of the user for the email account

Authentication Type: Choose the authentication protocol that need to be used

Password: Provide the authentication password for the mailbox

Use SSL: Select the option, if the encrypted SSL connection should be enabled for sending mail to the Exchange server.

Out Going Mail Server: Provide the name of outgoing email server

Outgoing Server Port: Provide the name of outgoing email server port for communication.

User Name: Provide the user display name

Authentication Type: Choose the authentication protocol that need to be used

Outgoing Password Same as Incoming: Select the option, if the Outgoing Password is Same as Incoming

Allow Recent Address Syncing: Checking this option will allow recently used addresses to be synced with other devices.

Use Only in Mail: By enabling this option, we can restrict that the mail can only sent from mail application, not from any other browser or apps.

Use SSL: Check this option, if the encrypted SSL connection should be enabled for sending mail to the Exchange server.

Use S/MIME: S/MIME provides cryptographic security services such as authentication,, message integrity, non-repudiation of origin, privacy and data security for emails. Check this option, if this needs to be enabled.

Active Sync

The profile specifications for Active Sync are given below.

Account Name: Provide account name of the mail

Exchange ActiveSync Host:
Provide host name of the ActiveSync

Allow Move: Turn on this option to allow user to move messages received on the exchange account using a different mail account.

Allow Recent Address Syncing:
Checking this option will allow recently used addresses to be synced with other devices.

Use Only in Mail: Use this option to allow mails to be sent only from the native mail application, and not from any other apps or browser.

Use SSL: Select this option, if the encrypted SSL connection should be enabled for sending mail to the Exchange server.

Use S/MIME: S/MIME provides cryptographic security services such as authentication,,

message integrity, non-repudiation of origin, privacy and data security for emails. Select this option, if this needs to be enabled.

Domain: Provide domain name for the account

User: Provide username of the account

Email Address: Provide the email address for the account

Password: Provide password of the account

Configure Active sync

Account Name: Exchange ActiveSync

Exchange ActiveSync Host: Microsoft Exchange S

Allow Move: ☐

Allow Recent Address Syncing: ☐

Use Only in Mail: ☐

Use SSL: ☐

Use S/MIME: ☐

Domain:

User:

Email Address:

Password:

Past Days of Mail to Sync: Three days ▼

Identity Certificate: ▼

Make Identity Certificate Compatible with iOS 4: ☐

Past Days of Mail to Sync: Specify the number of past days' mail that need to be synced on the devices

Identity Certificate: Identity certificate holds the encrypted information of owners details. You can upload this certificate under iOS policy settings > Credentials > Add the certificate. The certificate name will be displayed in this section.

Make Identity Certificate Compatible with iOS 4: Select this option, if you need to make the Identity Certificate Compatible with iOS 4

LDAP

The profile specifications for configuring LDAP are given below.

Account Description: Provide account name of the LDAP

Account User Name: Provide user name of LDAP account

Account Password: Provide password of LDAP account

Account host name: Provide server name or IP address of LDAP account

Use SSL: Select this option, if the encrypted SSL connection should be enabled for LDAP connection.

Configure Ldap

Account Description

Account User Name

Account Password

Account host name Required

Use SSL ☒

CalDav

The profile specifications for CalDav are given below.

Account Description: Provide the name to be displayed on the account

Account host name: Provide the CalDav host name or IP address

Port: Mention the communication Port

Principal URL: Provide the principal URL for the CalDav account

Configure CalDav

Account Description

Account host name Required

Port

Principal URL

Account User Name

Account Password

Use SSL ☒

Account User Name: Mention the CalDav Username

Account Password: Mention the CalDav Password

Use SSL: Select this option, if the encrypted SSL connection should be enabled

CardDav

Hexnode MDM lets you configure CardDav settings to enable users sync their CardDAV contacts list on their mobile devices.

You need to configure the following settings

Account Description: Name you want to be displayed for the account

Account host name: Host name or IP address

Port: Communication port no.

Principal URL: Location containing information about the user address books

Account User Name: Account Username

Account Password: Account Password

Use SSL: Enable/Disable SSL

The screenshot shows a web form titled "Configure CardDAV". It contains several input fields: "Account Description", "Account host name" (with a red "Required" label below it), "Port" (with the value "8443" entered), "Principal URL" (with an asterisk icon), "Account User Name" (with an asterisk icon), and "Account Password" (with an asterisk icon). At the bottom, there is a checkbox labeled "Use SSL" which is checked.

Subscribed Calendars

The profile specifications for Subscribed Calendar are given below.

Account Name: Provide the name to be displayed on the account

URL: Provide the principal URL for the calendar

Username: Mention the calendar Username

Password: Mention the calendar password

use SSL: Select this option, if the encrypted SSL connection should be enabled

The screenshot shows a web form titled "Configure Subscribed Calendar". It contains several input fields: "Account Name", "URL" (with a red "Required" label below it), "User Name", and "Password". At the bottom, there is a checkbox labeled "use SSL" which is unchecked.

Web Clip

The profile specifications for configuring Web Clip are given below.

Label: Provide the label name for web clip

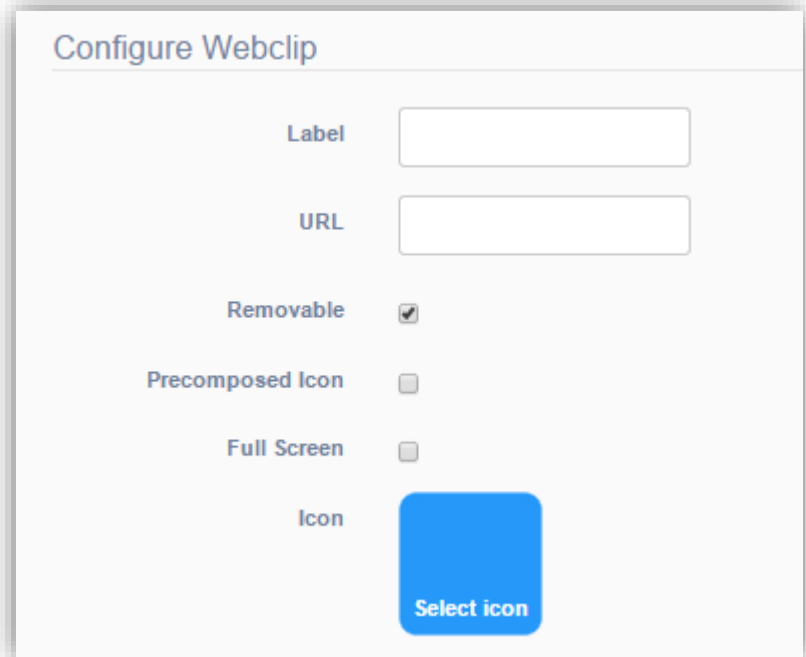
URL: Provide the web URL for the web clip

Removable: Select this option, if the web clip should be removable by the user

Precomposed Icon: Select this option to remove the other effects on the icon

Full Screen: Select this option to open the web URL in full screen

Icon: You can browse and apply the image file which need to be used as icon. The icon can be in GIF/ JPEG / PNG image formats.



The screenshot shows a web form titled "Configure Webclip". It contains the following fields and options:

- Label:** A text input field.
- URL:** A text input field.
- Removable:** A checkbox that is checked.
- Precomposed Icon:** An unchecked checkbox.
- Full Screen:** An unchecked checkbox.
- Icon:** A blue square button with the text "Select icon".

Configure Access Point

The profile specifications for configuring Access point are given below.

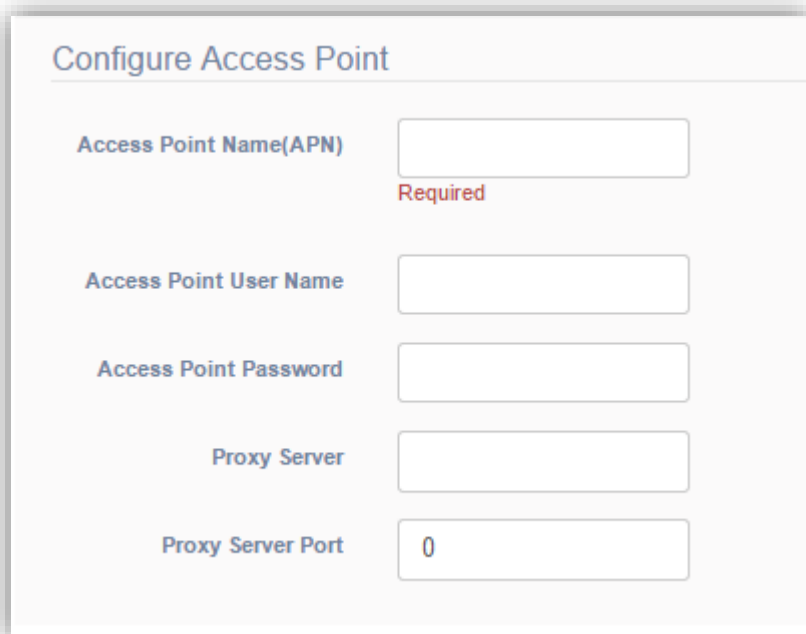
Access Point Name(APN): Provide access point name

Access Point User Name: Provide access point 's user name for authentication

Access Point Password: Provide access point 's password for authentication

Proxy Server: Provide IP address of the proxy server

Proxy Server Port: Provide the proxy server communication port number



The screenshot shows a web form titled "Configure Access Point". It contains the following fields and options:

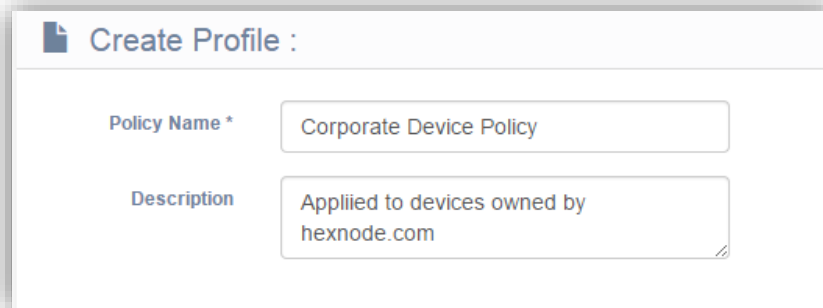
- Access Point Name(APN):** A text input field with a red "Required" label below it.
- Access Point User Name:** A text input field.
- Access Point Password:** A text input field.
- Proxy Server:** A text input field.
- Proxy Server Port:** A text input field with the value "0".

Configure credentials

You can specify the user authentication details and add the necessary certificates.

Steps to configure policy

1.Go to Policy tab, Click on new policy



Create Profile :

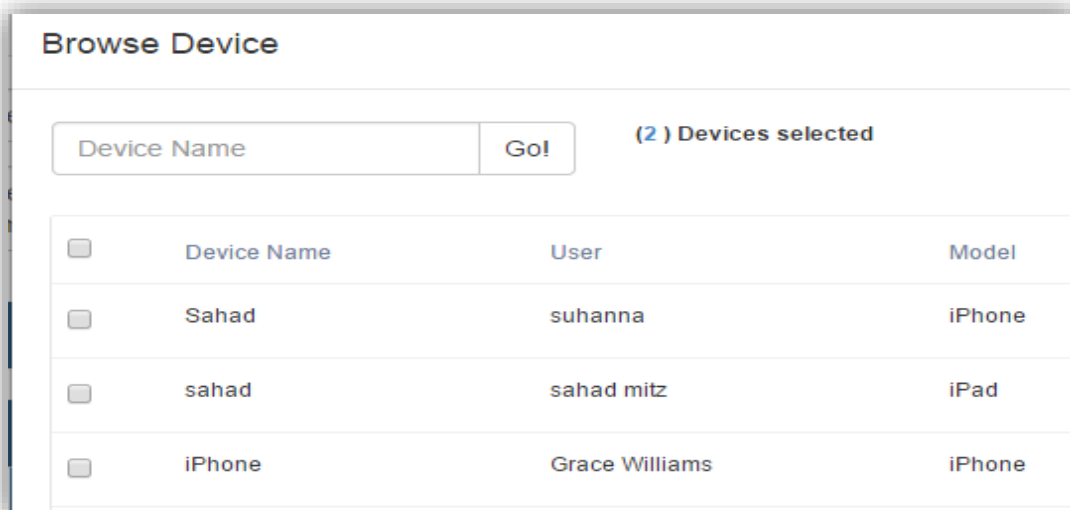
Policy Name * Corporate Device Policy

Description Applied to devices owned by hexnode.com

2. Add the policy name and description of the policy

3.Go to iOS policy setting and choose the required settings

4.The add the policy target, under which you need to associate the user/devices/groups



Browse Device

Device Name Go! (2) Devices selected

<input type="checkbox"/>	Device Name	User	Model
<input type="checkbox"/>	Sahad	suhanna	iPhone
<input type="checkbox"/>	sahad	sahad mitz	iPad
<input type="checkbox"/>	iPhone	Grace Williams	iPhone

5.Save the settings.

Steps to remove policy from the devices/user or from groups

1.Go to policy tab

2.Click on policy from which you need to disassociate from the device/user/group

3.Click on policy target and choose the device and click on remove

4.You can also do the same from management tab, choose the device and disassociate the policy.

Management

Management section lets you to configure and administer the devices, users and groups. Here you can create and manage custom groups based on the organization structure or import groups from corporate directory services. Groups can be modified or users swapped to and fro. Policies can be dynamically applied on user groups or individual users. You can access all the principal management features in here including device scan, lock, wipe and disenroll.

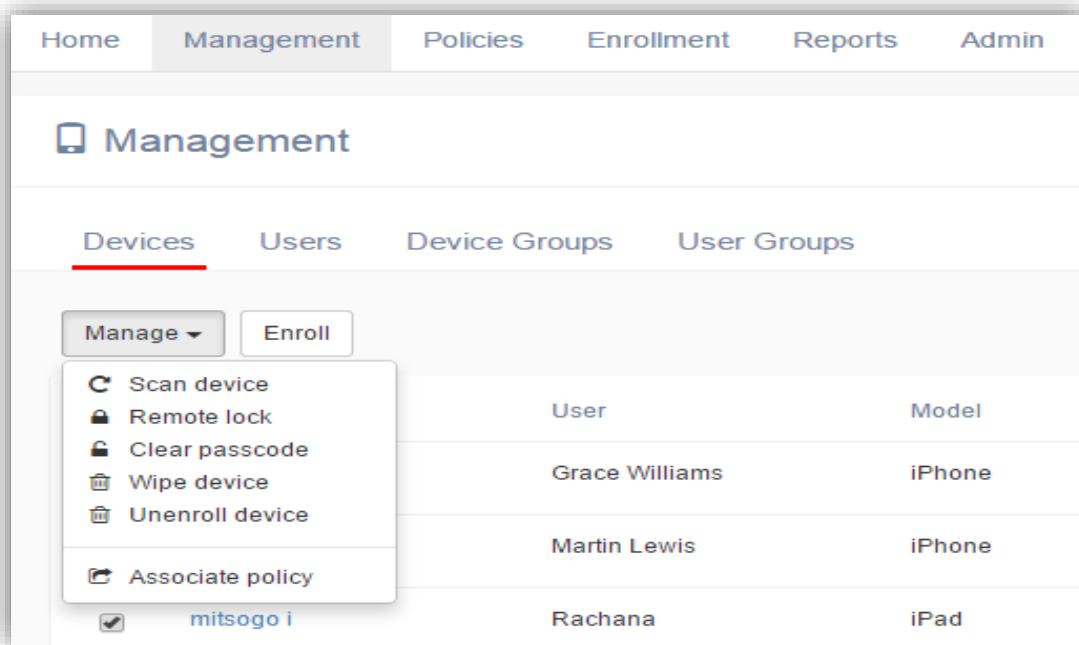
Devices

Hexnode MDM allows you to manage iOS devices using device/user groups for segregation and by imposing policies.

Scanning the device

The scanning of enrolled device(s) can be done by the following steps

1. Click on management tab
2. Click on devices
3. Select the device(s) which you want to enroll
4. Click on manage button
5. Click on scan device



Viewing the details of devices

Once the scan is completed successfully, you can view the details of the device.

To view details of the device


1. Click on management tab

2. Click on devices
3. Click the device on which you need to view the details

The device details have multiple sections






Ribbon that shows status of device scan summary

This shows the number of apps in the device, policies applied, active status, compliance status, passcode status and the last reported date.

Apps	Profile	Active	Passcode	Compliant	Last Reported
58	3				23 ds

Device Summary

Device Summary shows hardware information, compliance information and the enrollment details

Hardware Info		Compliance Info	
Model	iPhone4,1,(MF266HN)	Mdm profile removed	
Device Type	Smart Phone	Passcode compliance	
OS Version	iOS 7.1.1 (11D201)	Application compliance	
Imei	01 353200 983934 8	Profile compliance	
Device Memory	5.98712539672852	Data protection enabled	
Free Memory	2.23302459716797		
Battery Level	0.0500000007450581		
Enrollment details			
Enrolled	Enrolled		
Last reported	29/11/2014 16:11		
Last scanned	29/11/2014 16:11		

Device information

This displays the device and network information of the mobile.

Device Info		Network Info	
Model	iPhone4,1,(MF266HN)	ICCID	8991 1972 3116 6200 994
Device Type	Smart Phone	Bluetooth Mac	2c:be:08:73:eb:64
OS Version	iOS 7.1.1 (11D201)	Ethernet Mac	
Serial No	C8WMWBR6FMLD	Wifi Mac	2c:be:08:73:eb:63
Imei	01 353200 983934 8	Current Carrier Network	Idea
Meid		Sim Carrier Network	Carrier
Device Memory	5.98712539672852	Subscriber Carrier Network	Carrier
Free Memory	2.23302459716797	Carrier Setting Network	16.1
Battery Level	0.0500000007450581	Phone No	+919495160384
		Roaming Enabled	true

Security details

Data regarding security details are displayed in this section. This includes device functionality scope, application's restriction, content settings, cloud details, configuration profile list and provisional profiles list.

Device functionality	Applications
Allow installing apps	Allow use of YouTube
Allow use of camera	Allow use of iTunes Store
Allow faceTime	Force user to enter iTunes store password for all purchase
Allow siri	Allow Safari
Allow siri while device locked	Enable autofill
Allow automatic sync while roaming	Enable javascript
Allow In-App Purchase	Block pop-ups
Allow multiplayer gaming	Force fraud warning
Allow Passbook while device locked	
Allow screen capture	
Allow voice dialing	
	Content
	Allow explicit music, podcasts, & iTunes U

Applications

Displays the list of Apps installed along with its details of bundles size, identifier and version.

Name ▾	Identifier	Bundle Size	Version
	com.amazon.Amazon	22962176	12280.4
Bluefire	tv.bluefire.bluefirereader	36986880	2.3
Calculator	in.uniconesystems.thescientificcalculator	1519616	1.0
CamCard	com.intsig.camcard.lite.eng	55758848	5.5.0.5527
CamScanner Lite	com.intsig.CamScannerLite	40427520	3.5.1.9482
ChennaiBus	com.econnect.eConChennaiBus	954368	1.2
Chrome	com.google.chrome.ios	77258752	38.0.2125.59
Design Tools	com.veamstudios.designtools	8556544	15
Drive	com.google.Drive	36626432	3.2.2
Dropbox	com.getdropbox.Dropbox	76472320	3.5.004

Associated policies

This section shows the policies associated to this particular device

Device Summary

Device info

Security

Applications

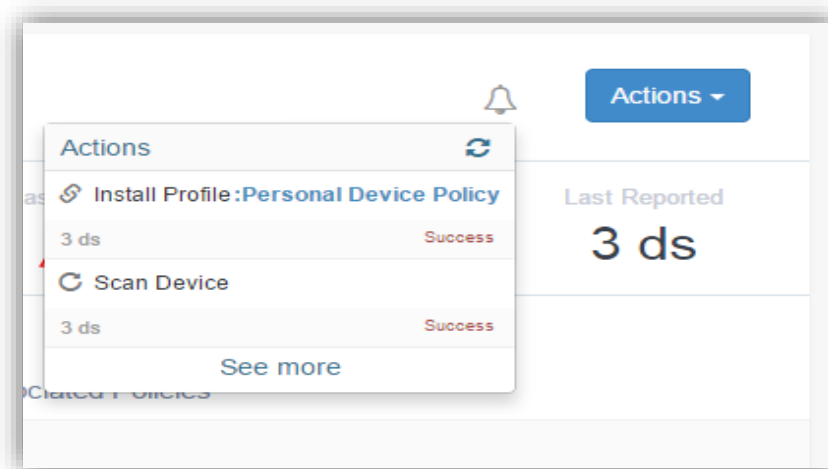
Associated Policies

Search here

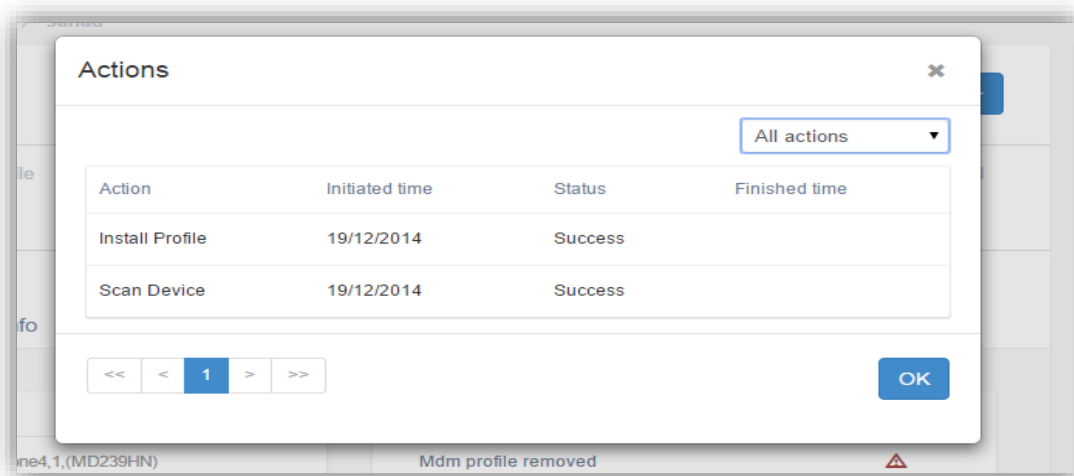
Name	version	Status	Mapping
Corporate Device Policy	1	Installed	Usergroup
Default Org Policy	1	Installed	Usergroup Org-level
Personal Device Policy	3	Pending	Devicegroup Direct Usergroup

Action feed

This provide information of latest actions done on the device and its details.



When you click on “see more”, you can find the detailed information of all actions performed with a filter for the action status.



Activity feed

This event based timeline shows type of action and days passed after the activity has done for that particular device. This provides a better insight the device status for IT managers.

Activity feed shows the most recent activity in the form of an event based timeline.

This provides the IT managers with better insights on the devices' status

Activity feed

Device apns details updated

3 ds

Device Enrolled

3 ds

Filters

Filters are available in the device list view, which allows us to check the segregated list view of the devices.

Filter Devices

Status

- ☐ Active
- ☐ Inactive

Type

- ☐ Smartphone
- ☐ Tablet
- ☐ Others

Ownership

- ☐ Personal
- ☐ Corporate
- ☐ Others

Remote Device Management

Remote Management functions available are

Clear passcodes

If user doesn't know the passcode, then administrator can clear it using this feature.

Remote Lock

The user can be blocked from accessing the device using this function. It can be done from the management tab > devices > choose the device > manage > remote lock.

Wipe device

The data can be immediately cleared from the device through this feature, in case of theft or security risks, from management tab > devices > choose the device > manage > wipe device.

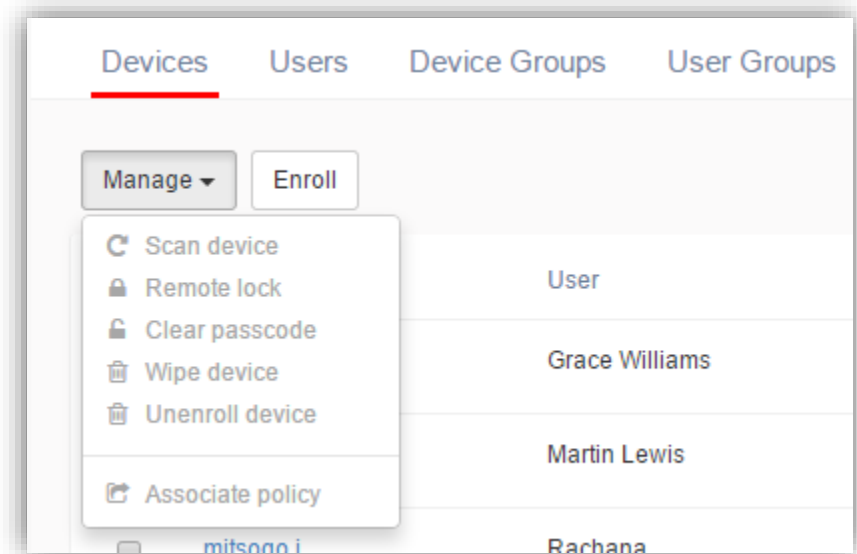
Disenroll Device

Disenrolling a device can be done, from management tab > devices > choose the device > manage > disenroll device.

Associate policy

The devices(s) can be imposed with restriction and settings by applying policies. The policies can be associated to the device from management tab > devices > choose the device > manage > Associate policy.

All these options are available under each device details page, as given below.

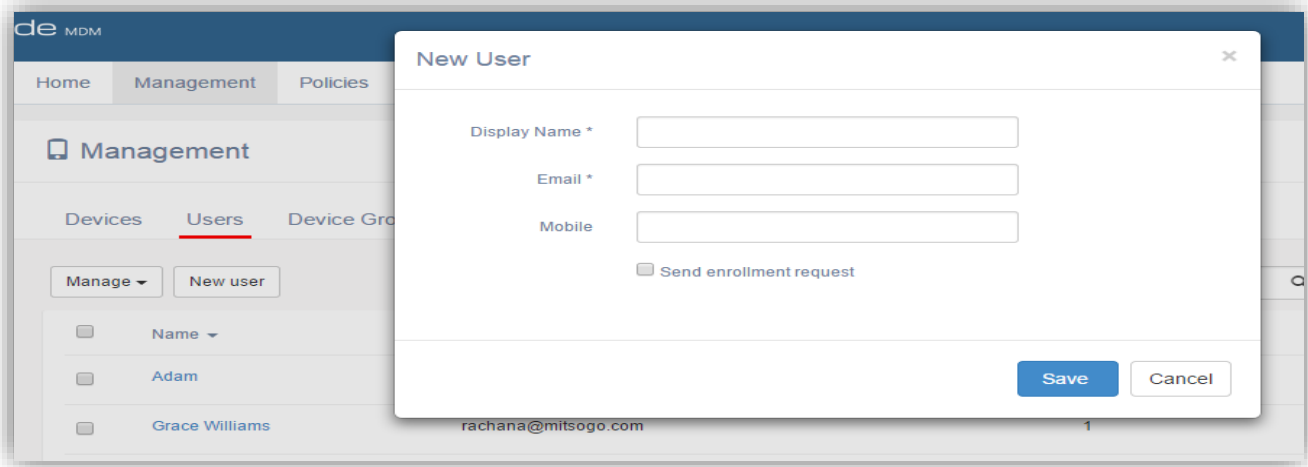


User

The employees in an organization are managed under this section.

Adding a user

The user can be added from Management tab > users > new user. Mention the details of email and phone number. You can also send enrollment request from here itself.



Viewing user details

User details are available under management tab > users section

Devices

Users

Device Groups

User Groups

Manage ▾

New user

Search here

<input type="checkbox"/>	Name ▾	Email	Phone	No of devices
<input type="checkbox"/>	Adam	Adam@mitsogo.com		0
<input type="checkbox"/>	Grace Williams	rachana@mitsogo.com		1
<input type="checkbox"/>	John Darwin	darwin@hexnode.com		0
<input type="checkbox"/>	John Doe	support@hexnode.com	+1203786111	0

Sort

Sorting of users can be done by clicking on the specific column name. The ascending and descending order sorting is possible for now.

Search

Searching option is available the right top of the users list view. Searching with user name or email

address is feasible.

Filter

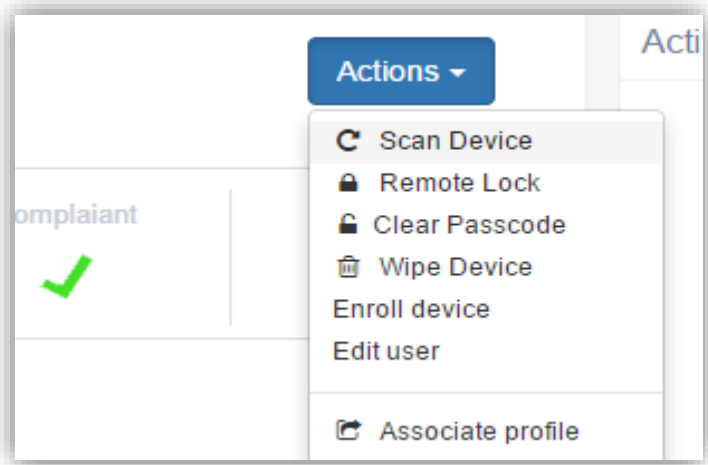
Filter option is present on the right top of the page, through which you can filter users with enrolled devices and users without enrolled devices.

Management

Global and local Management functions are available as same as device section.

Global management functions can be accessed under user list view, under management tab > users > manage button.

User level management functions available under actions of each user details.



Clear passcodes

If the user doesn't know the passcode and the administrator can clear it using this feature,

Remote Lock

The user can be blocked from accessing the device using this function. This is mainly used during the theft of the device. It can be done from the management tab > devices > choose the device > manage > remote lock.

Wipe device

Using this feature, administrator can immediately delete all of the device data in case of a theft or security risk. This feature can be accessed from management tab > devices > choose the device > manage > wipe device.

Disenroll Device

Disenrolling a device can be done, from management tab > devices > choose the device > manage > disenroll device.

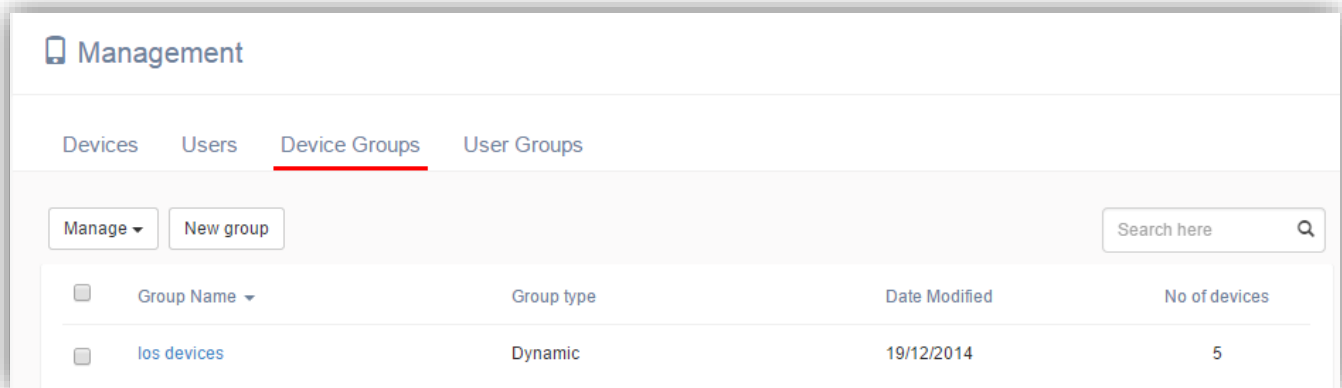
Associate policy

The devices(s) can be imposed with restriction and settings by applying policies. The policies can be associated to the device from management tab > devices > choose the device > manage > associate policy.

Device Groups

The purpose of grouping devices is to manage them by applying configurations and policies in bulk. The device group is a collection of devices which share some logical behavior.

Generally, devices/users are grouped based on the department, type of device or any other parameters of the device. A device can be associated to multiple groups. When you apply multiple policies to a device, then the most restrictive settings of all the policies will get applied.



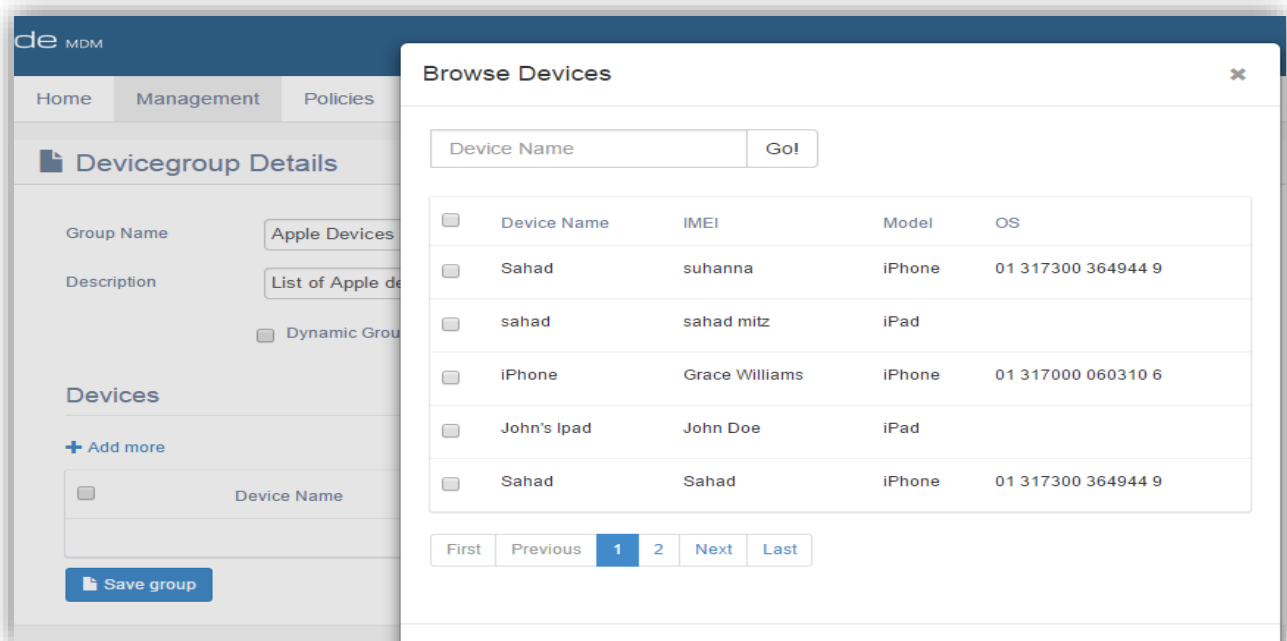
Type of groups

There are two types of grouping available to manage the mobile devices.

Static grouping

Follow the steps below to create a static group

1. Go to management tab
2. Click on device groups



3. Click on add new group
4. Mention the name and description
5. Now you need to browse and select the devices under the group, clicking on add devices
6. Once devices are added, save the group details

As the name suggests, in static groups we need to add the devices manually.

Dynamic grouping

Dynamic grouping allows you to define criteria according to the device functionality or ownership. The devices matching to that criteria will be added to the application dynamically.

Follow the steps below to create a dynamic group

1. Go to management tab
2. Click on device groups
3. Click on add new group
4. Mention the name and description
5. Choose the criteria from the drop down list
6. Save the group details

Devicegroup Details

Group Name:

Description:

☒ Dynamic Group

Conditions

☒ All Of the below conditions ☐ Any of the below conditions

[+ Add filter](#) [Show Devices](#)

7. Click on show devices will list all the devices which match that criteria
8. choose the devices and add them to the group
9. save the group settings

oode MDM

Home

Management

Policies

Search

Devicegroup Details

Group Name

Finance Group

Description

☒ Dynamic Group

Conditions

☒ All Of the below conditions

☐ Any one of the below conditions

device make info

+ Add filter

Devices

Device Name	IMEI	Model	OS
Martin Lewis	71e94b7db71e720425364a35f17e167342536bab	1	2
Sahad	be01f632d314286a77f15311fbb31be058d1d902	1	1
suhanna	be01f632d314286a77f15311fbb31be058d1d902	1	1
sahad mitz	7778510cc222a9848ecc44aade279e32a2eead33	1	1
Rachana	7778510cc222a9848ecc44aade279e32a2eead33	1	1
Rachana	7778510cc222a9848ecc44aade279e32a2eead33	1	1
John Doe	7778510cc222a9848ecc44aade279e32a2eead33	1	1

First

Previous

1

Next

Last

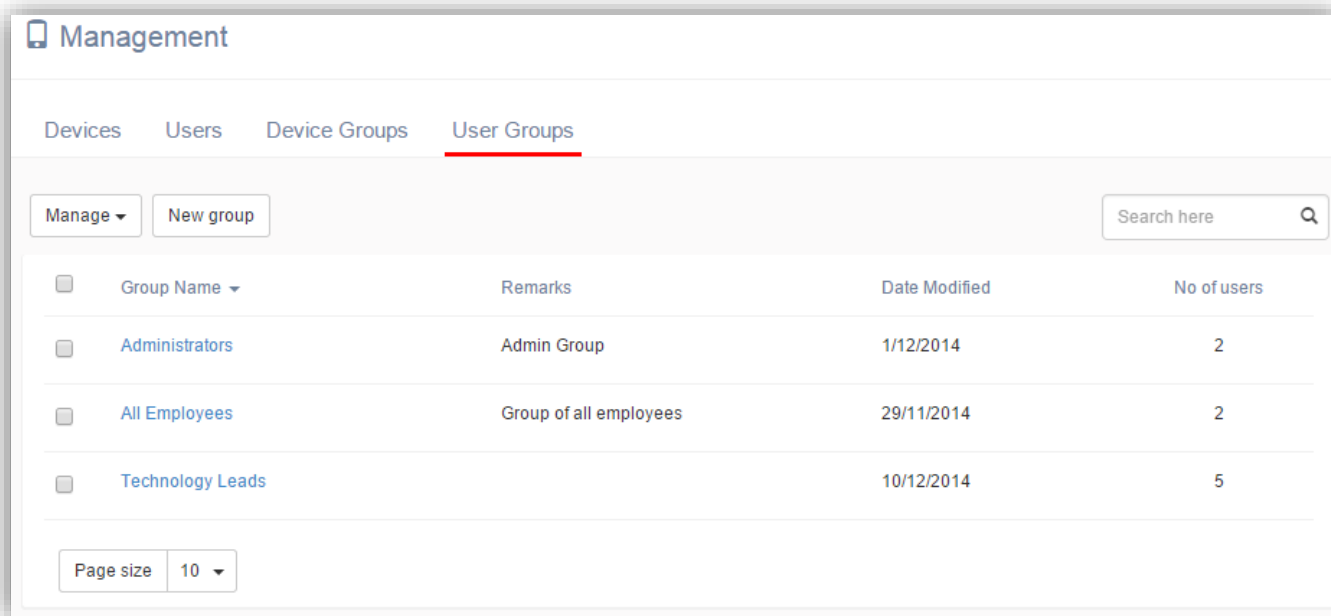
OK

Show Devices

Note: You can add multiple criteria to the group. You can also choose if it should match all the criteria or any one of the criteria

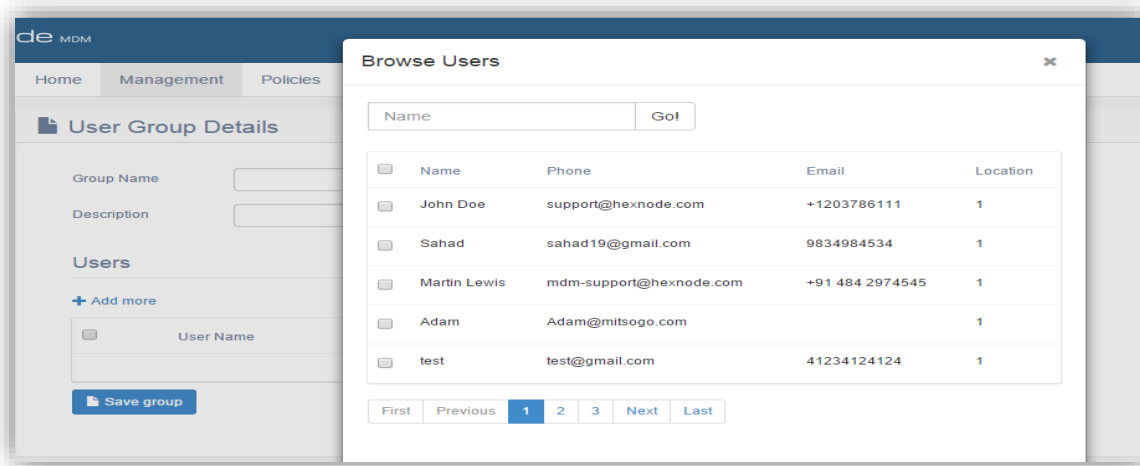
User group

User group is a collection of users who share the same job title, location, department etc.



Follow the steps below to create a user group

1. Go to management tab
2. Click on device groups



3. Click on add new group
4. Mention the name and description

5. Select the user from the users list
6. Save the group details

Group Management Functions

Global and local Manage functions are available as same as device/user section, however here the groups are associated to the function. So any operation done to the group will affect all the members in the group.

Clear passcodes

If the user doesn't know the passcode, the administrator can clear it using this feature.

Remote Lock

A group can be blocked from accessing the devices using this function. It can be done from the management tab > device/user group > choose the device/user group > manage > remote lock.

Wipe device

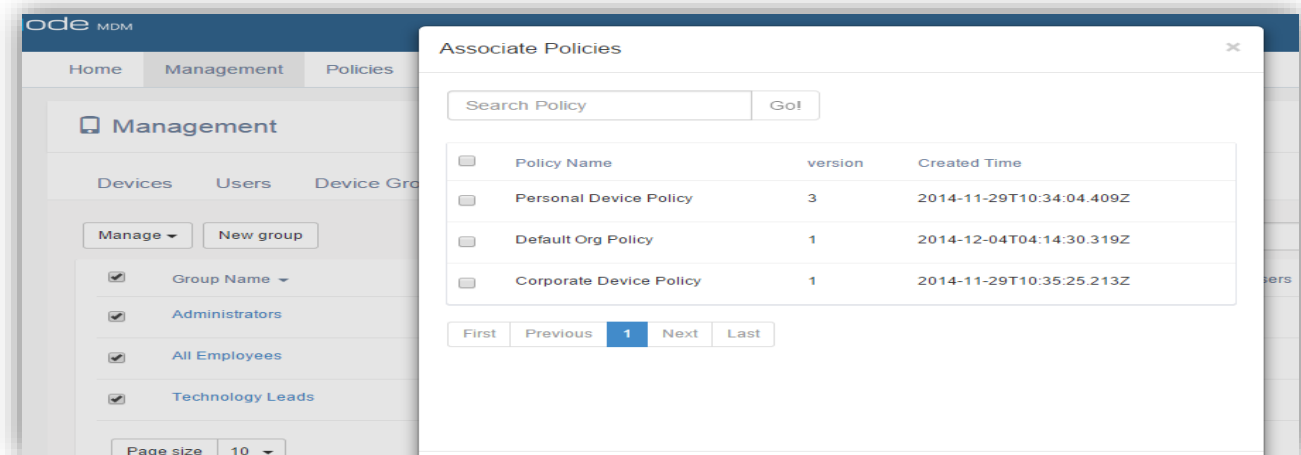
Using this feature, administrator can immediately delete all of the device data in case of a theft or security risk. It can be accessed from management tab > device/user group > choose the device/user group > manage > wipe device.

Disenroll Device

Disenrolling the device can be done, from management tab > device/user group > choose the device/user group > manage > disenroll device.

Associate policy

The devices(s) can be imposed with restriction and settings by applying policies. The policies can be associated to the group, from management tab > device/user group > choose the device/user group > manage > associate policy.



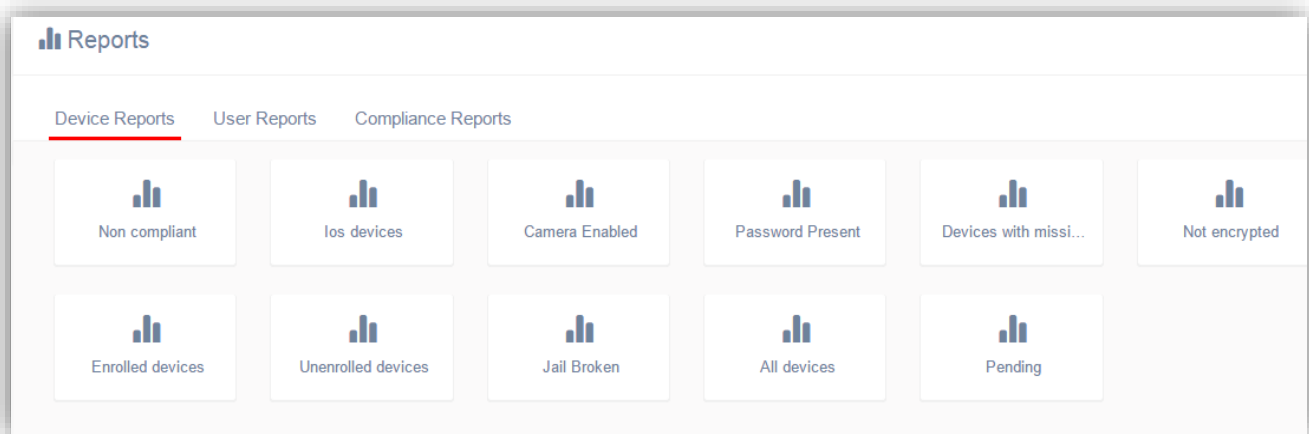
MDM Reporting Module

Hexnode allows to you generate all required reports you need for Enterprise Mobility management in any business. The detailed reports along with graphs and filter options helps you to identify the compliance status of the devices in the entire organization in no time. The policy violations can also be detected and can be informed on time using the reports module.

Types of reports

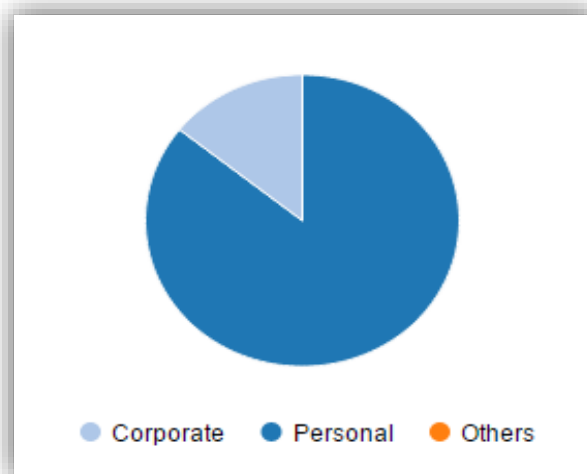
There are three major segment of reports available.

1. Device reports
2. User reports
3. Compliance reports



Graph section:

For each report, the pie chart is available on the right-top-panel which will help in analyzing the data.



Sorting of columns

The data in any column of the report can be sorted in alphanumeric ascending or descending order by clicking on the column title.

<input type="checkbox"/> Name	User name ▾	Model	Status	Type
<input type="checkbox"/> iPhone	Grace Williams	iPhone	Active	Smartphone
<input type="checkbox"/> John's Ipad	John Doe	iPad	Inactive	Tablet
<input type="checkbox"/> Martin	Martin Lewis	iPhone	Inactive	Smartphone
<input type="checkbox"/> John's Ipad	Rachana	iPad	Inactive	Tablet

Filters

The filters for device status, device type and ownership are also available at the right-bottom-panel, which will help in segregation of data.

Filters

Status

☐ Active

☐ Inactive

Type

☐ Smartphone

☐ Tablet

☐ Others

Ownership

☐ Personal

☐ Corporate

MDM Device reports

Non-Compliant

The devices that don't meet the compliance requirements

iOS devices

List of apple devices

Camera Enabled

The devices that have camera enabled

Password present

The devices that have passcode lock enabled

Missing mandatory apps

The devices that have missing mandatory applications

Non-encrypted

The devices that don't have data encryption enabled

Enrolled devices

The devices that are enrolled successfully

Unenrolled devices

The devices that are not enrolled

Jailbroken devices

The report on the devices that are jailbroken

All devices

Report on all managed devices

Enrollment Pending

Devices which were sent enrollment requests, but are yet to join

Non Compliant				
All non-compliant devices				
<div>Search here</div>				
<input type="checkbox"/> Name ▾	User name	Model	Status	Type
<input type="checkbox"/> John's Ipad	Rachana	iPad	Inactive	Tablet
<input type="checkbox"/> John's Ipad	John Doe	iPad	Inactive	Tablet
<input type="checkbox"/> Martin	Martin Lewis	iPhone	Inactive	Smartphone
<input type="checkbox"/> mitsogo i	Rachana	iPad	Active	Tablet

MDM User reports

All users

Report on all users

Unenrolled user

Report on all users who have been unenrolled

Non-Compliant user

User with the devices that do not meet the compliance policy

Users without passcode

Users who have not set passcode for their devices

Users with inactive device

The users who have devices that are inactive

Camera enabled users

The users who have devices with camera enabled

Enrolled users

Report on all users who hold enrolled devices

Users with unencrypted devices

Report on users who hold unencrypted devices

Compliance reports

Compliant Devices

The devices that meet the compliance requirements

Profile Compliant

The devices that have met the policy associated

Passcode Compliant

The devices that have passcode lock enabled

Non-Compliant

The devices that don't meet the compliance requirements

Profile Non-compliant

The devices that have not met the policy associated

No Passcode

The devices that has have no passcode lock enabled

Inactive

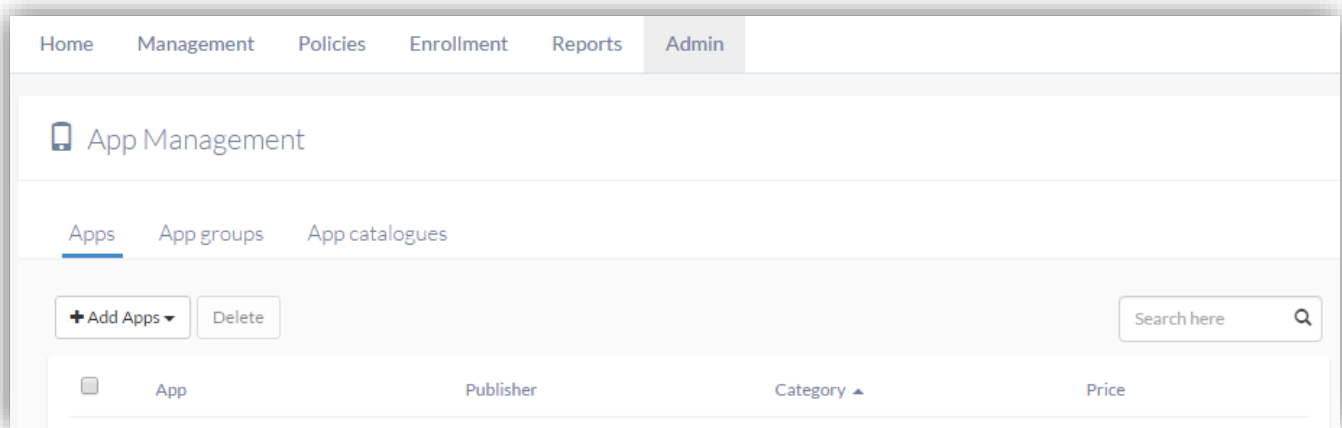
The devices that are not scanned for a particular number of days as per the setting, under admin tab > MDM settings

Mobile Application Management (MAM)

You can access all the core Mobile Application Management features in here. You can create a dedicated Enterprise App catalog for easily deploying and managing enterprise apps, Blacklist or Whitelist to regulate the apps coming into the enterprise, Monitor and provision mandatory apps for compliance and a perform a host of other app management functions.

Getting started with Mobile Application management

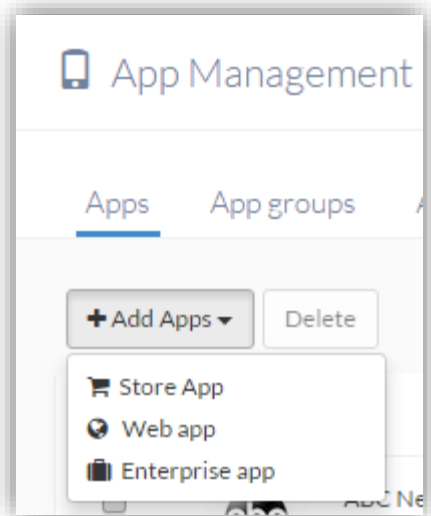
Head over to the admin tab and select App settings. Here we have three sub-tabs Apps, App groups and App catalogues.



Apps (App inventory)

Here, you have the entire apps in your inventory. You can sort them by the App name, Publisher, Category or Price. You can also search for a specific app. Now, click on the Add apps button.

There are three options Store app, Web app and Enterprise app. Click Store app. A search window will pop up. Type a name and hit the search button. You'll see a list of relevant apps with an add button for each of them. Start by adding a few apps to your list. Choose 5-6 apps for now. After adding, press done and close the search window.

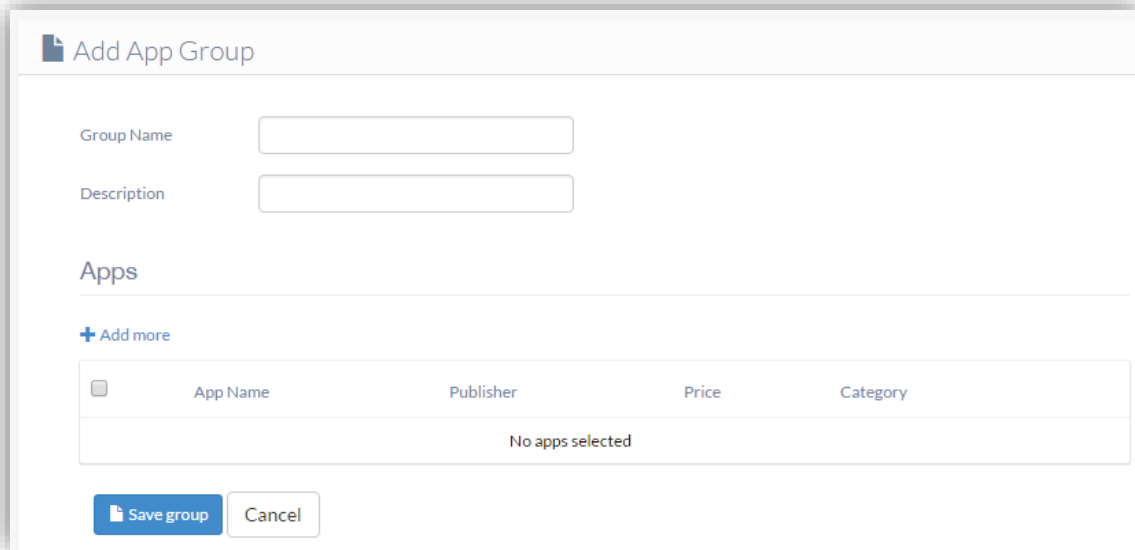


The newly added apps will appear in your apps list. If you have an Enterprise app you can add it too. We'll show you how later. You can filter apps based on category, app type or license.

App groups

Here you can create groups to better organize your apps. It will come in handy once you start dealing with a large volume of apps.

Groups can be sorted by their Name, Date modified and the number of apps in them. Groups are searchable too. Now click on Add group.



Add App Group

Group Name

Description

Apps

[+ Add more](#)

<input type="checkbox"/>	App Name	Publisher	Price	Category
No apps selected				

Choose few apps from your list. You can select 'Add more' if you want to add other apps not in your list. Now give a sample name for your group and a description. Now save group. You have successfully created a new App group.

Enterprise App catalogs

App catalog provides the users with a sort of custom app store to easily install the apps required. You can set up multiple catalogs to effectively provision apps for different sets of targeted users. You can add app groups and individual apps to a catalog.

Let's now create a new catalog. Click add catalog. Choose a few apps and the one app group you created and hit Save catalog

Your new App catalog should appear in the list.

Add App Catalogue

Name

Description

Apps Groups

[+ Add more](#)

App	Publisher	Price	Category
No items selected			

[Save catalogue](#) [Cancel](#)

Deploying apps via Enterprise app catalog

Now that you have created an app catalog, let's see how you can assign them to individual users to ease app installation. Start by creating a new policy.

Select Home > Policies

Select New Policy.

Create Policy

Policy Name *

Description

iOS Settings App Management Policy Targets

Black/White list

Mandatory Apps

Catalogue

[+ Add Catalogues](#)

Name	description
No Catalogues Selected	

[Save](#) [Cancel](#)

Now click on App Management. Select Catalog > Add catalog. Choose the catalog you have created. Now click on Policy targets. Select users and choose a user. You can also associate this policy to a device, group or even a domain.

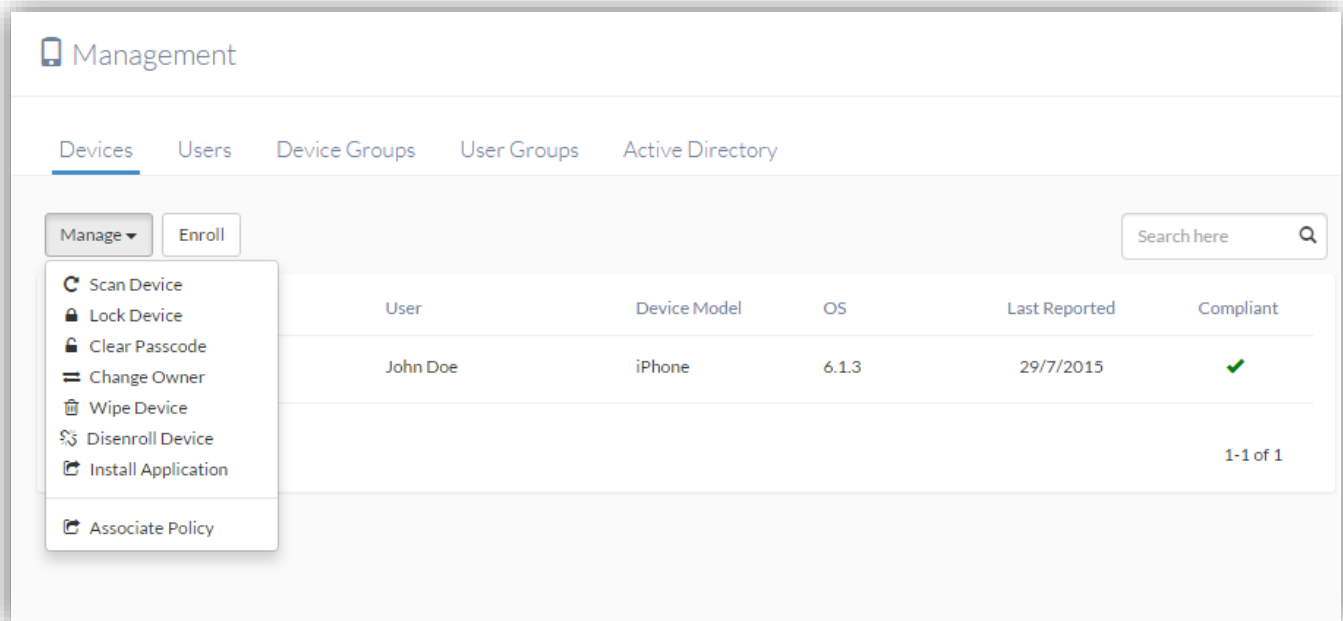
Once you are done. Save the policy. You have now associated this particular app catalog to a specific user. A link to access this app catalog in the form of a web clip is instantly saved on the user device.

App installation

Hexnode MDM lets you install any app you want on the user devices.

Choose Home > Management > Devices

Select the device. Click on Manage and select Install Application.



Under local apps, you can see the apps in your inventory. If you want to install an application not on the list, click on Public Store and search for the particular app. Once you have selected the app, click done and the selected app will be installed on the user device.

App Blacklisting/Whitelisting

Blacklisting works in combination with policy. You need to be able to blacklist different sets of apps for different users. One global blacklist for the enterprise doesn't work. So, what you do is you create a policy and within that policy you define a blacklist by adding the potentially risk applications. Now you can assign this policy to any device, user or groups.

For blacklisting,

Select Home > Policies

Select New Policy. Click on App Management. Select Black/White list.

Select Add > Add app.

Under local apps, you can see the apps in your inventory. If you want to blacklist an application not on the list, click on Public Store and search for the particular app.

Once you have selected the required apps. Click Save. Now Click on Policy Targets and select the desired device. The desired apps will be blacklisted for the device.

Push Enterprise Apps

For pushing Enterprise apps, first, you need to upload the application archive file (.ipa) to Hexnode MDM. The enterprise app will appear in your app inventory. You can then install it on any device.

Select Admin > App settings > Apps

Click on Add apps and choose Enterprise app.

You can upload the ipa file for your app or specify the manifest URL. Select the category for your app and provide a description. Check Remove with MDM if you want the app to be uninstalled on removing the MDM profile. Check prevent backup to disable the enterprise app data from getting synced with the users personal iTunes account. Once you have selected the app click on add. The

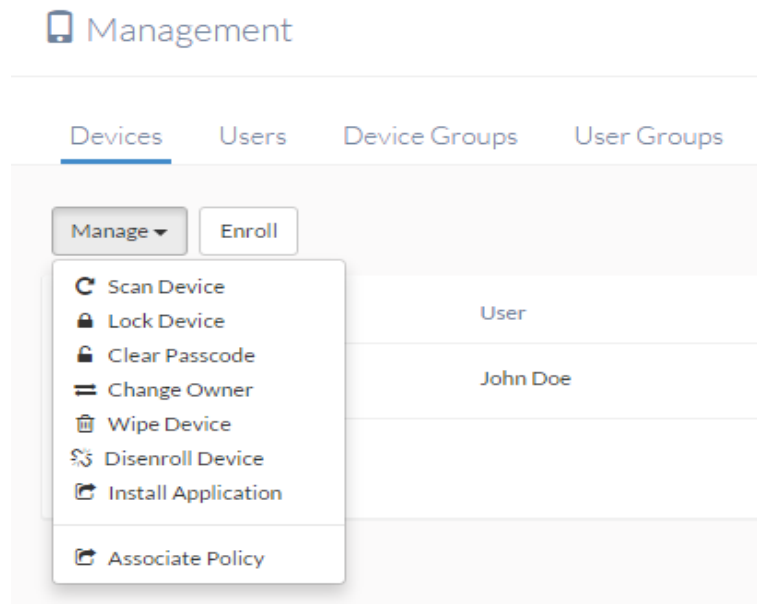
enterprise app will be added to your app inventory.

Now, for installing this app on a user device.

Choose Home > Management > Devices

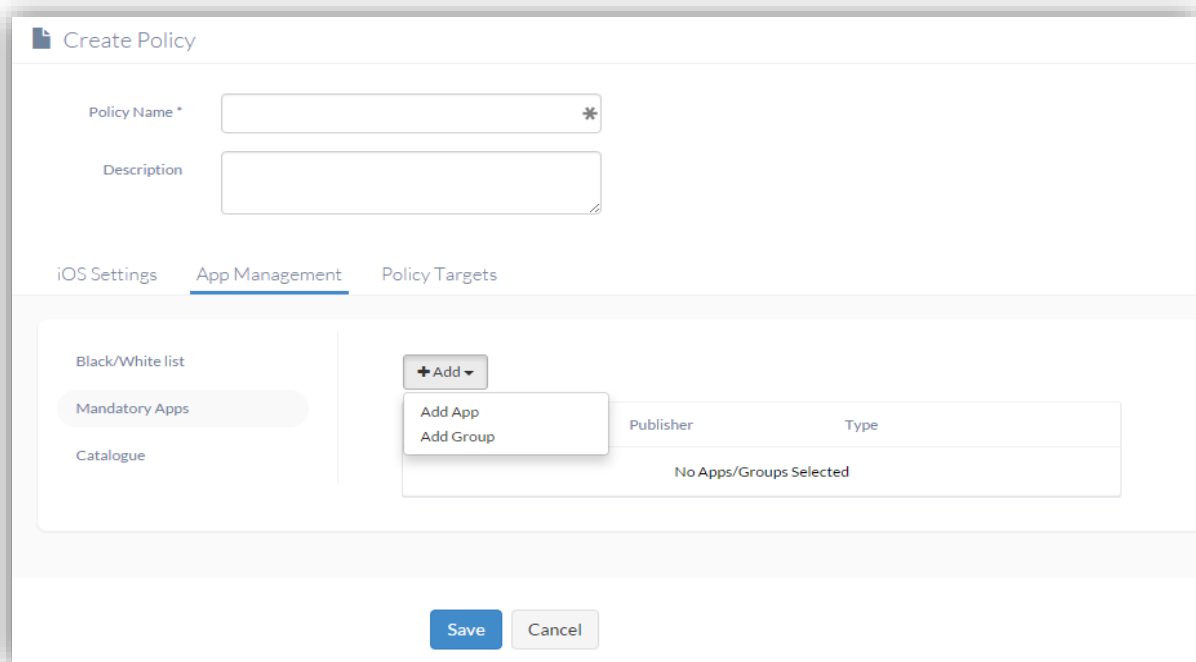
Select the device. Click on Manage and select Install Application.

Under local apps, you can see the enterprise app you have uploaded. Once you select the app, click done and the app will be installed on the user device.



Mandatory Apps

Defining mandatory apps helps you make sure the users have installed all the essential apps. Mandatory apps too work in combination with policy. You create a policy with the list of mandatory apps and assign it to any entity – user, device, group or domain. The selected apps will be pushed to all the devices that fall under the target entity.



Select Home > Policies

Select New Policy. Click on App Management. Select Mandatory apps. Click Add button and select Add app. Under local apps, you can see the apps in your inventory. If you want to choose an application not on the list, click on Public Store and search for the particular app. Once you have selected the apps, click Done.

Now click on Policy targets. Select users and choose a user. You can also associate this policy to a device, group or even a domain. Once you are done. Save the policy.

You have now successfully defined a list of mandatory apps for the user. All the apps in the list will be installed on the user devices.

Active Directory settings

Hexnode MDM lets you import your Active Directory into Hexnode MDM and apply policies straight to the existing users, groups or OUs. No hassle of adding users manually.

Start by setting up your Active Directory.

Select Admin > AD settings

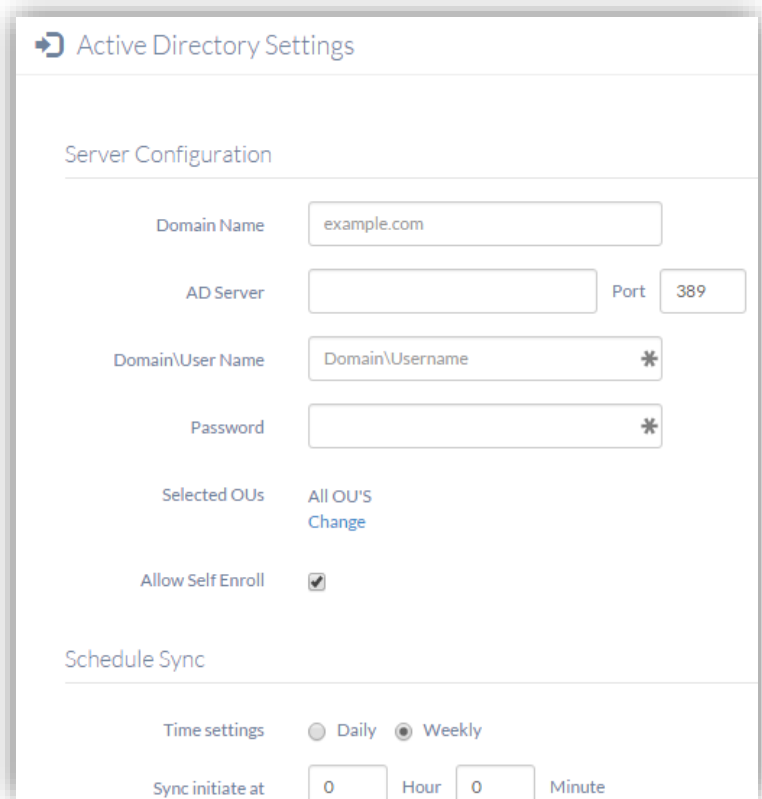
If you have already configured an AD, it will be displayed here. You can click open it to edit the current settings.

Let's now add a new Active Directory.

Click on the empty slot with the + sign.

Specify your Domain Name, AD server address, Port no and your AD username and Password.

Selected OUs: By default, all the OUs in the domain will be selected. You can click on change to select the specific OUs you want.



The screenshot shows the 'Active Directory Settings' interface. It is divided into two main sections: 'Server Configuration' and 'Schedule Sync'.
In the 'Server Configuration' section, there are several input fields: 'Domain Name' (pre-filled with 'example.com'), 'AD Server' (empty), 'Port' (pre-filled with '389'), 'Domain\Username' (pre-filled with 'Domain\Username' and a '*' icon), and 'Password' (empty with a '*' icon). Below these is a 'Selected OUs' section showing 'All OU'S' with a 'Change' link. At the bottom of this section is a checkbox for 'Allow Self Enroll' which is checked.
The 'Schedule Sync' section has 'Time settings' with radio buttons for 'Daily' and 'Weekly' (selected). Below this is a 'Sync initiate at' section with input fields for '0' hours, '0' minutes, and a 'Minute' label.

Allow Self Enroll: If you enable Self Enroll, users in this particular domain will be able to enroll directly

from the portal without any enrollment requests.

Schedule Sync: You can choose here, how often you want the AD to be synced with Hexnode MDM. You can select the days of the week you want synchronization to occur. You can also schedule a daily sync and choose the time of the day.

Once you are done, click Save. Your Active Directory will be synced with Hexnode MDM databases.

Applying policies on an AD group

Once you have synced your Active Directories with Hexnode MDM, you can apply policies on the existing usergroups, organizational units or the entire domain.

Let's start by creating a policy,

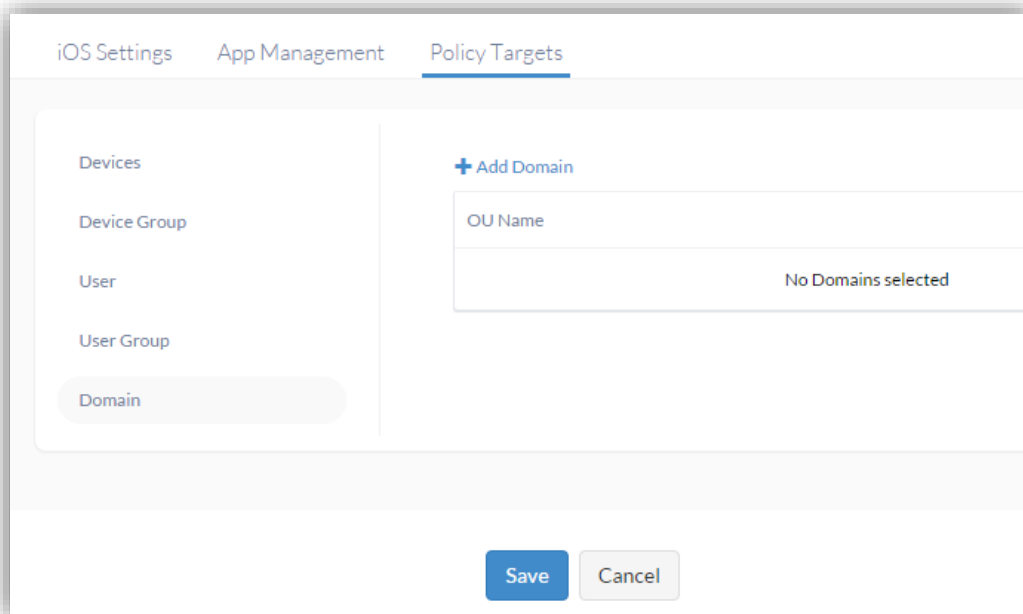
Select Home > Policies

Choose a policy you want to set for an AD group, OU or domain. For the sake of simplicity, let's choose web clip configuration.

Select New Policy > Web clip. Click on configure. As for label and URL, give your company name and website. For icon you might want to select your company logo or image. Click Save.

Now select Policy Targets. Select Domain. Click on Add Domain. You can see your domains listed. For any domain, click on the arrow next to it to expand. Now you can select multiple OUs or the entire domain. After selection click Ok.

Now select Usergroups. Click on Add Usergroup. You can see all your AD usergroups listed in here. Select the desired usergroups and click Ok.



You have now successfully set your AD groups and OUs as policy targets.

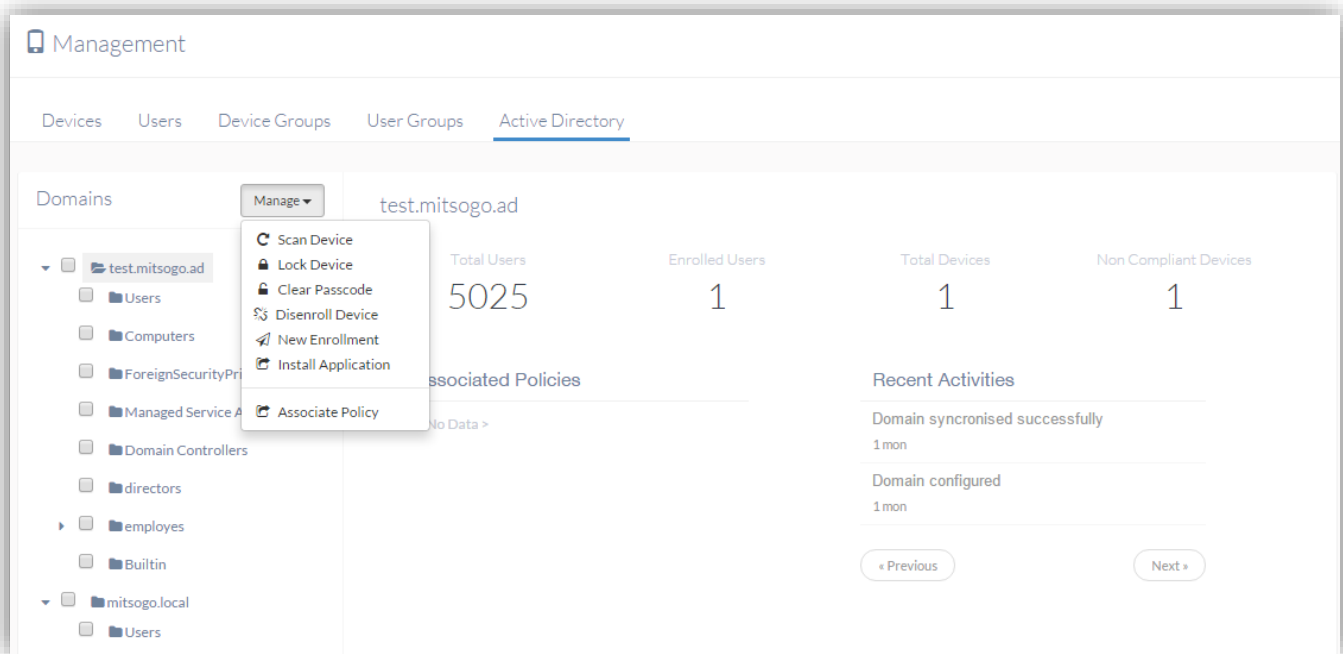
If you click Save now, the web clip policy you have configured will be active on all the targets you have selected. If you want to apply the policy, click Save else click cancel.

Active Directory based Remote Device Management

Hexnode MDM lets you perform bulk actions to lock device, clear passcode or even install applications on the devices linked to your AD groups.

For bulk management,

Select Home > Management > Active Directory



All your AD domains will be listed here. Click on the arrow adjacent to any domain. It will expand to show the OUs within. Now you can select multiple OUs or the domain as a whole.

Select any and click on Manage. Here we have multiple options. Clicking on any of them performs the corresponding actions in bulk on the groups, OUs or domains selected.

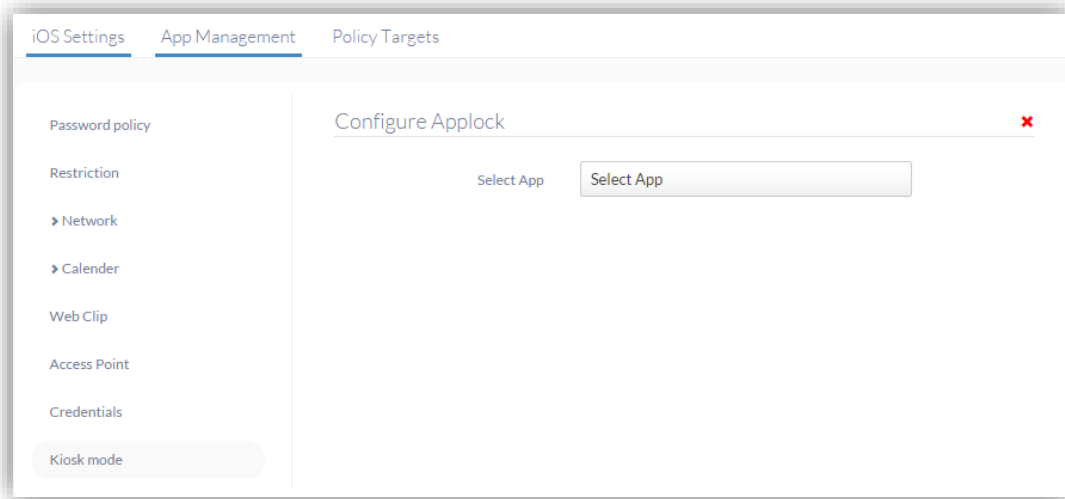
- ✓ Scan device – Hexnode MDM performs a device scan to fetch the current device info and settings.
- ✓ Lock device – Hexnode MDM locks the devices remotely.
- ✓ Clear passcode – Hexnode MDM resets the password on the devices.
- ✓ Disenroll device – Devices will be disenrolled from Hexnode MDM.
- ✓ New enrollment – Enrollment requests will be sent to the devices.

- ✓ Install application – Selected applications will be installed on the user devices.
- ✓ Associate Policy – Selected policy will be applied on the user devices.

App lock

While deploying iPads, at times, you may need the device to work in a kiosk mode i.e. lock the iPad on to a single app. Hexnode MDM lets you do this precisely.

For the app lock to work, Supervisory mode needs to be enabled on the iPad. You can turn on supervision by using the apple configurator tool.



Note that you have to manually connect the device to a Mac computer.

Once supervision is turned on, you can enable app lock from Hexnode MDM

Select Home > Policy > iOS Settings

Now, choose Kiosk Mode. Click on Configure.

Click Select App. In the drop down list, you'll find the apps in your inventory. You can also search for any app. If you want to choose another app not in the list. Click Search Store. Once you have selected the desired app click Save and proceed to Policy targets.

Click on devices and select the desired device. Once you are done, save the policy.

The selected device will switch to Kiosk mode. In kiosk mode, user won't be able to exit the app environment or access anything beyond it.

Location Tracking

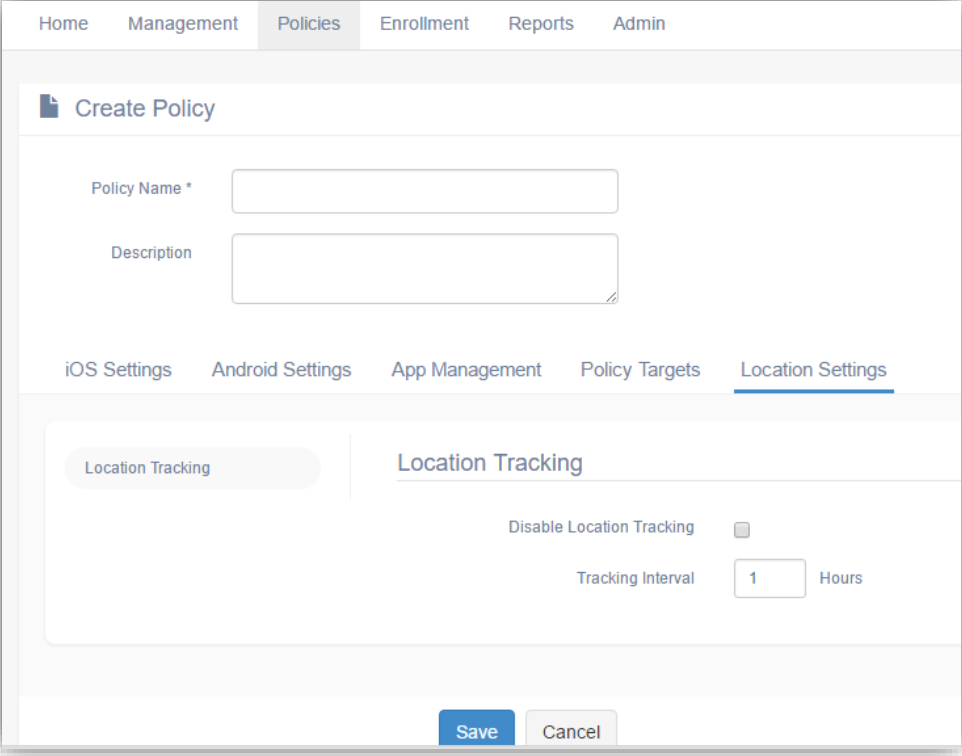
Hexnode MDM gives you an option to track any device and know its recent location. This information is available on the device details page.

Prerequisites: For iOS devices, location tracking is enabled only if Hexnode MDM app is installed on the device.

To enable and configure Location on devices

Location parameters can be configured through policies being applied to the devices. Once applied, these settings cannot be modified by the users.

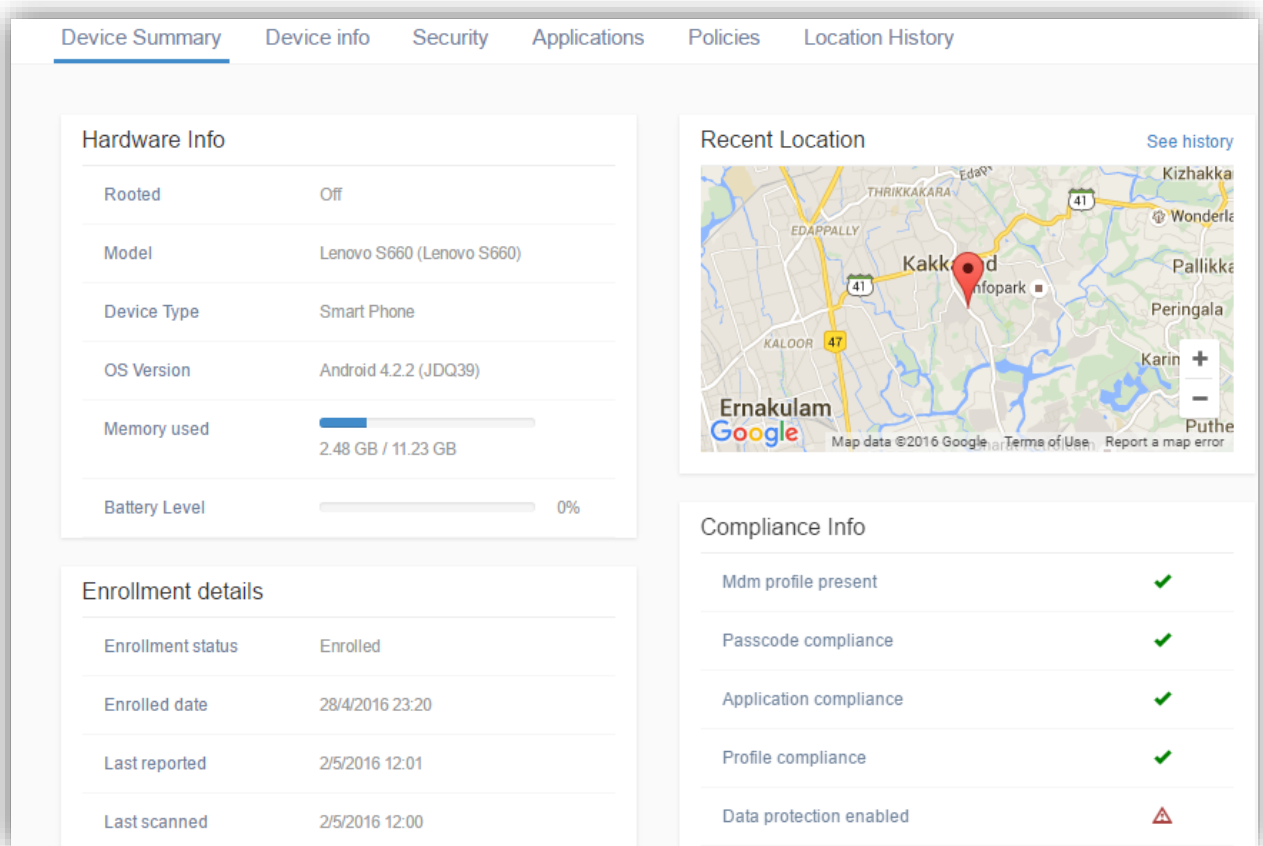
3. Click on policies
4. Go to a new policy or edit an existing policy.
5. Go to Location Settings sub tab.
6. Click 'Configure'.
7. This gives you an option to enable or disable tracking and also allows you to set the tracking interval as shown below.



The screenshot shows a web application interface for creating a policy. At the top, there is a navigation bar with tabs: Home, Management, Policies (selected), Enrollment, Reports, and Admin. Below the navigation bar is a section titled 'Create Policy' with a document icon. It contains two input fields: 'Policy Name *' and 'Description'. Below these fields is a sub-tab bar with options: iOS Settings, Android Settings, App Management, Policy Targets, and Location Settings (selected). Under the 'Location Settings' sub-tab, there is a 'Location Tracking' section. It includes a toggle switch for 'Disable Location Tracking' (currently off) and a 'Tracking Interval' set to '1' with a unit of 'Hours'. At the bottom of the form are 'Save' and 'Cancel' buttons.

To view the current location of the device

5. Click on Management tab
6. Click on devices
7. Click the device for which you want to view the details
8. This page has multiple sub tabs after a ribbon showing summary of the device.
9. Click on 'Device Summary' tab. This shows the Recent Location along with Hardware Info, Enrollment details and compliance Info for the device.



Location History

Based on the location information sent from the devices periodically, we generate a location history which shows the path the device has traversed. This location scanning frequency is a configurable setting and can be set while creating a policy.

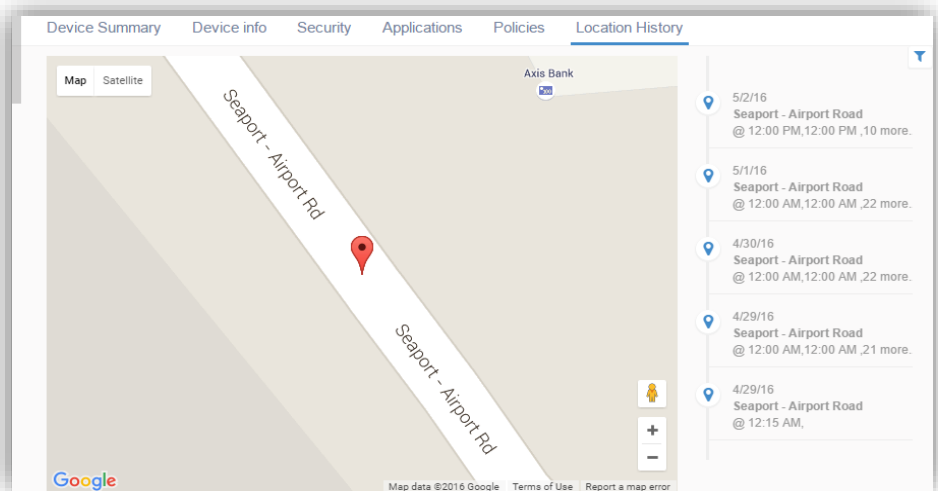
To view the device location history:

- Click on Management tab
- Click on devices
- Click the device for which you want to view the details
- Click on 'Location History'

This page has multiple sub tabs after a ribbon showing summary of the device.

This marks the most recent location of the device on the map.

On the right side of the map, it lists the device's locations over a period of time. When you click on a

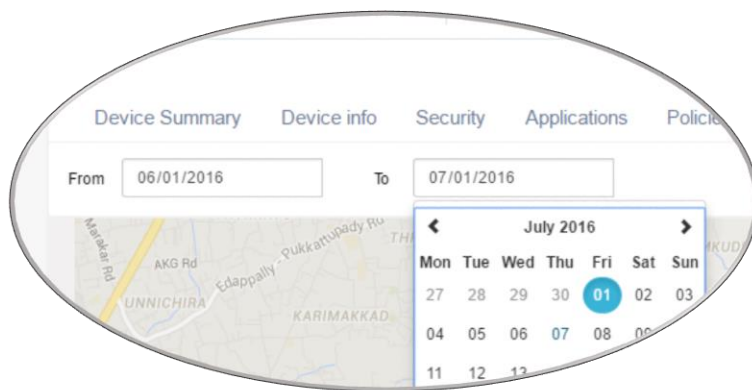


particular location on the right, it is marked on the map.

We also provide you an option to filter location information based on date.

Click on filter button on the top right corner.

It displays from and to date options to choose. Based on the dates you choose, only device locations between those dates are listed.



Contacting Hexnode support

Contact information

Website: https://www.hexnode.com	
Email: support@hexnode.com	
United States 340 S Lemon Ave #5997 Walnut, CA 91789 Phone: +1-510-545-9700	India Seaport Airport Road CSEZ PO, Cochin Kerala – 682037 Phone: +91-484-297-4545

Technical support

Phone: +1-866-498-940 +1-510-545-9700
Email: mdm-support@hexnode.com