

How to manage Ascom devices using Hexnode UEM



hexnode

Ascom is a global device provider focused on healthcare ICT and mobile workflow solutions.

The Ascom range of mobile devices includes medical-grade mobile devices, enterprise-grade Android™ smartphones, DECT and VoWiFi handsets, and ATEX- and IECEx-certified DECT handsets.

Hexnode's partnership with Ascom enables our users to leverage Ascom's API for device management via OEMConfig which extends the management capabilities beyond our native features.

Note:

Ascom's OEMConfig app is called the Ascom OEMConfig.

The main list of Ascom devices include:

- Ascom Myco 3
- Ascom Myco 2

Besides these, they specialize in pagers, ruggedized DECT handsets, VoWiFi devices, nurse call devices and software.

How to manage Ascom devices using Hexnode's native device management feature?

Hexnode's Android device management capabilities can be leveraged to manage Ascom devices directly.

Enrollment

Hexnode MDM provides a wide variety of enrollment methods for Android devices, you are free to choose the ones that are convenient for your business model.

No authentication enrollment:

It is the fastest enrollment method available. It only requires the server name. No authentication and no enrollment credentials are needed. All devices enrolled this way are assigned to a default user.

Email/SMS enrollment:

Here the enrollment credentials are sent to the users via email or SMS. These credentials have to be entered to complete the enrollment process.

Self-Enrollment:

This method allows the users to enroll their devices via Azure Active Directory, Active Directory, or Google user credentials. For other users, the admin may create a default user and a dedicated password manually or assign a common password or individual passwords for the users and send it to them as a bulk mail. The enrollment process is pretty much the same.

QR code enrollment:

In certain scenarios, it is difficult to enroll devices with credentials like username, password and portal name. Hexnode MDM lets you enroll devices easily by scanning a QR code.

ROM enrollment:

If your enterprise has a collaboration with Ascom you can flash a custom ROM to the Android Device with Hexnode MDM as a system app.

Android Enterprise enrollment:

Previously known as Android for work, it is currently the main enrollment method for android devices. It creates a separate work container on the devices. The separation of corporate and personal data is necessary if the devices are BYOD (Bring your own device) or COPE (Corporate owned personally enabled). The Hexnode for work app is used for Android enterprise enrollment. AFW# and ADB methods are also used for Android Enterprise Enrollment.

Zero-touch enrollment:

This is ideal for bulk deployment of devices. The devices need to be purchased from a Ascom zero-touch reseller partner. It is ideal for corporate-owned devices as it is a one-time configuration process. Hence, the devices come pre-configured out of the box. This also eliminates the need for user intervention in setting up the devices.

Management

Hexnode provides the A – Z in device management. The main management features for Ascom devices include:

Device info and monitoring:

Android Device monitoring features include a device summary which provides a summary of the hardware info like model, type, OS version, root info, battery level,

memory level. It also provides enrollment details (last checked-in, last scan, device id, enrollment date, and status).

Location information is also available with map support to pinpoint the exact location the device was the last active at. Compliance with policies and restrictions, the number of apps currently on the device, activity status, the number of policies currently associated, kiosk status, and last checked-in time can also be viewed from the Manage section.

The device info section includes the device model name, the manufacturer (Ascom), Serial no, UID, etc. The network Info section includes the phone number of the SIM cards on the device, IMEI numbers of the device, roaming status, carrier details, etc.

Application, Policies, Security sections under manage has the full list of associated policies and applications.

Actions:



A large list of actions are available for Ascom devices. Scan option is used for scanning the devices to refresh the data and listing the current device status, it can also be used to scan the device location. Lock, wipe, remote ring, enabling lost mode actions are useful in cases of emergency (lost or stolen devices with valuable corporate data).

Changing the device owner, installing and uninstalling applications, associating configured policies, OS updates, changing the friendly name for the device, changing ringtone, importing contacts to the device can all be done remotely via the actions tab in the device management.

Enabling and disabling kiosk mode can be achieved at the click of a button. Broadcasting notifications and messages to the selected devices are very popular among our users.

The action tab also allows the exporting of device details as a pdf file. When you are all done with a device you can disenroll it from the Henoxide MDM portal using the Disenroll device action.

Action History section shows the activity log for the device along with the status of each action and messages related to it.

Remote control and view:

The manage tab for Android devices provides the remote device view option. This is achieved via the remote view app which can be remotely installed on any device. It lets

you view the user's device in real-time. This nifty feature lets you monitor the users that require supervision.

The remote control feature is available for Android 5.0+ and Android Enterprise devices. The remote control allows admins to monitor and take control of the device from their PC. It can come in handy when you need to take control of the devices to diagnose and fix problems reported by the users in real-time.

Data Management:

The data management section under Manage shows the data usage by the device as a whole and for each app individually.

Total data usage, Mobile data usage, WIFI data usage as a whole, and for each application are listed under this section. The data usage details can be exported as a CSV or PDF from here. The section also has filters to view the usage by dates and periods. A list of apps with blocked data access is also listed here.

Users, devices, and groups:

All enrolled devices can be divided into groups for easier monitoring. Similarly, users can also be grouped.

Grouping of devices and users not only allows easier monitoring, it also helps in managing them together via actions and policies. Grouping is highly recommended in cases where the device count is high.

Hexnode MDM also supports dynamic grouping. Dynamic groups keep changing automatically based on certain specified conditions. In dynamic grouping, devices move in and out of the group during the periodic group sync, whereas custom groups maintain devices as a fixed list. The sufficiency of minimal manual effort makes dynamic grouping more desirable than manual grouping.

Restrictions

Device Functionality:

Enable or disable device functionality features like camera, USB file transfer, safe mode, lock screen orientation and lock screen timeout.

Network Settings:

Provision to forcefully turn the Wi-Fi on and off besides disabling or enabling the feature can be useful to certain enterprise needs.

Enabling or disabling Bluetooth, tethering, a portable wi-fi hotspot, and data roaming can be done.

Synchronization settings:

Backing up or restoring data from google drive can be disabled on Android 8.0+ devices in device owner mode.

Advanced device functionality restrictions:

Disabling of the device microphone, screen capture, making a call, volume adjustment, and the copying of content between normal and work profiles are available for Ascom devices.

Advanced Display settings:

Hiding the device status bar and displaying dialogs/windows are available under this section.

Advanced Connectivity settings:



Bluetooth data transfer, android beam, configuring Bluetooth, configuring cell broadcast, configuring cellular network, configuring Wi-Fi, configuring hotspot and tethering, and the ability to reset network settings can be disabled from the Hexnode MDM portal.

Advanced account and application settings:

Sending SMS, configuring user credentials, and modifying the user's Google accounts (add, delete, switch) can be done here.

Installing and uninstalling apps, modifying application settings, app verification before installations, allowing the installation of applications from unknown sources, parent profile app linking, and app runtime permissions can all be enabled or disabled to suit your enterprise's needs.

Other advanced settings:

Factory reset protection can be disabled or bypassed on devices in Android Enterprise device owner mode.

Enabling location sharing, USB debugging, factory reset, reading external connected media, setting up time zone, updating date and time automatically, and configuring VPN can also be done via the Hexnode MDM portal.

All advanced device settings are available only for Android Enterprise devices.

Policies

Password:



Secure your Ascom devices with Hexnode's password policy. Password complexity, password age, password history can be configured for the devices. Added security via auto-lock and device wipe after a set number of failed attempts can also be configured. This method is used to lock the entire device in normal mode. In device owner mode the password policies are only applicable to device owner container and work apps.

For devices running Android 7.0+ enrolled in profile owner mode the work profile alone can be locked with the password policy.

App Management:

Mandatory app policy allows you to install applications on the device. In android enterprise mode (as managed google apps), rooted devices, and devices with Hexnode MDM app as a system app, apps can be installed on the device silently. In all other cases, user intervention is required to install applications.

Blacklisting of apps in Android Enterprise devices will cause the device to fall out of compliance if the blacklisted applications are present on the device. In the Profile Owner mode, blacklisted apps will be hidden from the work container. Whitelisting of apps causes all other apps(not whitelisted) to be considered as blacklisted.

App Cataloging is used to create a customized app store on the end user's device. App configuration and app permissions can be used to manage and configure the applications before pushing them to the devices (Only in Android Enterprise).

Networks:

Wi-Fi networks can be pre-configured and associated to the devices so that they can connect automatically to the network without prompting the users to enter passwords. This saves the organization the hassle of sharing the credentials with each employee.

Security:

Certificates can be installed on the Ascom devices remotely to ensure higher security. Similarly, OS updates can also be scheduled on devices enrolled in Device Owner mode.

Configurations:

Wallpaper for the device home screen is customizable on all devices with Android 4.4 and above from the Hexnode MDM portal.

Mobile Data Management and File Management:

The Mobile data management feature on Android 6.0+ devices allow admins to monitor how Wi-Fi and mobile data connection are used. Usage limits can be set up, network connectivity can also be restricted if limits are reached (monthly, daily, etc. on the device as a whole or on apps individually). This can be useful in tracking data-hogging applications.

File Management can be used to upload files (videos, audios, images, documents) to a designated space within an enrolled device.

Kiosk Features:



In most enterprises, the devices are used to access only a limited set of applications. Single app and multi-app kiosk modes by Hexnode MDM can be used for locking down your devices to only the required applications.

Hexnode also provides the option to run apps in the background as certain apps require access to other apps to function properly. The devices can be turned into Digital signages for advertisements and can be set up as a self-service kiosk. A custom kiosk launcher, kiosk screen savers, website kiosks are just the tip of the iceberg.

Kiosks can also be highly customized by restricting device actions and buttons. Kiosk exit settings and website kiosk settings should be configured as per the requirement to adapt the kiosk to the enterprise's needs. Hexnode browser lite and Hexnode kiosk browser features can also be modified to control how the website kiosk works.

Ascom devices are commonly used as rugged devices, hence Hexnode's extensive kiosk capabilities will complement it quite nicely.

Geofencing and Location Tracking:

Location tracking is useful for turning automatic location tracking on and off and setting the location tracking interval. Users will not be able to change these settings once the configuration policy is associated.

Geofencing is used to create a virtual fence on the map when devices exit the fence they will be marked as non-compliant and the admins will be notified. One of the many high-security Hexnode features.

Android Enterprise Compliance:

This policy can be used to deactivate the Android Enterprise container on non-compliance. The deactivation time can be set for securing corporate data.

Other key features

Apps:



The apps tab has everything related to applications. You can add enterprise apps and push them to the devices directly or via policies. App catalogs, app grouping, store layouts can be configured here.

You can turn websites into web apps and push them to the devices.

Customizing apps, creating file shortcuts for video and pdf files, app management, app configurations, app permissions, and OEMConfig capabilities can be created and modified here.

Admin Settings and Reports:

In addition to all the specific features, Hexnode's common alert and management features are also available for Ascom devices.

Inactivity settings to mark devices as inactive after a specified period. Scheduling device scans at regular intervals. Added compliance settings like device encryption, device inactivity, MDM app removal from the device, battery level alerts and notifications, etc.

Action and compliance notifications can be enabled/disabled to notify the admins or users as the case may be. A detailed report section shows a list of devices, users, compliance, location, data management, application, and audit reports. These reports can be filtered and viewed. They can also be scheduled and exported as a CSV or PDF file.

How to manage Ascom devices using Hexnode's OEMConfig capabilities?



To access the OEMConfig set of features for Ascom devices

Step 1: Go to the Apps tab on your Hexnode portal

Step 2: Select Add apps > Managed Google Apps

Step 3: Search for the Ascom OEMConfig application and Approve it

Step 4: Go to policies > New policy > New blank policy > Android > App configurations > Configure > Add new configuration > Select the Ascom OEMConfig app

Selecting the application will show you the list of all available device features that can be managed on Ascom devices using OEMConfig.

Select the management options for the required features and save the policy. Assign this policy to the required Ascom devices for management.

Ascom's OEMConfig capabilities with Hexnode MDM

Selecting the application will show you the list of all available device features that can be managed on Ascom devices using OEMConfig.

Select the management options for the required features and save the policy. Assign this policy to the required Ascom devices for management.

Connectivity Settings

Wi-Fi location services:

When turned on, third-party applications will be allowed to access Wi-Fi access point info via the proprietary location API. This setting also controls if Wi-Fi events are written

to the event log or not.

Wi-Fi location scanning:

Turn on to perform Wi-Fi location scans within a specified scanning interval. The scan result will be available to all installed third-party applications.

Wi-Fi scanning interval:

Set the number of seconds (minimum 5 and maximum 300) to wait between each scan. If left blank, the scanning interval will be set to 10 seconds by default.

Save logs:

Select the time for saving the logs.

Additional SIP trace:

If enabled, additional debug logs are produced by the SIP stack.

Additional Wi-Fi trace:

When turned on, additional debug logs will be produced by the Wi-Fi stack.

Network packet logging:

Choose the network packet logging mode: Off – to disable the network traffic logging. Local – to start tcpdump logging traffic on a network. If disabled later, the stored files should be removed manually. Remote – to enable remote logging. Switch to this mode to allow Wireshark sniffer to connect to the device to get network traffic from it.

Network logging hostname:

Specify the IP address or hostname that is allowed to connect to the device and receive network traffic.

SIP Transport:

Define the protocol to carry the SIP signaling traffic. The change will take effect once the device is restarted.

Primary SIP proxy:

Define the SIP PBX by an IP address, a domain name, or an IP address with a port number. If left blank, SIP telephony will be disabled. Examples of valid formats are: pbx1.mydomain.com or 192.168.1.1:5060

Secondary SIP proxy:

Define the optional SIP PBX, if the handset fails to register with the primary SIP PBX. Specify an IP address, a domain name, or an IP address with a port number. Examples of valid formats are: pbx1.mydomain.com or 192.168.1.1:5060

Listening port:

Specify the port that the handset listens to for incoming SIP traffic. If not specified, 5070 port will be set by default.

SIP proxy ID:

Define the ID to be used as the Primary/Secondary SIP message headers (optional).

SIP Register expiration:

The number of seconds for register expiration. If not specified, 120 seconds will be set by default.

Key Settings

Function:

Defines what function is triggered by a long press on this button. (activate barcode scanner, send custom intent).

Duration for long press:

Defines how long the button shall be pressed until it is recognized as a long press.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Function:

Defines what function is triggered by multi press on this button.

Number of button presses:

Defines how many times in one sequence the user must press the button to get multiple presses.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Function:

Defines what function is triggered by a long press on this button.

Duration for long press:

Defines how long the button shall be pressed until it is recognized as a long press.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Function:

Defines what function is triggered by multi press on this button.

Number of button presses:

Defines how many times in one sequence the user must press the button to get a multiple press.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Function:

Defines what function is triggered by long press on this button.

Duration for long press:

Defines how long the button shall be pressed until it is recognized as a long press.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Function:

Defines what function is triggered by multi press on this button.

Number of button presses:

Defines how many times in one sequence the user must press the button to get a multiple press.

Define the action of the intent:

Specify an action to be performed.

Define the component of the intent:

Specify the component name (if the explicit intent should be sent). The component can be any of the following formats: package, package/component or package/.component.

Define the data of the intent:

Specifies the data to be acted on. The data must be in a Uri format.

Profiles:

Create profiles with the list of supported symbologies. Profile 1 is the default profile.

Profile name:

Set the profile name.

Advanced Device Settings

Linear barcodes:

Select the enabled barcode symbologies in this profile.

Postal barcodes:

Select the enabled barcode symbologies in this profile.

Matrix (2D) barcodes:

Select the enabled barcode symbologies in this profile.

Advanced settings:

Option to specify parameter settings following the format P[parameter number]=[desired value], e.g. P7=1. Entries are separated with a “,”. When conflicting, advanced settings will override other settings.

App configurations:

Configure the scanner for specific apps.

Package or Activity name:

Entitle the app that will use this configuration. Use the package name, optionally joined by a ‘/’ and the activity class name. Use a wildcard ‘*’ in the end to match multiple packages or classes.

Profile:

Assign the scanning profile to this app (name or number). If empty, Profile 1 is used.

LED:

Set the default setting for the LED light beam. LED can also be temporarily turned on/off directly on the viewfinder screen.

Viewfinder:

When turned on, the scanning area is shown on the handset screen.

Start scanning in viewfinder automatically:

When turned on, scanning starts immediately in the opened viewfinder. If disabled, scanning is triggered manually by pressing the scan button.

Picklist mode:

Choose the aiming pattern to be shown on the viewfinder screen. Only those barcodes that are placed in the center of the selected pattern will be scanned.

Keystroke output:

Enable output of data in the form of simulated key presses.

Send Enter key:

Enable to automatically send Enter key when a barcode has been successfully scanned.

Action key character:

Set a special character to trigger the action key if found embedded in the barcode.

Intent output:

Configure the scanner for specific apps.

Intent target:

The target component type of intent sent for this app.

Intent identification prefix:

Prepend an optional package name to intent identification strings which start with a dot. Applies to action, category and extras identifiers.

Intent action:

The intent action to use for the output data.

Intent category:

The optional intent category to use for the output data.

Scanned string intent extra:

The intent extra key that identifies the scanned data when sent as a string.

Scanned data intent extra:

The intent extra key identifies the scanned data when sent as a list of byte arrays.

Source intent extra:

The intent extra key that identifies the data source for the barcode data. This key will always have the value of 'scanner'. If left empty, the intent extra will not be included in the intent.

Type intent extra:

The intent extra key that identifies the type of the scanned barcode. If left empty, the intent extra will not be included in the intent. The value for the type intent extra shall be LABEL-TYPE-< symbology >, e.g. LABEL-TYPE-EAN13.

IR location services:

If enabled, third-party applications will be allowed to access the IR location of the handset. The four latest detected IR Locators can be provided to the application.

IR short range:

Short range mode reduces the impact that sunshine or incandescent light has on the IR coverage area, and is typically used when large glass areas are present at a site. If short range mode is not used at these sites, the coverage area will differ between day and night.

Endpoint ID:

Set the identity to register with at the SIP PBX (use the phone number or name).

Password:

Set the password to register with at the SIP PBX.

Codec configuration:

Defines which codec to use for speech

DTMF type:

Defines the signaling path to use for sending DTMF. Either in the RTP stream, as specified in RFC 2833, or with SIP signaling, using the SIP INFO method.

Hold type:

Define the type of hold to send when the handset puts a call on hold. The selection depends on what type of hold the PBX supports.

Replace Call Rejected with User Busy:

Turn on to send “User busy” instead of “Call rejected” cause code if an incoming call is rejected.

Dialing tone patterns:

Defines which tone pattern to use when dialing. When there is a SIM card, the phone will revert to the SIM card’s country and dialing tone.

Voicemail Message Server number:

Specify the number to the Message Server. If specified, the handset will interrogate the Message Server for voicemail message waiting for indications (MWI) after registering with the SIP-Proxy.

Voicemail number:

Specify the user’s voicemail number in the Voicemail Message Server.

Reset voicemail MWI:

Turn on to reset message waiting indications (MWI) in the Message Server once the user has listened to all new messages.

Lock Home screen layout:

Enable to prevent the widgets and shortcuts from being removed or repositioned. You will no longer be able to add any apps to the Home screen.

Automatic updates:

Turn on to allow the device to automatically download and install the latest available

updates. Note that an update will start when the device is placed in a charger and the battery level is at least 20% of charge.

Software policy URL:

Enter the URL to the policy where available software updates will be downloaded from. Valid URL protocols are http and https. If no protocol is specified, https will be set by default.

Note:

It is highly recommendable to use the native policies wherever possible as the OEMConfig features are still relatively new. The introduction of OEMConfig has opened up a new set of possibilities that will be added to in the future and the existing features are expected to get more fine-tuned.

Ascom's brand enterprise-grade devices have been improving workplace efficiency, safety and providing patient and customer satisfaction worldwide.

A dedicated device management service like Hexnode MDM can assist such devices to maximize productivity at any workplace.