



## eScan Enterprise Mobility Management (Android Enterprise)

Enterprises empower their employees by allowing the use of mobile devices under a Company Owned Devices (COD) policy or by implementing Bring Your Own Device (BYOD) policy for work operations. The use of Android devices in the workplace increases the risk of data loss and unauthorized data access. Therefore, it is necessary to keep personal and work data secure and separate, as well as to configure restriction policies on the devices.

Our Android Enterprise solution plays a vital role in the management of Android devices as a COD or BYOD within the organizations infrastructure. eScan EMM keeps personal and enterprise data separate and secure by enforcing required security controls on the devices. EMM introduces a single centralized platform to secure data from a diverse range of mobile devices. With policy-based controls and sophisticated threat protection, it allows proactively enable mobile productivity without compromising enterprise security.

### Benefits

- Deploy, manage, and protect Company-Owned Devices (COD) and Bring Your Own Devices (BYOD).
- Implement various device controls on user's device remotely.
- Install/Uninstall applications on devices without user intervention.
- It allows admin to define and set the customized passcode policy for the enrolled devices and work profile.
- Allows enrolled devices to connect only to the listed Wi-Fi networks.
- Secure data and resources and enhance user's productivity.



## Device Management

---

Today, most of the employees are using mobile devices to perform corporate tasks and access corporate data from anywhere and anytime. Use of mobile devices improves productivity and allows employees to work in a favorable and flexible environment. With improved productivity, mobile devices may be harmful if hacked, stolen, or lost. Thus, the management of devices is a crucial part of any enterprise. eScan EMM helps the IT Administrator to manage the mobile devices within an organization, the devices are enrolled either as COD or BYOD.



## Company Owned Device - COD

---

In this case the device is provided by the enterprise, it will be enroll as COD (Company Owned Device), and the security policies will be applied on them to safeguard corporate data. These devices are centrally managed by IT admins through the eScan Management Console with security protocols and business applications.



## Bring Your Owned Device - BYOD

---

On the other hand, employees can use their personal devices for enterprise work without compromising their own privacy. In this scenario, devices are enrolled as BYOD by applying security policies to avoid data confliction and loss. In the case of BYOD, a work profile will be created on the employee's device to allow them to use same device for both work and personal purposes. It ensures the users privacy as well as enterprise security, keeping enterprise data and applications separated from personal data and applications. The work profile is indicated by a suitcase symbol. Containerization and its benefits are available for BYOD.

# Features of Enterprise Mobility Management (Android Enterprise)



## Mobile Device Management

---

This module allows you to create a new group, task, and policy template as per requirement. Admin can add one or more new devices to single group and deploy policies for both Android and iOS based devices that are enrolled in the group. Admin can move devices from one group to another and also remove them from the group.

## Features of Enterprise Mobility Management (Android Enterprise)

### App Store

Our App store module lets you add applications directly from Google Play store and iOS App Store. The Administrator can create separate Managed Configurations for these applications as per their requirements. One can also install and uninstall these applications silently as required. In-house Applications can also be uploaded for Managed Devices.

### Content Library

This will allow the administrator to deploy documents to the managed devices through the web console. The document types that are supported for deployment are PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, TXT, JPG, JPEG, PNG, and BMP. You can use this feature to share work related documents across multiple devices at the same time.

### Anti-Theft

eScan EMM's Anti-Theft feature make it possible to recovery of device in case of loss/ stolen preventing it from being misused. Admin can remotely wipe all the data available on device and also block a device. It allows to send a message on stolen device as per requirement. Additionally admin can remotely execute commands such as Scream and Locate through eScan Anti-Theft Portal.

# eScan<sup>TM</sup>

Enterprise Security

An ISO 27001 Certified Company

Toll Free No.: 1800 267 2900

[www.escanav.com](http://www.escanav.com)

**MicroWorld Software Services Pvt. Ltd.**

CIN No.: U72200MH2000PTC127055

Tel.: +91 22 6772 2900

email: [sales@escanav.com](mailto:sales@escanav.com)

#### Awards



#### Partnerships



#### Comprehensive Protection for

SOHO • BUSINESS • CORPORATE • ENTERPRISE

