



eScan Enterprise Mobility Management

Enterprises empower their employees by allowing the use of mobile devices under a Company Owned Devices (COD) policy or by implementing a 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 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 for Android and iOS devices, it allows proactively enable mobile productivity without compromising enterprise security.

Benefits

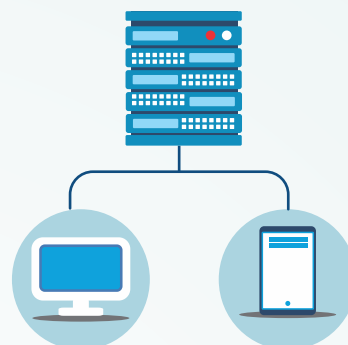
- BYOD & COD Management & Security
- Common QR Enrollment
- Silent App Install/Uninstall
- Custom Passcode Policy Management
- Wi-Fi networks restrictions
- Device Restrictions
- Kiosk Mode

Solution Sets



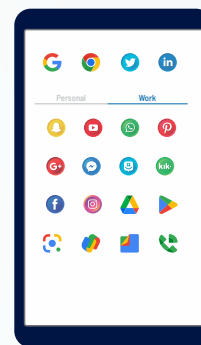
Device Management

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 employee's 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.



Bring Your Own 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.



Company Owned Device - COD

In this case the device is provided by the enterprise, it will be enrolled 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 to perform work related tasks.





Kiosk Mode

The Kiosk Mode policy, allows admin to control the usage of devices within organizations by limiting the device functionalities that keep employees focused on work. It lets you run a device in Single App Mode or applications selected by limited. Additionally, admin can restrict the hardware key controls such as volume and power buttons on the enrolled devices to the kiosk mode.



Key Features



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.



Mobile Threat Defense (MTD)

Mobile Threat Defense (MTD) is the process of identifying and analyzing security risks on mobile devices, such as virus attacks, phishing, and OS vulnerabilities. It displays threat alert statistics of multiple threat events that occurred on managed devices, categorized by severity into critical, high, and low alerts, to help prioritize responses.



Two Factor Authentication (2FA)

Two-factor authentication (2FA) is a security process that requires users to provide two forms of identification to access their accounts. Unlike single-factor authentication (password only), which is less secure and exposes data to higher risk, 2FA adds an extra layer of protection to your eScan web console login.



Enterprise Play Store

Our Play store module lets you add applications directly from Enterprise 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.



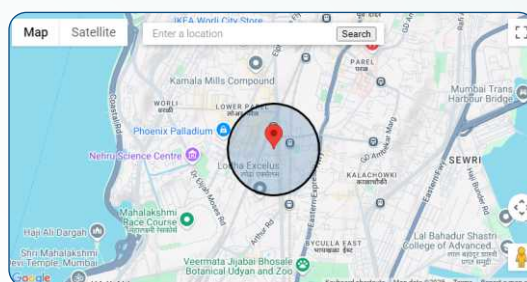
Anti-Theft

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 EMM console.



Geo-Fencing

Geo-fencing is an eScan Web Console feature of EMM which involves creating a virtual boundary around a specific location using GPS (Global Positioning System) or IP addresses. This boundary can range from 100m to 5000m in radius. When a device enters this defined area, the security policy set by administrator gets activated on the device. This policy automatically gets deactivated when a user takes the device out of Geo-fencing.







Other Highlights

- ◆ Device Management Console
- ◆ Manage App Permissions
- ◆ Silent App Installation
- ◆ Single-App Mode
- ◆ Web Apps
- ◆ Bluetooth control
- ◆ USB File Transfer control
- ◆ Factory Reset Protection
- ◆ Camera disable control
- ◆ Disable Airplane Mode
- ◆ Facetime control
- ◆ Screenshot Capture control
- ◆ Siri Control
- ◆ Email Configuration Policy
- ◆ Safari Configuration policy
- ◆ System Updates
- ◆ Disable Cross Profile Copy/Paste

Pre-requisites

Server

-  Public IP address for eScan server
-  The domain name should be mapped to public IP
-  SSL and CA certificate
-  A Google Account

 **Note:** This account should be a personal account, not an account associated with G Suite or other managed domain accounts

Server OS

Microsoft® Windows® 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-bit and 64-bit Editions)

Minimum Hardware Requirements

- ◇ CPU - 2GHz Intel™ Core™ Duo processor or equivalent
- ◇ Memory - 4 GB and above
- ◇ Disk Space - 8 GB and above

Minimum Device Requirements

Android Endpoints Platforms Supported:

- ◇ Android version: 7.0 and above
- ◇ Storage: 50-60 MB

iOS Endpoints Platforms Supported:

- ◇ iOS version: 12.0 and above
- ◇ Storage: 50-60 MB

 **Note:** Rooted and Jailbroken devices are not supported.

Supported Browsers

- ◇ Internet Explorer 9 and above
- ◇ Firefox 14 and above
- ◇ Google Chrome latest version

Product Information

Link: <https://androidenterprisepartners.withgoogle.com/provider/#!/nGfPhZPy5tgNywsyx6nG>

Connect with us:

Technical Support	: support@escanav.com, android@escanav.com
Sales	: sales@escanav.com
Forums	: https://forums.escanav.com
eScan Wiki	: https://www.escanav.com/wiki
Live Chat	: https://www.escanav.com/english/livechat.asp



An ISO 27001 Certified Company

Toll Free No.: 1800 267 2900

www.escanav.com

MicroWorld Software Services Pvt. Ltd.

CIN No.: U72200MH2000PTC127055

Tel.: +91 22 6772 2900

email: sales@escanav.com

Awards



Partnerships



Comprehensive Protection for
SOHO • BUSINESS • CORPORATE • ENTERPRISE

