eScan™
Anti-Virus & Content Security

eScan
Mobile Device Management

Adding Mobility to your Enterprize

www.escanav.com

sales@escanav.com

eScan Mobile Device Management

eScan™
Anti-Virus & Content Security

Overview

Business world is no stranger to their transformation towards Enterprise mobility and with advancement in technology, progressive incorporation smartphones, tablets into companies is now a reality. Ensuring that the employees can work from their mobile device efficiently and securely is vital for business success. The widespread proliferation of mobile devices puts unprecedented computing power and information at the fingertips of individuals throughout an organization. The growth of enterprise mobility solutions has been fuelled by the rapid evolution of next generation mobile devices, high speed internet access and adoption of smart mobile devices including smartphones and tablets by the workforce. In last few years focus has shifted from securing physical devices towards securing the information on devices. Unlike PCs, which are provisioned and managed centrally by IT as part of the enterprise IT infrastructure, mobile devices continue to be purchased by end users and are easily introduced into today's networks with little or no control over the data, applications, and resources present on the devices. Once a personal device is connected to the enterprise network, the IT administrator has regulatory responsibility to know essentially everything happening or occurring on or through that device. Our Solution enable secure mobile device use in companies, safeguarding sensitive corporate data and shielding the network from mobile threats, while deploying, and complying with regulatory and corporate policies.

eScan Mobile Device Management

Features at a Glance

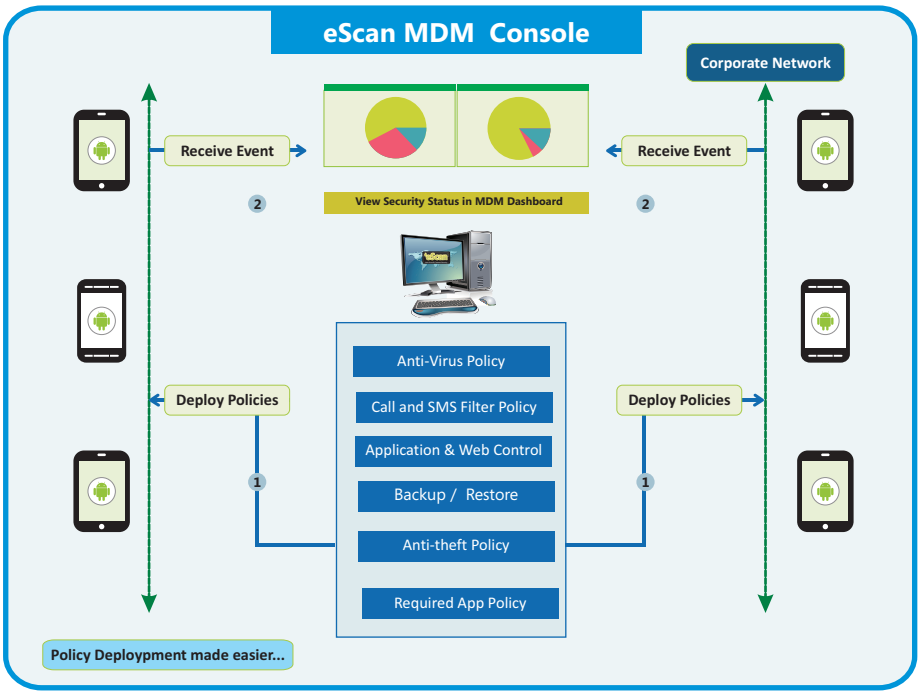
eScan offers variety of robust features from a single web based console that can manage computers as well as mobile devices on your network, meeting all the needs of volatile world of Enterprise Mobility through advanced security and management features supported by robust technology architecture.

- **Device Discovery** - eScan Mobile Device Management console displays the entire list of mobile devices present on the corporate network along with important details like MAC ID, manufacturer and IP address allocated to it.

- **Enrolling Devices** –eScan facilitates easy deployment of security suite on all android devices. It allows adding of Android devices on it MDM Server after which a download link is automatically sent to the email address of the user that was used during enrolment.For registering the device it provides manual enrollment (where the user fills registration details manually on the device)as well as enrollment through QR Code(where the registration details are captured from the QR Code sent on enrolment email). "Enroll Devices so that users can securely and seamlessly access corporate data."

- **Secure, Easy, and Scalable Policy Deployment** – eScan Mobile device Management system facilitates deployment of security policies on devices

through an easy-to-use web based Management Console. These policies are the rule sets that ensure total security of Devices where eScan is installed, facilitating centralized management and providing visibility over enrolled mobile devices.



Devising a Security Policy

Any approach to securing Mobile Devices in an enterprise must focus on finalizing policies that define the limits. It is very critical for an Enterprise to define policies, on one hand set limits and on the other create efficiency in compliance with the IT policies of the company.

- Devices must be categorized on the bases of Workgroups or departments to which they belong to.
- User groups must include employees, customers, visitors, partners and other miscellaneous groups as a part of well-planned security structure.
- Companies must finalize the web access policy along with required app policy for all work groups.

For example – International Sales group may be allowed to use Facebook whereas Accounts group may not be allowed to do so. Similarly, use of Mobile Camera may not be allowed in office. A mix of well-thought-out policies and up-to-date technologies are needed to protect and manage Devices on corporate network.

Core Elements of eScan Mobile Device Management Policy

Elements	Description
Anti–Virus Policy	Allows you to configure settings for protecting and scanning enrolled android devices.
Call and SMS Filter	Allows you to Filter Calls and SMS on enrolled devices - Blocking of unwanted Calls and SMS on the basis of blacklist and whitelist defined by the administrator. It also allows you to whitelist certain numbers to which outgoing calls from the device will be allowed, calls to all other numbers will be blocked.
Parental Policy	Configure comprehensive policies of Application and Web control for all enrolled android devices. Allows you to block / allow websites or applications on the basis of pre-defined categories. Default allows or Default block list policies ensure hassle free policy deployment.
Anti-theft Policy	Configure settings for Anti-theft module that enables advanced security options on enrolled devices like remotely Wipe Data, Scream (Sound Alarm), Block Device, Send Message, and Locate Device.
Additional Settings Policy	Allows you to configure settings for Notifications, Log and default sync frequency of enrolled devices with server.
Password Policy	Allows you to define administrator Password for Administrator access rights for eScan installed on enrolled android devices.
Device Oriented Policy	Allows you to configure settings to enable / disable GPS on enrolled devices.It also allows you to disable Camera, Bluetooth, or USB Connectivity.
Required Application Policy	Allows you to deploy approved applications on enrolled devices that are in accordance with the compliance policies of the company.
WI-FI Settings Policy	Allows the administrator to define settings to Disable WLAN / WiFi, Enable WiFi Restrictions, allow the device to connect ONLY to listed WiFi network name (SSIDs), Lock Device / sound Alarm (Scream)- Device(s) will lock / Sound alarm when NOT connected to either of the listed WiFi network name (SSIDs)
Schedule Backup	Schedule Backup of Contacts and SMS at desired time or day
Content Library	Distribute Files and Documents to Managed Mobile Device groups using eScan MDM's Content Library module

eScan™
Anti-Virus & Content Security

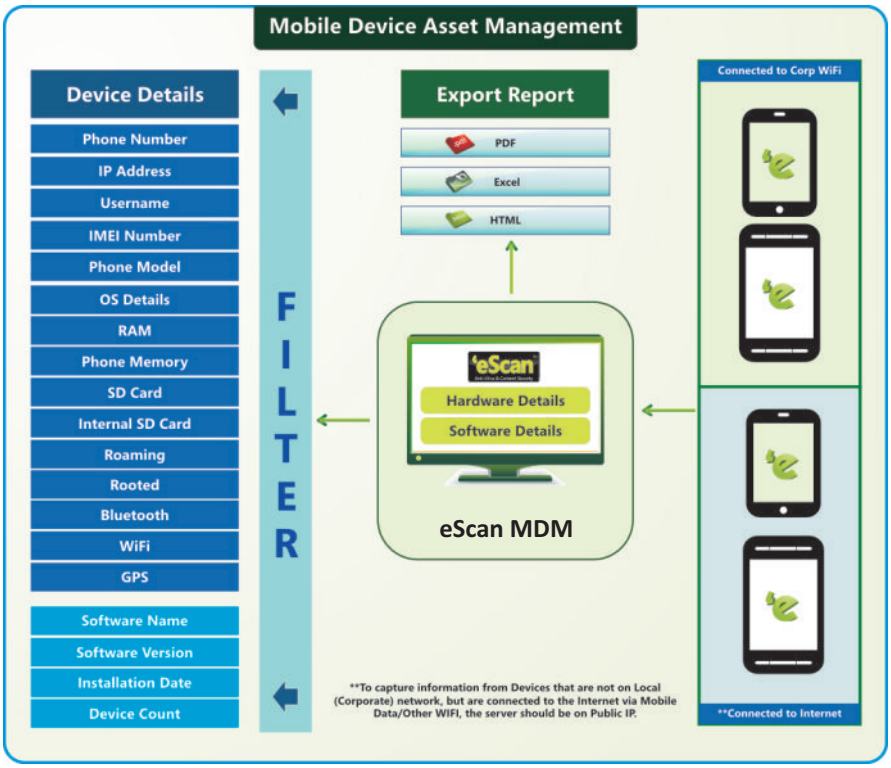
Business Benefits

- "Manage devices and network access policies, from a single Console."
- "Enforce security, or restrict internet access (only through selected WI-FI Network)."
- "Lock down devices to an approved set of websites or apps."

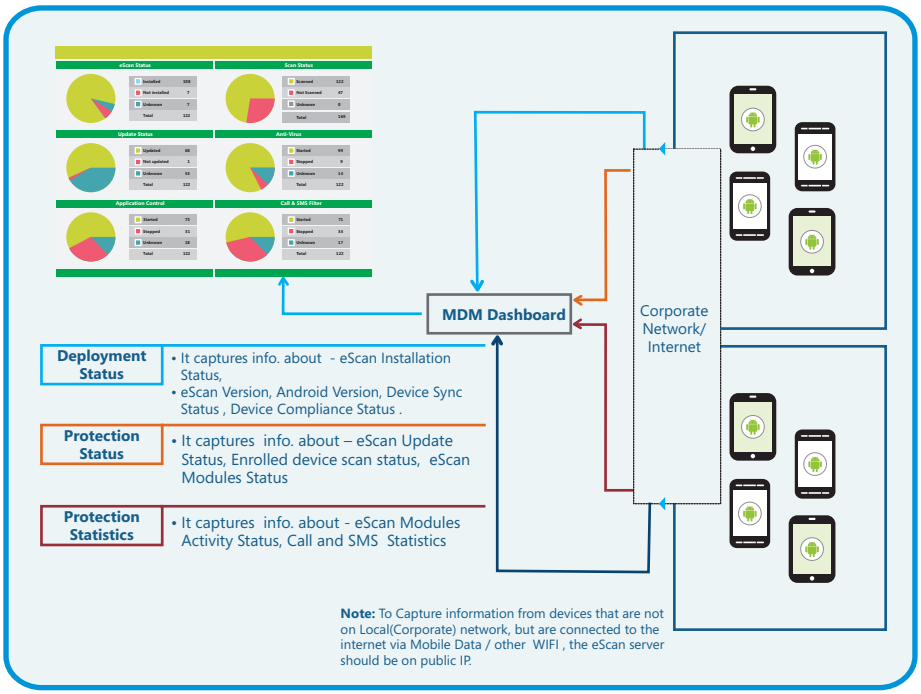
- **Managing Backup** – eScan allows you to take backup of SMS and Contacts from Devices to MDM Server. You can restore them on the device whenever desired.
- **Anti-theft** – It comprises of various options like Wipe Data, Block Device, Scream(Sound Alarm), Send Message and Locate Device providing security and ensuring complete protection of your phone from any unauthorized access if device is lost or stolen.
- **Asset Management** – It allows you to capture important information of all enrolled devices like Hardware description of all Managed (Enrolled) Devices. eScan provides easy filtering, based on any or all information captured from devices to be included in or excluded in the report. Generated reports can be exported to PDF, Excel or HTML format. Live Events are captured for Hardware and Software changes on all enrolled devices.

"You cannot secure what you don't manage, and you cannot manage what you don't see"

How it Works?



- **Reporting and Analytics** – eScan's Mobile Device Management System is equipped with modules for advanced Report Generation, Capturing real-time events from the enrolled devices for eScan Update status, and security status/ level of the device. It also displays eScan deployment status (eScan installation, eScan Version, and android version of the device), Protection status (Module status) and Protection statistics (Module activity status) in form of Pie charts and graphs, providing greater visibility on security status of the enrolled devices.



App Store

App Store enables you to install Apps on the enrolled Android mobile devices through. Using the App Store you can Add apps to eScan's MDM console. After adding the apps you can push these apps to the managed devices through policy deployment.

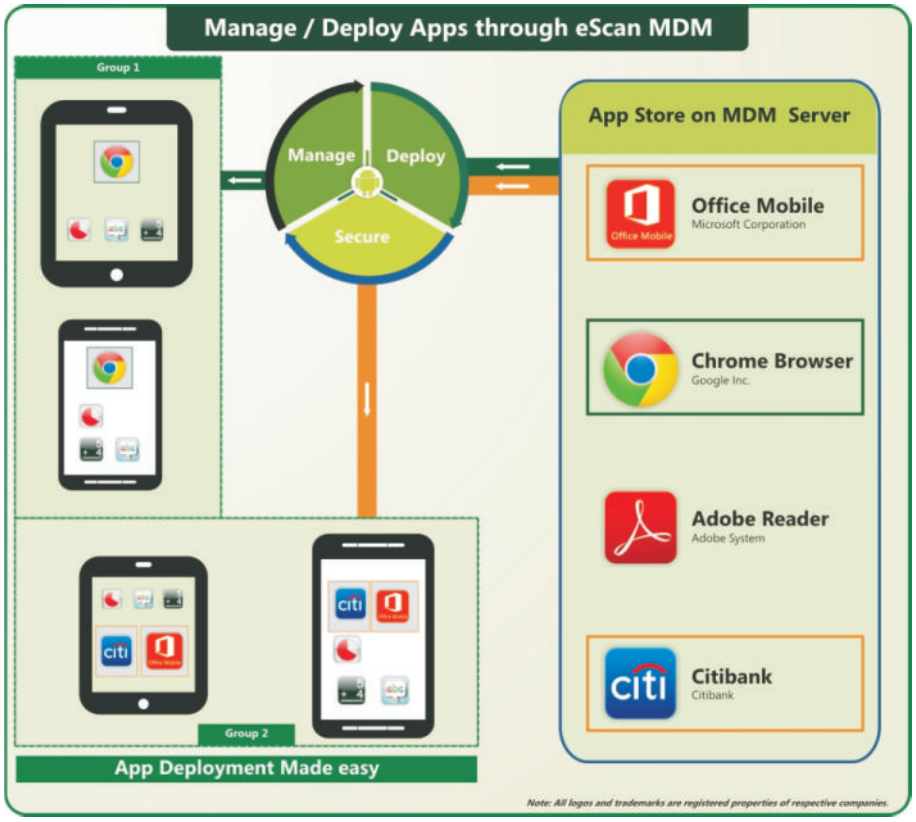
How it Works?

App Store on MDM Server

The app store on MDM allows the administrator to create a repository of all the apps required by the various employees in an Organization. The Administrator can add / remove apps from the app store and install them on enrolled android mobile devices.

Manage, Deploy and Secure apps through MDM

Administrator can deploy App on Mobile Devices based on the user's individual requirement or group policy, the following example shows that Chrome browser is installed on Group 1 where as office mobile and Citi Bank app is installed on devices enrolled under Group 2.



Call Logs

eScan maintains all incomming / outgoing as well as missed call logs on all enrolled mobile devices under Call Logs module on the MDM Console. It displays other vital details of the enrolled devices like contact number, name as in contact list, call / receive time and Call duration.

Content Library

Distribute Files and Documents to Managed Mobile Device groups using eScan MDM's Content Library module. Using this module you can easily distribute files with following extensions to enrolled mobile devices.Supported Formats - PDF, DOC, DOCX, XLS, XLSX, PPT, PPTX, TXT, JPG, JPEG, PNG, BMP.

Key Takeaways

- Device discovery and over the air device enrollment.
- Easy configuration and deployment of security policies on enrolled devices.
- Simple backup of Contacts and SMS from android devices to the MDM server and later restoring them back on the devices.
- Advanced Anti- Theft module that facilitates – Wipe Data, Block Device, Sound Alarm, Send Message and Locate Device remotely.
- Comprehensive Asset management giving complete visibility over enrolled devices.
- Advanced Reporting and Real time log management.
- Secured App Store for deploying Apps on enrolled devices.
- Advanced security features for malware detection, Web and Application control, Call and SMS Filter with strong policy deployment in accordance with the security policy compliance of the company.
- eScan maintains Incoming/Outgoing/Rejected call logs of all the enrolled Android devices.
- Distribute Files and Documents to Managed Mobile Device groups, using eScan MDM's Content Library.

Copyright Information

The Marketing Department
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334, USA.
Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024.
Web site: www.escanav.com
E-mail: marketing@escanav.com

Document Version – eMDM-14.1

Release Date – October, 2014