ENTERPRISE MOBILITY

Enterprise Mobility Management (EMM) is a holistic business strategy for enhancing the security and productivity of mobile devices used by employees. Kyocera's enterprise-ready mobile devices support EMM with a range of features, including device management, application management, information management and productivity tools.

SECURITY

Built-in security and encryption to keep your most sensitive documents protected. Includes customizable password requirements and encryption of files to ensure that important data is protected. For specific workplace restrictions, features such as camera, microphone, messaging, voice and data transmissions via Wi-Fi, Bluetooth and NFC can be disabled.

- FIPS 140-2 validated cryptographic module (includes AES 128/192/256) with NSA Suite B security
- Full encryption of Internal Storage and SD card (Data at Rest)
- Secure transfer of data (Data in Motion)
- SecureBoot enabled
- TrustZone support for Trusted Execution Environment (TEE)
- Certificate Management (i.e., for SSL connections)

VIRTUAL PRIVATE NETWORK (VPN)

Easily access your corporate network wirelessly from your mobile device anywhere a data connection is available. Includes customizable corporate profile and control settings.

- Advanced VPN capabilities utilizing Mocana solution
- Extensive Protocol Support: Internet Key Exchange IKE v1 (Aggressive Main Mode) IKE 2/ IPv4 / IPv6 / XAUTH / NAT Traversal
- VPNC compliant solution supporting most routers such as Cisco, Juniper, F5 and more
- Kyocera Enhanced MDM APIs to manage VPN

✳ MOBILE DEVICE MANAGEMENT (MDM)

Remotely monitor and manage employee devices to make sure they are compliant with company use and security policies. Gives the administrator the ability to locate, lock, and wipe devices remotely.

- Policy Violation Detection
- Remote lock and wipe of full device including SD card
- Password Robustness detection (password quality, repetition, detection and expiration interval)
- Network connection restriction (Wi-Fi, Bluetooth, NFC, Roaming)
- Sensor restrictions (Camera, Microphone and more)
- Device function restrictions (OTA updates, Sim Card Lock, Date/Time and more)

- Prevent storage of corporate data on SD card
- Enforce location policies (restrict/require location, prevent passive location data)
- Silent Install/Uninstall of applications
- Whitelist/Blacklist applications
- Prevent screenshot or clipboard cut/paste to protect sensitive data

♺ EXCHANGE ACTIVE SYNC (EAS)

Seamless access to corporate email, calendar, contacts, and meeting information wirelessly from your mobile device. EAS allows you to set features, syncing options, and functions according to your preferences or company policies.

- Enhanced Email client
- Advanced EAS Account settings for e-mail, contacts and tasks
- Improved EAS Account management (Add, Modify, Remove accounts)
- Advanced Calendar with sync, accept, forward and propose meetings along with meeting conflict detection

- Sync, view and change status of tasks
- Enhanced Global Address List (GAL) support
- Secure authentication with TLS/SSL certificate
- Secure attachments including S-MIME support
- Compliant with EAS device management solutions
- Support for file downloads over only Wi-Fi

Discover how Kyocera's devices can make your mobile network more secure and productive. Contact one of our business solution experts at 858-882-1833 or http://www.kyoceramobile.com/business/contact/

KYOCERƎ

KYOCERAMOBILE.COM