Remote MasterMind 4.0

Honeywell

Standard Support For Google® Android™

Google play

Honeywell's Remote MasterMind™ 4.0 software allows enterprises to manage virtually all mobile devices, including Google® Android™ operating system based devices, from a single remote location. This support provides you with the ability to manage your collection of geographically dispersed data collection devices with corporate or employee-owned consumer grade devices.

Support for Android™ Smartphones & Tablets

Organizations can optimize return on investment and welcome personal devices in the workplace by adopting a mobile device management (MDM) solution to reliably manage, track, support and secure their mobile devices. Remote MasterMind's innovative, industry-leading technology allows businesses to monitor their mobile field force with a comprehensive set of quality features.

Remote MasterMind enables the following device management value drivers to be performed on Google® Android™ devices.

Advanced Security Management

- Web filtering and white lists enforce and control web access policies to ensure secure, safe and authorized access to web content
- Antivirus/Malware protection monitors and safeguards device file systems and installed applications
- Out of contact device policies protect lost or stolen devices from data loss
- Implement lock-down screens to limit application and feature access
- Enforce strong password protection and certificate usage to ensure sensitive data is kept in authorized hands only
- Detect rooted devices to force remote security or prohibit access to corporate networks and data immediately
- Remote lock devices in real time to prevent unauthorized use
- Remote wipe corporate data only, or the entire device back to factory settings, in case of loss, theft, or misuse

Device Configuration & Communication

- Remotely manage up to tens of thousands of Android™ devices efficiently over the air (OTA). Devices can be enrolled, provisioned, configured and group managed wirelessly.
- A central, multi-platform display reports a wealth of device information including live device status, network connection, security policy compliance, and installed applications. This display also provides alerts on important device information, such as security status, encryption enabled, data roaming, and corporate email access.
- Easily deploy encrypted configurations OTA to customize device settings and enforce corporate security policies, allowing personal and corporate devices to be customized appropriately.

Asset Management

- Remotely access a variety of device information including Device ID, carrier, phone number, signal strength, battery status, memory, installed applications and more.

Mobile Application Management

- A customizable and private enterprise application catalogue allows businesses to automate the deployment of in-house applications to users OTA. Enterprise-developed applications can be sent directly to provisioned devices, without the use of Google® Play.
- Enable, disable or simply remove applications including those pre-loaded on the device such as YouTube.
- Monitor installed applications
- Protect application data through use of certificates and data wiping

Location-Based Services

- Locate and track remote devices
- Send driving directions to remote users' devices
- Apply location-based management policies by means of Geofences

Secure Content Library

- Securely distribute and manage access to corporate documents and resources.
- Configure on demand and push deliveries via synchronization

Telecom Expense Management

- Set up group and individual voice and data profiles to easily monitor data and voice usage limits.

Mobile Email Management

- Configure authorized sync of corporate email, calendar, and contacts using NitroDesk TouchDown, the most secure Microsoft® Exchange Active Sync Android™ application. License codes can be pushed to end users to simplify the purchase and deployment of the application.
- With NitroDesk TouchDown corporate email in a configurable sandbox, lock-down mode where corporate email settings can be enforced and data loss can be prevented, without the need for end user interaction. The application allows attachments to be restricted, sync settings to be customized, and corporate email to be remotely wiped or blocked, at any time.
- Block unauthorized mobile devices

Certificate Management

- Add, renew and deliver authentication certificates from a certificate authority to managed devices.

About Honeywell

Honeywell Scanning & Mobility is a leading manufacturer of high-performance image- and laser-based data collection hardware, including bar code scanners and rugged vehicle mount, hand-held and wearable mobile computers. With one of the broadest product portfolios in the AIDC industry, Honeywell Scanning & Mobility provides solutions that help improve operations and enhance customer service for users in vertical markets including retail, healthcare, warehousing, manufacturing, and transportation and logistics. Its innovative products are complemented by advanced software, service and professional solutions that enable customers to effectively manage data and assets. Honeywell products are sold worldwide through a network of distributor and reseller partners. For more information, please visit www.honeywellaidc.com.

For more information:
www.honeywellaidc.com/ReM

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
800.582.4263
www.honeywell.com

REM-4.0 Android Rev A 07/13