42GEARS®

Android Device Management For Beginners

Rise of Android Ecosystem

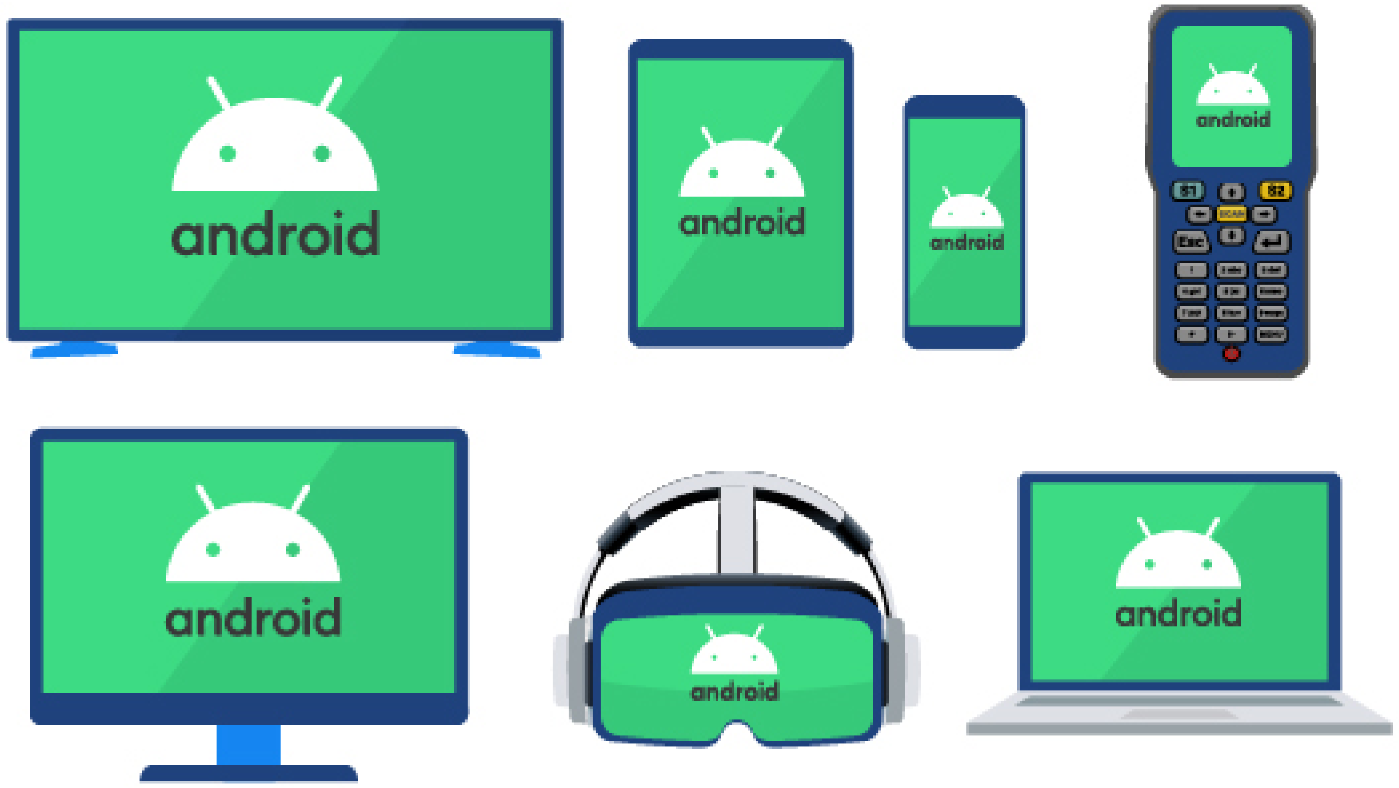
Adoption of Android devices by businesses has exploded in the past few years.

One of the primary reasons why organizations choose to use Android devices is their versatility. Android devices are available in a wide range of sizes and form factors, making them suitable for a variety of use cases. Another important advantage is the integration capability of Android with other Google services, such as G Suite and Google Drive.

In addition to their versatility and integration capabilities, Android devices are often more affordable than their iOS counterparts, which makes them a popular choice for organizations with limited budgets.

Android Device Management (ADM)

However, like with any platforms, Android comes with its own set of challenges, especially around security and manageability. Android is an open-source platform which makes it more susceptible to security threats than closed-source operating systems like iOS. Also when deployed for business use, mobile devices can break down due to software issues, or due to mishandling by the worker or the user. Inability of the IT team to resolve issues on Android devices deployed in the field can cause severe downtime causing direct and indirect losses to the company.



The most appropriate answer to the challenge of managing Android devices is to use a Mobile Device Management solution, sometimes also referred to as Unified Endpoint Management solution due to its capability to manage not only smartphones and tablets, but also desktops, laptops, and other non-standard form factor devices, running on any of the various Operating Systems.

Enrollment

Corporate-owned devices are owned and managed by an organization, and are typically used by employees for work purposes. Employee-owned devices, on the other hand, are mobile devices that are owned by the individual employee, but may also be used for work purposes through a bring your own device (BYOD) program.

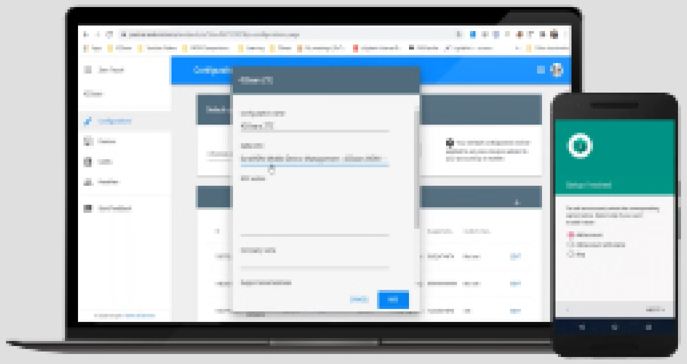
Irrespective of the ownership type, management of Android devices goes through a lifecycle with multiple stages. The first step involved in Android mobile device management is to enroll the devices into an Android MDM solution.

Enrollment Options

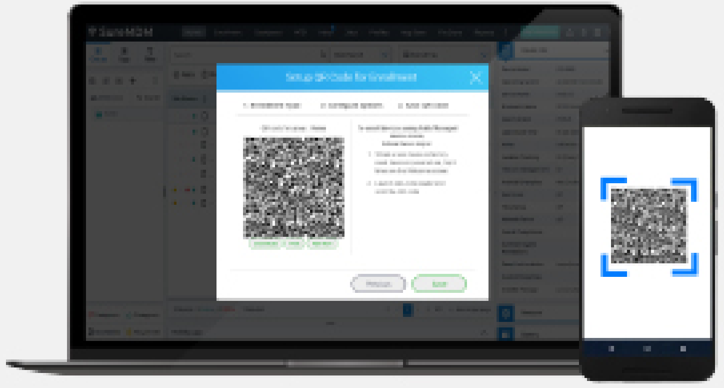
For Android Enterprise enrollment,
you can use either **Google Zero-touch** or **QR Code** based enrollment.

Android Enterprise is the most common and recommended method of enrollment of Android devices and is available for GMS certified devices. GMS Certified devices are Android devices that have been certified by Google to meet certain standards for compatibility and functionality with Google Mobile Services (GMS). GMS is a suite of Google apps and services that are pre-installed on Android devices, such as the Google Play Store, Google Maps, and Gmail. Android Enterprise is not supported on AOSP based devices as they are not GMS certified.

Google Zero-touch



QR code



Additional OEM specific tools such as **Knox Mobile Enrollment (KME)** from Samsung, or **Stage Now** from Zebra are also available which makes enrollment of their specific devices fast and easy.

Encryption

Corporate and personal data security is one of the most important reasons for using an MDM solution. Android natively provides built-in security technologies to protect and secure data residing on the Android devices. Starting with Android 10, Android supports File-based Encryption or FBE, whereby each file is separately encrypted using AES-256 based encryption. Earlier versions of Android supported Full-disk Encryption (FDE) which involves encrypting the entire user data partition with a single primary key.

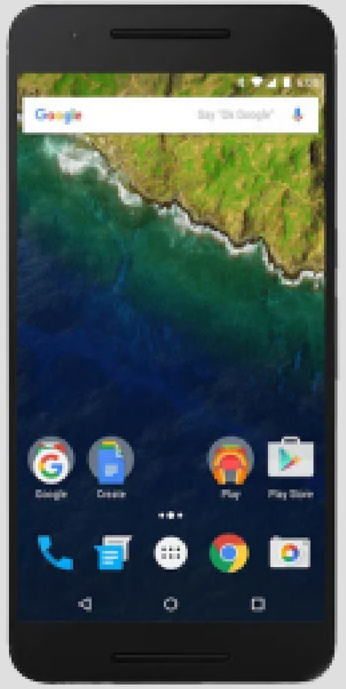
Hardware-backed security mechanisms in Android:

- Verified Boot
- Trusted Execution Environment (TEE)
- Application Sandboxing
- Backup Encryption

Provisioning and Setup

Provisioning is the second step in the Android lifecycle management process. During provisioning, a default profile with various policies and restrictions is applied to the devices. An example of such policies or restrictions would include enforcing strong password requirements, disabling USB Debugging, or Factory Reset by the end-user.

Some device manufacturers also support OEMConfig, which is a powerful mechanism to configure OEM specific features of the device. Once baseline policies and configuration are setup, the devices are handed over to the actual users or employees of the organization.



Strong Password

Disable Factory Reset

Disable USB Debugging

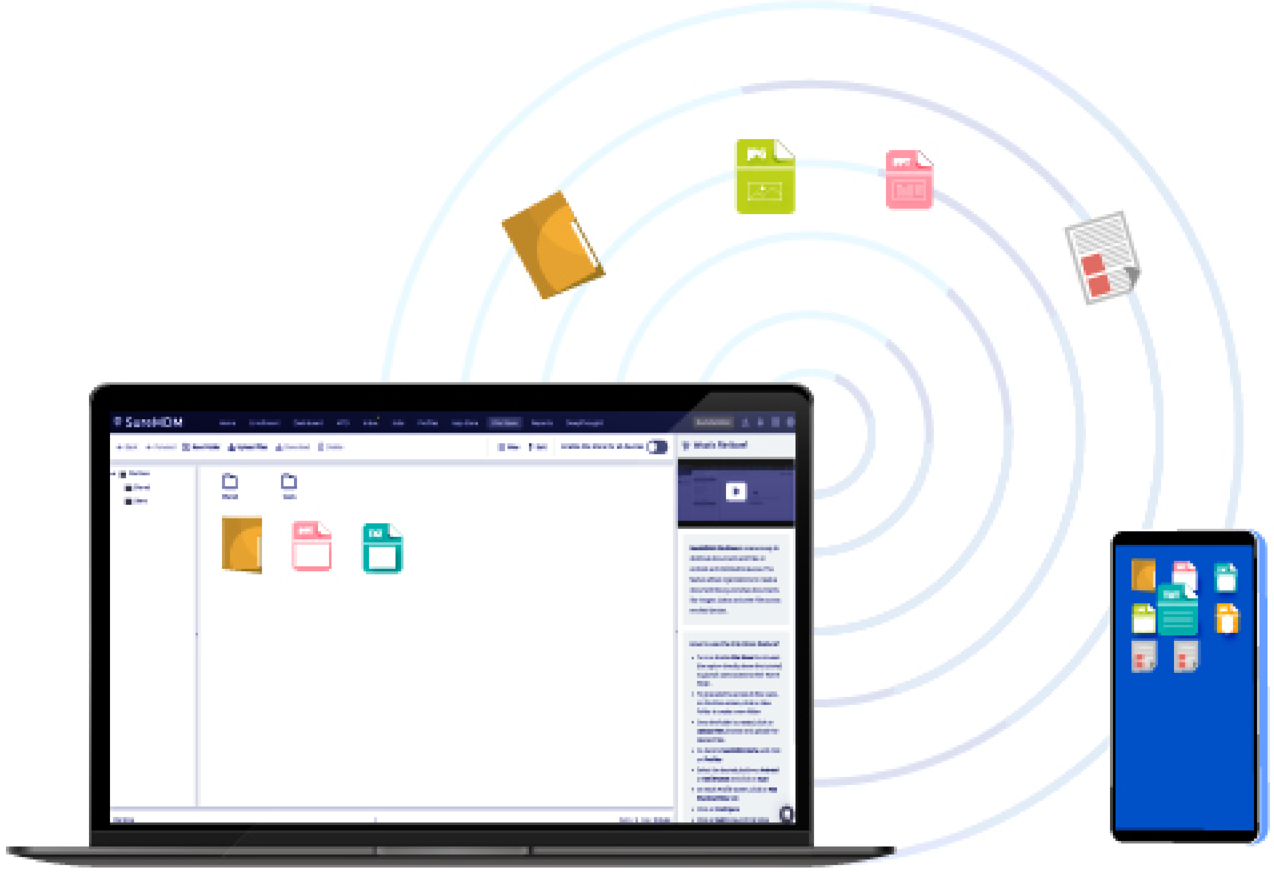
App Distribution

Using MDM, you can deploy play-store or private Android apps on the devices or make them available to the enterprise end-users via Managed Google Play. Granting runtime permissions to those managed apps is also possible, thus avoiding any operational issues in the field where the users may not be tech savvy. You can also configure work related apps remotely from MDM using the Managed App Config feature.

- Application Distribution and Update
- Grant runtime permissions
- Managed App Config

Content Distribution

You can also use the MDM to easily distribute content such as PDF, Excel files or any other kind of data files to your users devices.

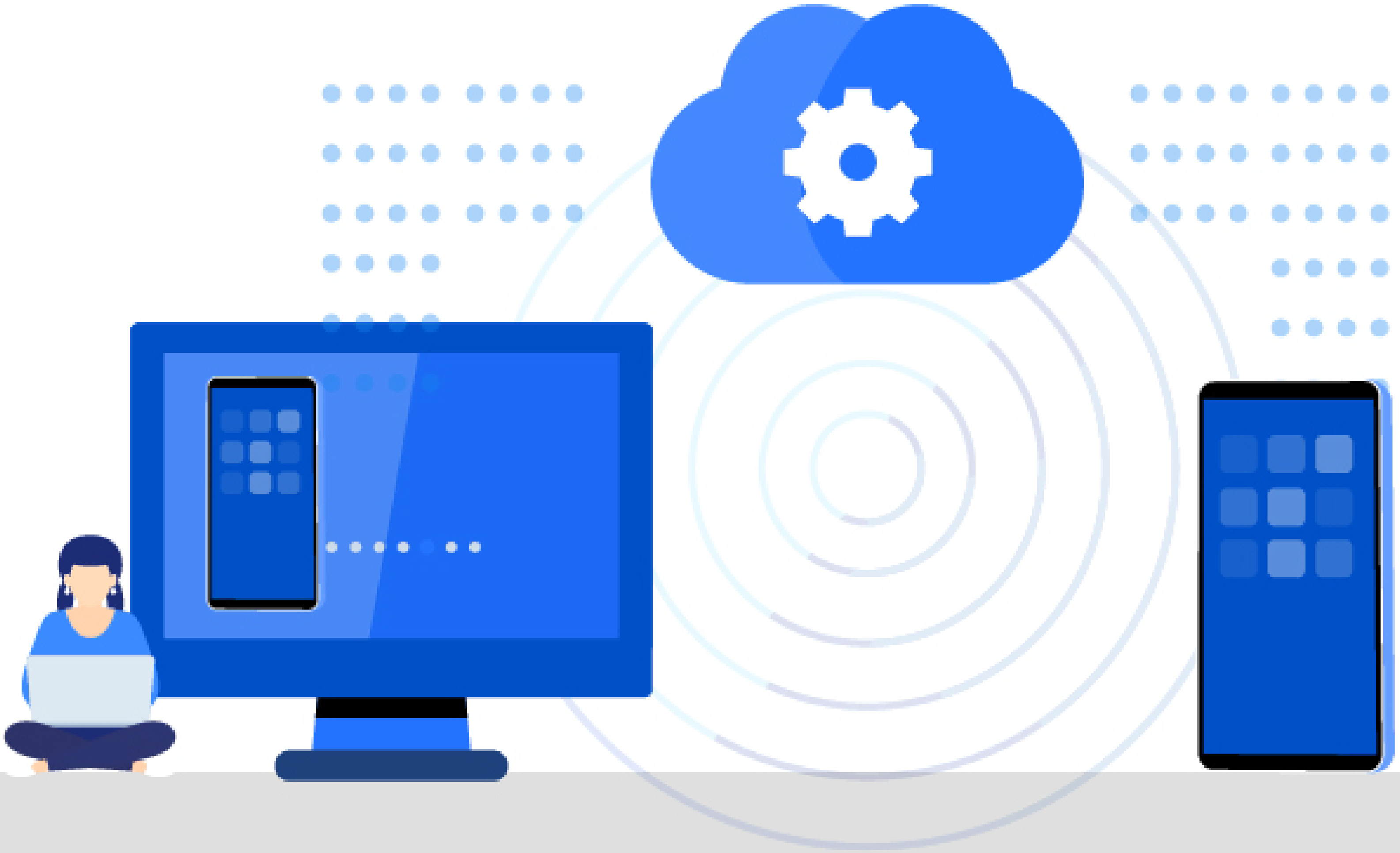


Secure Android Kiosk Mode

For frontline worker scenarios, you can also set up kiosk mode on the devices, and ensure workers can only use approved applications and websites. Properly locking down the devices results in a direct increase in worker productivity. Avoiding worker induced downtime due to improper use of devices, can free up the IT team to do other productive tasks for the organization.

Remote Troubleshooting

Even if the devices are properly provisioned, it is only a matter of time when something fails on the device making it unusable. In most cases, having access to the device can help the IT team troubleshoot the issue. However, if the devices are not physically close, IT needs a way to access the devices remotely. This is where the Remote Control feature of the MDM solution comes in handy. If you are part of the IT team, for troubleshooting issues, you can remote into the far-away devices and interact with them using your computer keyboard and mouse. You can also take screenshots, view files and folders on the device, and view the list of running processes. You can also use remote control to train the end-users right from your office.

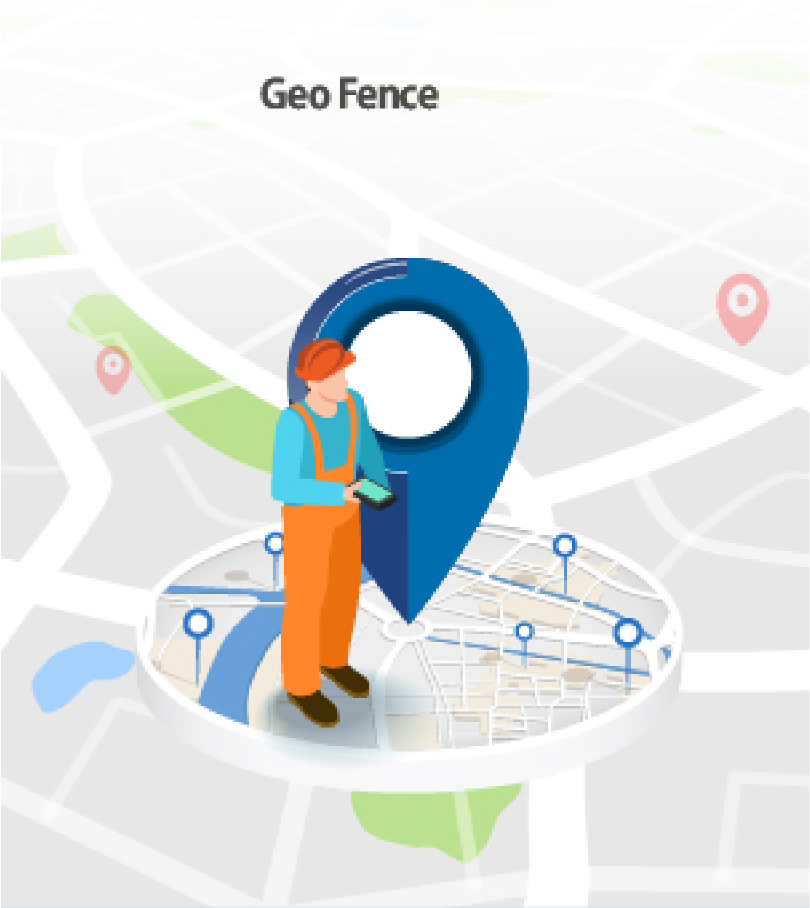


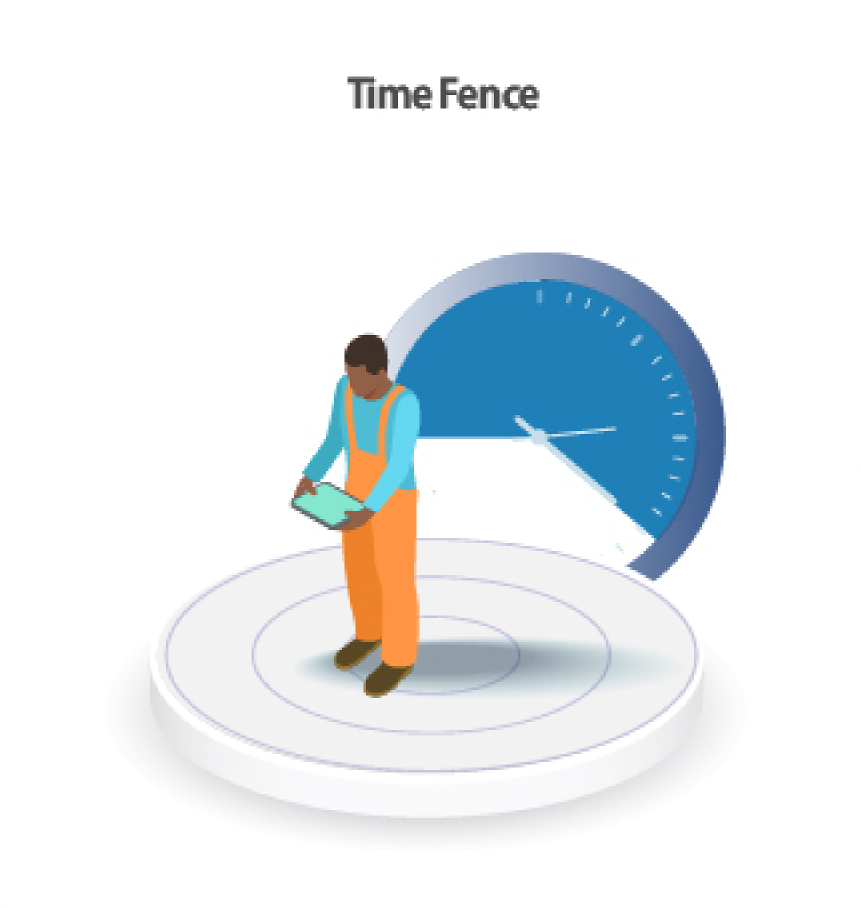
Location Tracking

Tracking the location of Android devices using an MDM solution can help organizations locate lost or stolen devices, monitor employee activity, and ensure compliance with security policies. Ability of the IT team to view the real-time or historical location of the device on the map could be very useful.

Fencing

You can use an MDM to apply location, time, and network fence policies based on a device's location, time of day, and network connectivity. This can help ensure that devices are being used in authorized locations and during authorized times, and can help protect against security threats. For example, an MDM solution might be configured to disable certain apps or features when a device is connected to an unsecured public Wi-Fi network, or to require a passcode when a device is outside of a designated geographic location. Similarity, if a time-based fence is active, a strict lockdown policy gets activated during say work hours, after which the device becomes open or relatively less restrictive allowing users some flexibility. Lastly, with network fencing, a special policy can be activated when the device connects with a known or unknown Wi-Fi network, and accordingly grant or restrict access to the resources.


Geo Fence


Time Fence

Network Fence

Security

Remote Lock and **Remote Wipe** are two important security features provided by mobile device management (MDM) solutions. IT teams use these features to remotely lock a lost or stolen device, preventing unauthorized access, or remotely wipe the device's data, removing sensitive information from the device. This action helps to protect corporate data and prevent data breaches in case of a lost or stolen device, and is an important aspect of corporate mobile device security.

Reports

MDM solutions typically provide a range of reporting capabilities that enable IT professionals to monitor device usage and ensure compliance with security policies. These reporting capabilities may include data on **device inventory, device health and performance, app usage, security events, and compliance status**. This information can be used to identify potential security risks, track device and app usage trends, and generate reports for stakeholders. Advanced reporting capabilities enable organizations to create custom reports, automate report generation, and visualize data with charts and graphs.

We invite you to sign up for a free trial of

SureMDM™

and experience the power of a truly best-in-class Android device management platform. We hope to become part of your digital transformation journey.

Sign up for a free trial of SureMDM

Disclaimer

This document is provided as a reference guide and is intended for informational purposes only. It is not intended to be a substitute for professional advice, and it is not recommended to rely solely on the information contained herein for decision-making. While reasonable efforts have been made to ensure the accuracy and completeness of the information, we do not guarantee its correctness or suitability for any specific purpose.

None of the authors, contributors, directors, employees, or any other related parties associated with 42Gears Mobility Systems Pvt Ltd. accept any liability for the information presented in this document or for the use or reliance upon it by any company or individual.

The trademarks, service marks, logos, and trade names mentioned in this document are the sole and exclusive property of 42Gears. However, please note that this document may contain references to third-party trademarks, logos, and copyrights that belong to their respective owners. The use of these trademarks, logos, and copyrights does not imply any affiliation with or endorsement by the respective owners.

Readers/viewers are granted limited permission to distribute this document freely, without modification, under the condition that the content remains intact and the original attribution to 42Gears Mobility Systems Pvt Ltd. is retained.

By distributing this document, 42Gears Mobility Systems Pvt Ltd. shall be held harmless from any claims, damages, or losses arising from its use or reliance on the information contained herein, and from any damages or losses arising from the use of any third-party content or material.