Scalefusion for Android: Effectively Manage Your Android Device Fleet

Deploy & secure Android endpoints, extend remote management & policy enforcement for Android devices to drive productivity for your business.

Overview

Manage Android devices with Scalefusion MDM and equip your workforce with mobile access to corporate resources. Manage and secure company-owned as well as BYO Android devices.

Benefits

- Android Enterprise Ready
- Effortless device deployment for diverse ownership models
- Out of the Box management experience with Zero Touch
- Extensive policy configuration to iron grip devices
- Enhanced security and DLP control using app containerization
- Remote troubleshooting integrating third-party ITSM tools
- Streamlined management with Workflows and Reports
- Low Total Cost of Ownership

Introduction

Scalefusion MDM drives your company's Android management through a clutter-free dashboard that effectively manages versatile devices. Scalefusion MDM ensures device security and resource delivery to optimize employee productivity. With Scalefusion MDM, IT admins can configure policies, publish apps and business-centric content and secure the devices from a single console.

With Scalefusion MDM and Android Zero Touch, IT admins can deploy Android devices and offer an unmatched unboxing experience to the end-users. Coupled with Interops, Scalefusion MDM establishes dependable, encrypted communication between the device and the admin. With Remote Cast and Control, admins can quickly resolve device issues adding to employee productivity.

On the company-owned devices, IT admins can impose strict policies by restricting browsing access only to whitelisted websites and applications, setting geofences and implementing Workflows to execute recurring tasks without user intervention.

Android Device Management: A Growing Need

Modern workplaces are facilitated with digital devices that are rigorously transforming the operations and productivity of businesses. Mobile devices are enabling employees to extend the efficiency and connectivity irrespective of their location. It is a win-win situation for the organization and its employees; since it's helping to get things done, rapidly. This accelerated growth in the use of mobile devices for work is raising the demand for IT support. The mobile devices need to be managed and secured while being powered with business-specific resources.

Scalefusion MDM extends management to a variety of company-owned devices such as smartphones, tablets, TVs, rugged devices, custom android devices and mPOS without compromising on user experience. Enable employees to use their favorite Android devices for work by publishing business-specific apps and content. Maintain employee-data privacy by compartmentalizing personal and work apps on the device.

Android Device Management with Scalefusion MDM

Android Enterprise Ready

Scalefusion is Android Enterprise ready. Businesses can select, deploy and manage Android devices and services as per the standards set by Google.

Supporting Various Deployment Types

Considering the diverse use-case of every business, Scalefusion extends different deployment types for managing company-owned Android devices.

Agent Mode

Enforce company policies, allow business-centric apps and websites, and customize the device branding aligning with your business. Restrict device operation and configure granular settings to secure the device. Track device location and performance through the dashboard. Uphold device security by configuring network and sharing settings and enforcing passcode policy.

Kiosk Mode

Lock the Android device to run into single or multiple applications. Turn the device into an interactive kiosk or digital signage. Remotely update applications, clear browsing sessions, publish content including images and videos, track battery level and troubleshoot device issues without physically accessing the device.

BYOD Mode

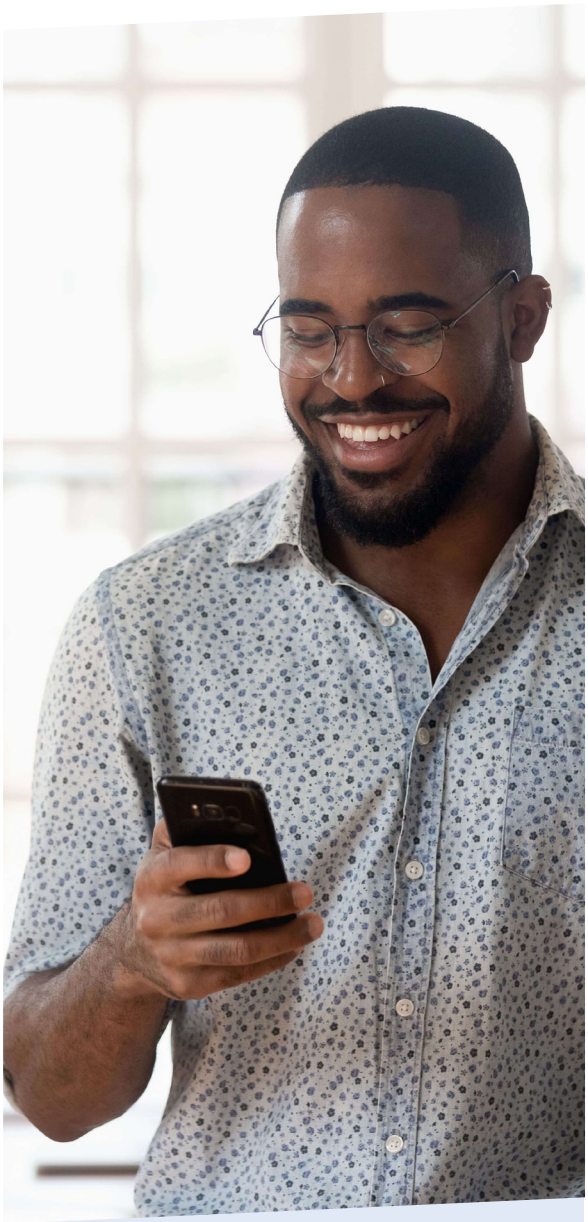
Scalefusion MDM presents effective containerization between business and personal apps on BYO devices. The control of app downloads, sharing and network settings lies with the device owner. Restrict employees to transfer and share data between work and personal apps.

This instills trust among the employees regarding the safety and privacy of their personal data. At the same time, companies can have total control over the corporate data distributed on the BYO devices. If the employee is no longer associated with the company, the company can remotely wipe-off the corporate data and apps from the employee's device without hampering the personal items on the device.

COPE/WPCO Mode

COPE/WPCO management empowers organizations to effectively manage their fleet of Android devices within a corporate environment while allowing employees to use the same device for their personal usage.

With Scalefusion, IT admins can seamlessly control and secure corporate-owned devices while allowing employees to use their devices for personal purposes. This balanced approach enhances productivity, data security, and user satisfaction.



Try it now for free

Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

Request a demonstration and see how Scalefusion can help you in managing your devices and securing your corporate data.

Book a Demo

Device Management Made Easy

Zero-touch Enrollment

The company-owned devices can be deployed with pre-applied policies, manually with Android for Work or using Android Zero touch for over-the-air deployment. The BYO devices can be manually enrolled. The devices can be onboarded using QR code, IMEI-based or serial number-based configuration.Users can also enroll their devices using IdP-based enrollment powered by PingOne, Okta, G Suite or Microsoft Azure AD.

Comprehensive Policy Application

With Scalefusion, IT admins can apply a comprehensive set of policies to devices or device groups. IT admins can customize policies depending on use-cases and configure crucial settings like network and sharing that can impact security. Policy application can be extended to access to apps, websites as well as hardware key configurations. To make device management more effective than ever, IT admins can make use of Device and user grouping capabilities on the Scalefusion dashboard.

Task Scheduling with Workflows

Administrators can schedule recurring tasks to be performed on device inventory and save IT efforts. Using Scalefusion Workflows, IT admins can schedule a profile switch, periodic lock/unlock, reboot for managed devices. Activities like clearing app data and browser cache can also be scheduled at regular intervals. Furthermore, IT admins can schedule compliance checks and alerts for violations, geofence breaches and data usage.

Advanced Reporting

To help monitor devices effectively, IT admins can quickly generate and download reports and audit logs. Reports are available for the following parameters

- Device usage
- Data usage
- App publishing
- Device availability
- Location
- App version
- Device inventory
- Account activity
- Remote cast
- SIM swaps
- Unlock attempts
- Device vitals
- FileDock analytics
- Screen time
- Geofence logs
- Battery history
- Workflows reports
- Connectivity history

Certificate Management

IT admins can authenticate devices and check for security when operating in unknown networks. IT admins can streamline the process of deploying Digital Certificates to end users' devices by automatically provisioning digital identities onto devices without end user interaction. IT administrators can push Identity certificates, CA certificates and Chained certificates on managed devices. IT admins can also push certificates for enterprise Wi-Fi to enable employees to seamless plug and work once in the office network.

Location Tracking and geofencing

IT admins can track device location in real-time and create geofences and get notified every time a device moves in or out of a geofence.

Point of Sale

Interactive Kiosk

Digital Signage

Phone & Tablet

Rugged & Handheld

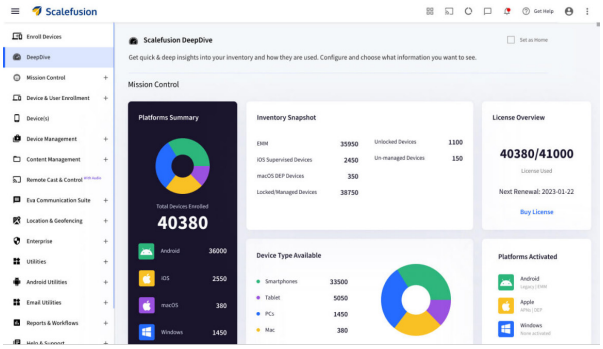
Custom Device

UEM-integrated identity and access management

Bring the power of UEM and IAM to your business to enhance enterprise security and compliance. Simplify user identity and access management with Scalefusion OneIdP. Integrate your existing directory or create your own on the .oneidp domain. Authenticate users and authorize access to enterprise devices, data, and applications seamlessly. Ensure robust identity governance with single sign-on (SSO) to enable your employees to access work apps with a single set of credentials. Efficiently manage user lifecycles and extend access permissions based on device management status. Set access conditions for trusted locations, Wi-Fi networks, and IP addresses and deny access to work apps and devices via unidentified networks and locations.

Unified Dashboard & Device Analytics

Scalefusion MDM comes with an intuitive dashboard that enables IT admins to track, manage and secure multiple devices through a single console. The DeepDive feature in the Scalefusion dashboard helps IT admins to track various device analytics including device battery, device storage, data usage and device location. DeepDive also provides analytics around compliance violations and security incidents like SIM-Swap and wrong passcode attempts on company-owned devices.



Effective Content Management with Scalefusion MDM

Whitelisting Apps and Websites

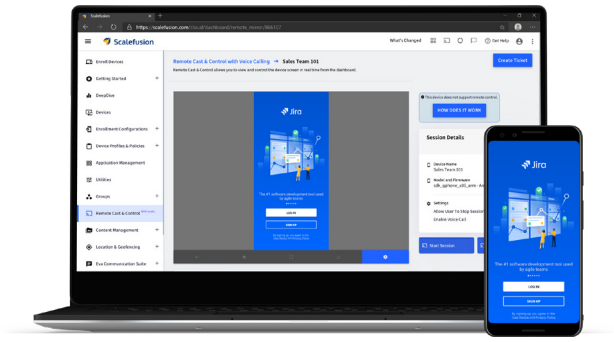
IT Admins can whitelist apps and websites on company-owned devices. Admins can silently install and uninstall Playstore, Play for work as well as enterprise apps on managed devices. Administrators can control browser settings and create shortcuts to whitelisted websites and pin them to the homescreen on managed devices.
To protect Microsoft Office 365 apps on managed Android devices, IT admins can make use of Intune® App Protection or Data Loss Prevention Policies.

IT teams can also push Progressive Web Apps (PWA's) on managed Android devices using Scalefusion.

Content Distribution

Distribute essential company resources on managed devices. Admins can publish content including images, text, audio and videos on company-owned as well as BYO devices through FileDock app by Scalefusion. IT admins can also control folder settings, service analytics for content publishing, create shortcuts to run presentations on demand and leverage touch analytics for screensaver and presentation.

Seamless Remote Troubleshooting



Remote Cast and Control*

Troubleshoot device issues and mitigate device downtime by enabling screen sharing via Remote Cast. On select Android devices, IT admins can take screen control. Remote Control is also available on Zebra Devices. Kill tasks, uninstall applications and navigate through viewable system information remotely. Establish support over voice calls while casting and effectively guide the end-user to solve device issues. Take screenshots and record cast sessions for quick device issue escalation.

Effortless Ticketing

Scalefusion has integrated ticketing services such as Freshservice and JIRA into its dashboard facilitating the ticket creation and ITSM process for managed devices. IT admins can create device tickets along with context-aware device information on Scalefusion Dashboard and it will be reflected on the chosen IT support desk. If your organization uses any other ITSM tool, Scalefusion can extend support to the same using a valid API.

Extensive Security Configurations

Enforce Passcode Policy

Enforce strong passwords policy to secure corporate devices and data. Define the password complexity, minimum password length and the frequency at which passwords should ideally be changed. Configure advanced settings to define the password expiry period, idle time for device auto-lock and maximum failed attempts to factory reset to prevent data leakage and unauthorized system access.

Detect Compliance Violations

Create automated workflows to detect compliance violations such as Geofence breaches and wrong password attempts. Obtain a comprehensive summary of your Android device fleet with DeepDive analytics. Monitor device usage with a range of detailed reports. Schedule reports for a predefined time and frequency to create extensive, automated report repositories for broader compliance checks.

Factory Reset Protection

Activate Factory Reset Protection to secure your sensitive business information from being lost permanently. Authorize specific Google Accounts to sign in to your EMM Android devices that have been factory reset to revive critical corporate data.

Conditional Email Access

Secure your corporate email access, especially in a BYOD environment with Conditional Email Access (CEA) for Exchange Online & IceWarp. Configure CEA with a default global access policy to restrict corporate email access to all devices that are not enrolled with Scalefusion and compliant with enterprise-specific policies.

Summary

Leverage the capabilities of Android devices at work and choose Scalefusion to manage your Enterprise Mobility and escalate your IT productivity. Experience flawless management for every business use-case and deploy Android devices with ease, with Scalefusion.

Try it now for free

Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

Request a demonstration and see how Scalefusion can help you in managing your devices and securing your corporate data.

Book a Demo

About Scalefusion

Ambitious companies around the world trust Scalefusion to secure and manage endpoints including smartphones, tablets, laptops, rugged devices, POS and digital signages. Our mission is to make Device Management simple and effortless along with providing world class customer support.

Enterprise Sales & Partnerships

sales@scalefusion.com

partners@scalefusion.com

Call Us

US: +1-415-650-4500

UK: +44-7520-641664

NZ: +64-9-888-4315

India: +91-74200-76975