Scalefusion

Mobile Device Management for Modern Enterprises

Mobile technology has changed the way modern businesses operate. Learn how Scalefusion bolsters growth with mobility in enterprises.

Overview

Provision, configure & secure mobile phones, tablets, laptops, computers, rugged devices, POS systems & special-purpose devices over diverse operating systems. Administer content & apps on the devices whilst ensuring end-to-end device & data security.

Benefits

- Simplified device enrollment & provisioning
- Cross-platform support to adapt device diversity
- Uncluttered, user-friendly dashboard
- Extensive security for corporate data & device
- Streamlined application & content management
- Unified Communication for effective team collaboration
- Remote troubleshooting to reduce device downtime
- Task automation resulting in reduced IT work

Introduction

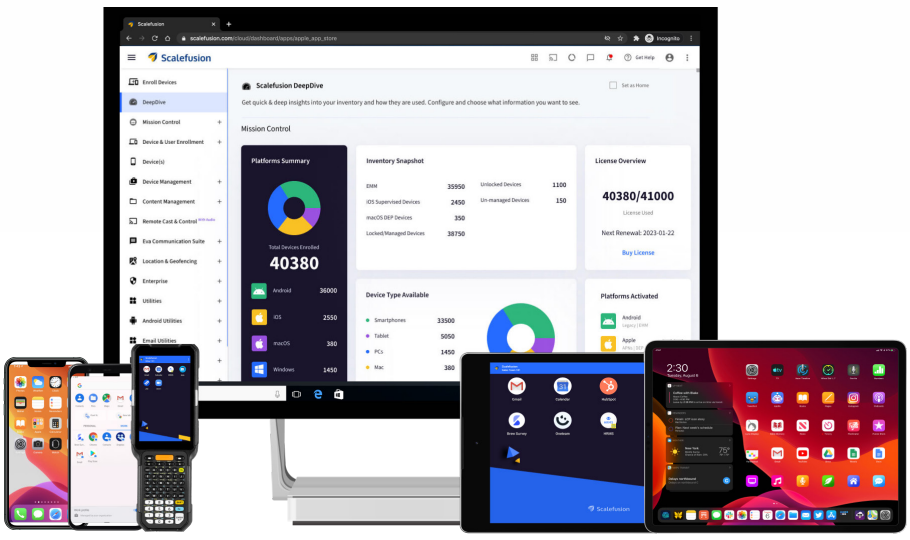
As businesses ascend the digital progression, managing enterprise devices is imperative in order to expedite the desired growth from the mobility pursuit. These mobile devices are rigorously utilized by enterprises and employees. Equipping them with pertinent device policies & business resources is hence, urgent. Enterprises seek out a scalable solution that not only aids in the provisioning of devices to speed-up workforce productivity but also ensures that the IT teams are not encumbered with increased liabilities.

Scalefusion MDM helps enterprises in addressing the growing need of provisioning mobile devices with business resources without burdening the IT teams. This, while ensuring end-to-end device & corporate data security and employee productivity.

Scalefusion Mobile Device Management for Enterprises

1. Cross-platform Solution

In modern enterprises that employ a mix of knowledge workers and frontline workers, there is considerable diversity in the kind of devices preferred by employees or required for the desired business operations. Understanding the need to facilitate this device diversity, Scalefusion MDM supports multiple OS and device types. With Scalefusion, IT admins can manage Android, iOS, macOS, Windows, and Linux devices. Scalefusion extends support for corporate-owned as well as BYO devices.



2. Faster time to market

For enterprises deploying multiple devices, it is crucial to quickly provision and enroll devices in bulk to ensure that the IT teams are not burdened with individually equipping each device with corporate policies and apps. For faster over the air deployment, Scalefusion offers support for:

- Android Zero-touch for Android devices
- Apple Business Manager and School Manager for iOS and macOS devices
- Samsung KME for Samsung Knox devices
- Windows Autopilot for Windows 10 devices

3. Simple, user-friendly dashboard

Scalefusion simplifies device inventory management with a non-arduous dashboard. The Scalefusion dashboard is highly scalable and can be used to manage any number of devices with ease. The Scalefusion dashboard presents exclusive device analytics for battery, data, storage usage, security incidents & platform details. Further, IT teams can automate recurring IT tasks, schedule alerts & compliance checks and generate reports for improved device inventory management.

3. 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.

4. Extensive Security Configurations

Data loss prevention (DLP) on managed devices is ensured with Scalefusion. IT admins can:

- Enforce passcodes & passcode policies
- Prevent factory resets
- Detect failed passcode attempts & SIM swaps
- Disable device boot in safe mode
- Disable hardware keys
- Ensure secure browsing in a controlled environment
- Remotely lock/wipe-off device data

Try it now for free

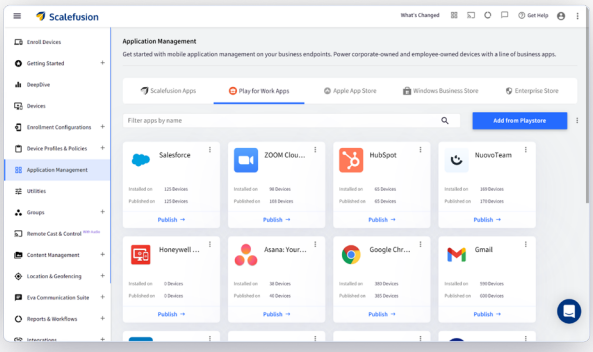
Register for a free 14-day evaluation at **www.scalefusion.com**

Get a Demo

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

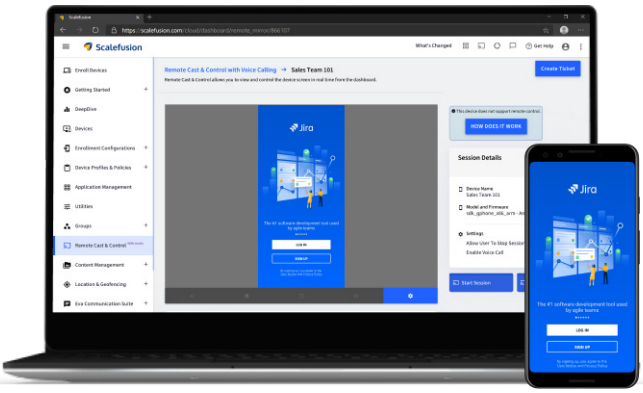
Book a Demo

5. Application & Content Management



Scalefusion MDM offers expansive content and app management where IT admins can curate the content made available on the managed device fleet. IT admins can publish, delete, and configure public as well as private apps, push business content files on devices; and remotely update them. IT teams can also allow or block certain websites and exert parental control over content accessed on managed devices.
Using Scalefusion, IT teams can publish:

- Play for Work apps on Afw devices
- Apps on iOS and macOS devices using Apple Volume Purchase Program (VPP)
- Private apps on Android, iOS, Windows, macOS, and Linux devices



6. Remote troubleshooting

To reduce device downtime on managed devices, IT admins can make use of the Remote Cast & Control feature of Scalefusion. IT teams can mirror the device screen, connect to the end-user over a VoIP call to quickly resolve issues, or sync files. To support ITSM, IT teams can take screenshots or screen recordings and create context-aware support tickets directly from the remote session.On Android and Windows devices, IT admins can also initiate Unattended Remote Cast & Control sessions.

7. Patch Management

To ensure the security of their managed Windows devices and protect them from vulnerabilities arising from outdated software, IT admins can manage software, driver, and third party application updates directly from the Scalefusion Dashboard.

Device & User Enrollment

- IMEI based/Serial Number Based enrollment
- Bulk Enrollment using QR Code / Config URL
- License Key Enrollment
- Configuration file-based Enrollment
- ROM-based enrollment
- Android for Work Setup
- Android Zero Touch Enrollment
- Apple Business Manager (APNs and DEP)
- Samsung KME
- Windows AutoPilot-based enrollment
- Microsoft Azure AD-based enrollment
- Active Directory-based enrollment
- Bulk Enrollment using Email Invite (only for BYOD)
- Work Profile Containerization (BYOD)
- User Management (Add and manage users)
- Create User Groups and subgroups

Device Management

- Kiosk mode
- Single app mode
- Multi-App Mode
- Agent Mode
- BYOD support
- Supervised & Unsupervised support for Apple devices
- Create custom branding
- Change home screen & lock screen wallpaper
- Create Device Profiles
- Create Device Groups and subgroups
- View registered devices with multiple filters
- Custom Payload
- LDAP Payload
- Usage Curfews
- Control/Defer Software Updates
- Deploy Powershell Scripts

Location Tracking

- Real-time GPS-based location tracking
- IP address-based location tracking
- Apply Geofences
- Multiple geofences
- Geofence-based switch profile
- Speed-based app locking

Content Management & Filtering

- Remotely push files and folders
- Digital signage kiosk
- Push content as screensaver
- Whitelist websites
- Multiple browser setting options

Note: Availability of certain features and functionality might vary based on operating system and device type.

Application Management

Silent App Installation
App distribution and management for App Store Apps, Play Store Apps, Windows Business Store Apps
Private App Distribution using Scalefusion Enterprise Store
App Configuration
Remotely remove/uninstall/block unused Apps
Google play integration
Apple App store integration
Windows Business Store integration
Support for Apple VPP- Volume Purchase Program
Office 365-based App Protection Policies

Utilities

Broadcast message
Lock/unlock devices
Buzz devices
Wi-Fi configuration
Find duplicate devices
Nudge inactive devices
Clear Browser Cache
Developer API
Configure Exchange ActiveSync Settings

Utilities

Configure & Manage Email Settings
App Notification setting
Lock Screen
Capture IP Address
Password protect safe mode
Internet connectivity indicator
Show OS upgrade menu option
Access root privileges (only for rooted devices)
Auto Publish Whitelist Websites
Hotspot setting
Timezone setting
Clear SD card files
Clear App data
Copy data from one device to other
Factory reset protection (for AFW devices)
Remote Mirroring
Data usage Report
Compliance Validation using SafetyNet Attestation
Detection and Compliance for Rooted Devices
Compliance Violation Action
Offline data sync and manage
Remote Alarm
Custom secured browser
File Sync

Note: Availability of certain features and functionality might vary based on operating system and device type.

Utilities

APN Settings
Active Directory Settings
Conditional Email Access for BYOD

Security & Compliance

Certificate Management
VPN Configuration
Passcode Policy
Minimum Passcode Length
Passcode Complexity
Passcode Validity
Passcode History
Passcode Failed attempts
Passcode Compliance Checks
Windows Information Protection
Windows Defender Policies
BitLocker
Windows Hello Authentication
File Vault Support
Firewall
Stealth Mode
Gatekeeper settings
Remote Enterprise Data Wipe

Security & Compliance

Allow/ Block use of Camera
Allow/ Block Screenshots
Allow/ Block Keyguard Trust Agent state
Allow/ Block fingerprint for unlock
Allow/ Block notification in lock screen
Allow/ Block adding of Google accounts
Allow/ Block adding of email accounts
Allow/ Block installation from unknown sources
Allow/ Block installing apps
Allow/ Block uninstalling apps
Allow/ Block clipboard between managed and unmanaged apps
Allow/ Block work apps to open documents from personal apps
Allow/ Block Personal apps to open documents from work apps
Allow/ Block Personal apps to share documents from work apps
Allow/ Block work apps to share documents from personal apps
Allow/ Block work contacts caller id info to show in Dialer
Allow/ Block apps widgets to be added to Home Screen

Note: Availability of certain features and functionality might vary based on operating system and device type.

Security & Compliance
Allow/Block sharing Enterprise contact with Bluetooth Devices
Allow/ Block work contacts in personal contacts app
Allow/Block use of Siri and Dictation
Allow/Block Apple Music
Allow/Block Touch ID to unlock device
Allow/Block password sharing
Allow/Block password Autofill
Allow/Block iCloud Drive and sharing
Allow/Block Airdrop
Allow/Block Mail
Allow/Block Messages
Allow/Block Reminders
Configure media sharing
Allow/Block/Read-Only Disk Images
Allow/Block/Read-Only DVD-RAM, CDs and CD-ROMS, recordable disks
Allow/Block Eject at logout
Allow/Block iTunes File Sharing
Allow/Block use of Game Center
Allow/Block Mouse
Allow/Block Accessibility
Allow/Block Parental Controls
Allow/Block Bluetooth

Security & Compliance
Allow/Block Printer & Scanner
Allow/Block Extensions
Allow/Block Fibre Channel
Allow/Block Startup Disk
Allow/Block iCloud
Allow/Block Time Machine
Allow/Block Ink
Allow/Block Internet Accounts
Allow/Block Trackpad
Allow/Block Keyboard
Allow/Block Wallet & Apple Pay
Allow/Block Language & Text
Allow/Block Xsan
Allow/Block Microsoft Feedback Notification
Allow/Block USB connections and Storage Card
Allow/Block Telemetry
Allow/Block Cortana
Allow/Block Microsoft account connection
Allow/Block Add non Microsoft Accounts
Allow/Block Sync Settings across Devices

Note: Availability of certain features and functionality might vary based on operating system and device type.

Audit, Dashboard & Reporting

- Audit Logs
- Detailed reporting
- DeepDive Dashboard

Reports

- Data usage Report
- Location Report
- Application Version Report
- Account Activity
- Remote Mirror
- Sim Swaps
- Unlock Attempts
- Device Vitals
- File Dock Analytics
- Device Availability
- Screen Time (App Analytics)
- Geo Fence Logs
- Battery History
- Workflow Reports

Workflows

- Schedule Profile Switch
- Schedule Geofence Based Profile Switch
- Publish Apps
- Schedule Lock/Unlock
- Schedule Reboot
- Schedule Clear App Data (9.0 and above)
- Schedule Clear Browser Cache
- Switch Presentation
- Battery Compliance
- Geo-Fence Compliance
- Data Usage Compliance
- Inactivity Compliance Alert
- Security Incidents Compliance
- Schedule Broadcast Messages
- Storage Compliance Alert
- Schedule Device Details Report

Remote Troubleshooting

- Remote Cast
- Remote Control
- VoIP calling
- File Sync

Note: Availability of certain features and functionality might vary based on operating system and device type.

Remote Troubleshooting
Screenshots and screen recordings
Context-aware ticketing on integrated ITSM platforms

Integrations
ITSM Integration -JIRA
ITSM Integration -FreshService

Note: Availability of certain features and functionality might vary based on operating system and device type.

Summary

Expedite business growth by leveraging the versatile capabilities of Scalefusion MDM and make the most of your mobility. Augment workforce productivity & corporate data security while enabling simplified device management for your IT teams.

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

(INDIA) +91-74200-76975