SureMDM for Windows

The Challenge: Managing Windows Devices

Windows has been the enterprise platform of choice in workplaces worldwide for decades. Strong support by software developers helps Windows stay useful in many use cases and form factors, including business computers, laptops, kiosks, POS devices, and many more. This introduces a huge challenge for IT teams tasked with remotely managing and maintaining this wide range of Windows-based devices.

The Solution: 42Gears SureMDM

SureMDM is a leading Mobile Device Management solution used by over 10,000 companies worldwide to manage their device fleets. Deploy, manage, and secure mobile applications and content; keep devices secure; and remotely monitor and repair any device from an easy-to-use central console.

Gartner®

"42Gears named as a Visionary in the Gartner Magic Quadrant for UEM Tools 2018 and 2019"

Key Features:

- Multiple Easy Enrollment Methods
- Easy Mass Provisioning
- Centralized Management Console
- Device Management
- Remote Troubleshooting
- Application Management
- Content Management
- Identity Provider Integration Service
- Plugin Support
- Powerful Analytics and Custom Reports
- Data Visualization
- Advanced Security

Key Benefits:

- Increase employee productivity
- Reduce device TCO (Total Cost of Ownership) with improved preventative maintenance and easier issue resolution
- Protect corporate data

Supported Devices:

- Devices running Windows 7 or later*

  * Some functionality may be restricted on devices that do not run Windows 10

Certifications and Compliances:

- ISO/IEC 27001:2013
  - Certified Information Security Management System
- GDPR Compliant

Device Enrollment

Easily add new Windows devices to your enterprise with Windows AutoPilot

Mobile Device Management

Remotely manage and secure your device fleet

- Set up devices with approved apps and settings and provision with Wi-Fi, e-mail or VPN
- Create role-based user permissions and restrictions
- Configure and apply OEMConfig policies
- Troubleshoot devices remotely with Remote Control functionality
- Track devices on a map in real-time
- Create and auto-apply policies based on location (geofencing) and time (time-fencing)
- Frequent device check-ins (3-hour intervals by default)
- Set up battery and connectivity alert notifications
- Track data consumption per-device and restrict data usage as needed
- Remotely lock, reboot or wipe devices
- Set up and apply password policies
- Historical data tracking
- Remotely execute custom script commands

Centralized Management Console

Manage all devices from a single web console

- Group or tag devices for easy classification and filtering
- Two-way communication: send and receive messages between console and any device
- Data visualization
- Advanced analytics
- Custom reports on-demand or scheduled
- Intuitive dashboard interface
- Custom columns
- Brand the console with company insignia
- Augment console functionality with support for plugins

Mobile Application Management

Deploy, manage, and secure apps on devices

- Remotely push and update applications on devices
- Update and deploy Windows Store Apps
- Deploy e-mail configurations
- Configure or apply AppConfig policies
- Silently install and update apps
- Push over-the-air OS updates to devices
- Manage software assets, view installed applications and versions

Mobile Content Management

Securely deliver data and keep it safe on devices

- Push content to devices remotely
- Set up File Store - Allows users to download files on-demand
- Secure content on mobile devices using containerization
- Wipe or delete data from non-compliant devices

BYOD for Windows

Facilitate BYOD policies

- System settings configuration
- Set application policies
- Containerization
- Network configuration
- Certificates
- Configure enterprise e-mail
- Configure enterprise Wi-Fi settings
- Mobile threat detection
- Data loss prevention

Mobile Identity Management

Integrate with your in-house Identity Provider to enable hassle-free and secure authentication of mobile devices

- Integrate with 3rd-party Single Sign-On providers: ADFS, Azure AD, Okta, Onelogin, GSuite, PingOne and more
- Remotely push identity certificates to devices and manage a list of installed certificates
- Self-service portal for admins to locate, lock or wipe their devices and view device health
- Enroll device using Active Directory authentication
- Transfer system and device activity logs into Splunk, an SIEM (Security and Information Event Management) system

Developer Support

Integrate SureMDM functionality into your own applications and more

- REST APIs
- Plugin development framework

Kiosk Lockdown

Ensure Windows kiosks and digital signage are secured and used as intended

- Allow access to only approved applications
- Enable single-application Kiosk Mode on Windows devices

Secure Web Browser

Enable secure browsing on kiosks and company devices

- Restrict website access to only pre-approved websites

About 42Gears

42Gears is a leading **Unified Endpoint Management** solution provider, offering Software as a Service (SaaS) and on-premise solutions to secure, monitor and manage all business endpoints, such as tablets, phones, rugged devices, desktops, POS terminals and wearables. 42Gears products support company-owned as well as employee-owned devices across many platforms, including Android, iOS, iPadOS, Windows, macOS, Wear OS and Linux platforms. Over 10,000 customers in more than 115 countries use 42Gears products in many industries, including healthcare, manufacturing, logistics, education, and retail.

To learn more about **SureMDM**, or to sign up for a free trial, please visit **www.42gears.com**.

For pricing questions, please contact our Sales Team at **sales@42gears.com**.