MOBILE DEVICE MANAGEMENT

Manage and secure mobile devices, apps and data from a unified console
Empower your business workforce with mobility without compromising on corporate security.

**Mobile Management**
Access, identify, and maintain mobile device information and configurations

**App Management**
Track the deployment and lifecycle of apps

**Incident Management**
Find rogue devices or security risks to patch and secure against cyber threats

**Security Management**
Enforce stringent security policies

**Device Security**
Configure, secure, and manage corporate or BYOD mobile devices

**Data Security**
Prevent data loss and protect corporate data to ensure regulation compliance
**Support Platforms**

- Apple
- Android
- Windows
- Chrome OS

**Full Control for Business Mobility**

**Enroll devices and authenticate fast**
Quickly enrollment and authentication for BYOD, mobile and corporate devices.

**Ensure policies applied to devices**
Configure profiles to enforce security for WiFi, VPN, certifications and parameters.

**Intuitive Centralized Dashboard**
Manage a simpler overview on your network ecosystem over your organization.

**Troubleshoot devices remotely**
Remotely control and view mobile devices to troubleshoot issues faced.
MOBILE DEVICE MANAGEMENT

FEATURE CAPABILITIES

Set Device, User, Security Policies
Apply your devices, users, security policies and 3rd party applications manually or automatically through one consolidated list.

Detect Non-Compliant Devices
Each profile lets you specify a device’s network access rights, overall security policy, antivirus scan schedule settings.

Remotely Wipe Device Data
Update your devices, OS, and 3rd party applications manually or automatically through one consolidated list.

Network Management
Set one time passwords or Active Directory or LDAP. Classify employee (BYOD) and corporate owned devices on your network.

Cloud-Based Architecture
Our lightweight agent to collect information and drill down into incidents with base-event-level granularity.

Streamline Mobile IT Operations
View in real-time deployment information of your mobile device management operations and compliance.

Secure Access Network
Set Android™ Configuration: mail, passcode, restrictions, Antivirus settings, VPN, and Wi-Fi (Samsung SAFE™ supported).

Run and Distribute Approved Apps
Administrators can view all devices in real-time to proactively manage all security policies, applications and rights.

Maintain Data Integrity Profiles
Enforce encryption, security policies, applications, and predefined actions to ensure devices and data security.
Headquartered in Bloomfield, NJ, Comodo's mission is to help customers avoid breaches with groundbreaking isolation technology that fully neutralizes ransomware, zero-day malware, and cyber-attacks that other security providers can’t do. We deliver active breach prevention with patented auto containment technology. Our Unified Endpoint integrates this technology with critical components like our highly rated advanced endpoint protection, endpoint detection and response, and endpoint management to offer a single cloud-accessible Active Breach Protection solution. Comodo's SOC as a Service team makes the solution a frictionless, high-security implementation.

For more information, visit https://www.comodo.com/.