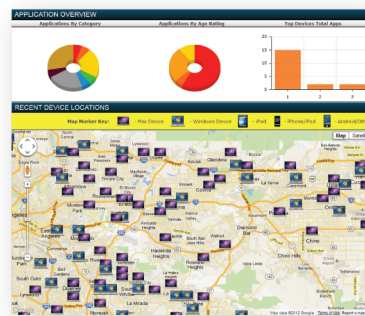# iboss™

MobileEther Mobile Device Management (MDM)

FEATURES

- Central cloud-based management
- Filter access while receiving directory user name
- Provide group based access tied to your directory
- No manual proxy configurations for filtering
- Allows teachers to push apps
- Tracks installed apps, including apps by age rating
- Inventory management for devices
- Inventory management for Apple VPP purchases
- Dynamic device-location-based maps
- Manages device and app access
- Filters Apple App store access
- Centrally push apps by group membership
- Remotely wipes devices
- Time- and location-based policies
- Wi-Fi management
- Apple VPP integration with purchase inventory tools
- Integration with iboss Security Filters for AUP enforcement
- Device tampering detection and alerting
- Student Information System integration with goLive! campus
- iOS including Snow Leopard Support Detects unauthorized apps

Education-focused mobile device management:

Manage compliance, save time, and expand learning

The mobile devices used in today's education system streamline communication and expand learning among teachers, staff, and students. With the expansion of mobile devices in schools, the demand for central management is growing, too, addressing the need to manage policies, track inventory, filter what apps can be installed, and ensure teachers and staff have access to the devices' full potential.

MobileEther Mobile Device Management provides education-specific tools to not only secure the devices but also expand learning. Utilizing the iboss goLive! campus feature along with integration with iTunes University, iboss MDM creates a robust learning environment that goes beyond standard device management. Advanced features, allowing teachers to push apps to students, guarantee that teachers have access to the content they need to foster and support uninterrupted learning.

Easily Enroll Devices With just Three Steps

iboss MDM Advantages:

Manage device locations: Visually identify where devices are physically located.

User based filtering: Filter devices with directory user name and group policy.

Share devices: Shared devices such as in labs and dynamically flip policy based on directory user.

User name based reporting: Dont settle for generic reports. Receive reports with directory user information.

Allow teachers to push apps: Ensure instruction continues uninterrupted.

Simple policy management: Enables group-based policies structures.

Directory Integration: Offers local directory authentication without on-premise hardware.

Manage device settings: Centrally update device settings such as camera, wifi by group.

Inventory VPP Purchases: Manages Apple volume purchase (VPP) inventory, reducing time and money.

Restrict Access to Apps Store: Ensures only apps aligned with the AUP are accessed.

Streamlined Setup: SaaS cloud-based solution, requiring no hardware or set up devices either on or off premise.

Time and Money are Factors

To help you avoid the complications of setting up servers or spending days configuring devices, iboss MDM was designed with education in mind. It provides a cloud-based system that does not require any hardware onsite. Additionally, its simple 2-set setup allows configuration of devices even if they are not onsite. Remote devices are identified and automatically redirected for installation, which means a quick setup and minimal cost investment for you.

Uninterrupted Instruction

Ensuring fluid instruction minimizes distractions and frustration in the classroom. To achieve this, teachers can be provided tools to manage apps they find of value for their students without having to wait for approval. In addition, collaboration with goLive! Campus and the integration of iTunes University with iboss MDM provides tools to share resources, discussion, videos and other learning material right in the classroom, uninterrupted.

More Inventory, Less Time

It's a reality — in today's education systems, the growth of education technology and the shear number of devices and programs being used has expanded opportunities in education; but the staffing that's supporting educational technology has become restricted due to budget constraints. Devices such as iPads not only introduce a need to manage physical device inventory but also software such as apps purchased for the district devices through the Apple Volume Purchasing Program (VPP). Going beyond physical device inventory, iboss MDM manages apps purchased through VPP, ensuring each license utilized. Licenses on lost or damaged devices can be identified, minimizing cost and reducing waste.

Reports Take Center Stage

A key factor in managing devices and apps is identifying where they are and what's on them. Expanding general MDM reporting, iboss MDM focuses on the information you need to quickly resolve threats or compromised devices. Advanced reporting includes Dynamic Geomapping Devices to identify where each device is currently and physically located over a live map and track lost/stolen devices quickly. Global app dashboard provides instant information on how many apps are installed on devices, apps by category, apps by age rating, and VPP purchased licensing. This ensures any unauthorized apps are quickly identified while also managing physical and software inventory. Reports designed to identify the information you need when you need it.

Great (and Not so Great!) Apps

Simple access to apps for education, instruction and productivity is essential. Unfortunately, this also opens general access to the app stores' undesired apps. Managing what apps can be accessed is critical for smooth deployments as well as maintaining compliance with the AUP and CIPA. iboss MDM allows administrators to filter what apps are accessible and those restricted by group membership, providing security without compromise.

CIPA Compliance, on or off Premise

Seamless integration with iboss SWG Filters creates central-Internet-access policy management and reporting whether devices are on- or off-premise. Information on all Internet traffic, including violations to the AUP, are logged and managed through the iboss SWG filter, providing detailed reporting for auditing, compliance and threat detection. iboss MDM integrates into the full suite of iboss SWG products securing networks on or off premise.

Entertainment 12+
17+
4+ **Education**
Games 9+

iboss MDM manages access to the app store by category, age rating, etc. Increasing flexability when managing apps to all devices.

The iboss Suite

Choose an All-in-one solution, or customize it to your networks needs.

- iboss SWG Web Filter
- iboss SWG IPS/IDS/Threat
- iboss SWG Firewall
- Mobile Security
- Mobile Device Management
- Email Spam Boss
- Email Archiver
- Activity & Threat Reporter
- iboss Pro

About iboss Security, a division of Phantom Technologies Inc.

Founded in 2003, Phantom Technologies, Inc is a global provider of network security solutions. Its iboss Security line provides educational focused solutions for network security. Proprietary engineering secures high demand network for web content management, intrusion, mobile device security and management, and email security.

To learn more about our services:
 www.iboss.com

Main: 1-877-426-7701 ext.1
Support: 1-877-426-7701

iboss Security is recognized by Gartner, the world's leading information technology research and advisory company. In addition to Gartner, iboss has received numerous awards related to web filtering and internet security.

Gartner®

OVERALL RATING	★★★★★
Features	★★★★★
Ease of us	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

Security and Reporting

Security and information is also key to ensuring proper management and CIPA compliance for these devices. Advanced reporting tools create a one-of-a-kind live-threat panel to provide detailed insight on device locations over a live, global map. Drill-down reporting provides information on installed apps by age rating, inventory, and users.

Cloud Based Interface

iOS

Take MDM for a test drive yourself!
Schedule an iboss demonstration today.

www.iboss.com