

# Mobile Device Management

**Gurumobility offers the only solution that provides unified management of mobile devices, Macs, PCs, and the entire network from a centralized dashboard. Enforce device security policies, deploy software and apps, and perform remote, live troubleshooting on thousands of managed devices.**

## UNIFIED MULTI-PLATFORM DEVICE MANAGEMENT

- Gurumobility provides over-the-air centralized management, diagnostics, and monitoring for the mobile devices managed by your organization — from iPads and Androids to Macs and PCs. Systems Manager monitors each of your organization's devices, showing useful metrics such as client hardware/software information and recent location, and even lets administrators remotely lock and erase devices.

## ROBUST SECURITY POLICY ENFORCEMENT

- Enforce policies across mobile devices administered by your organization. Protect devices and their data, control their usage with fine-grained passcode policies, and restrict access to the app store, gaming, and content.

## SCALABLE ENDPOINT CONFIGURATION

- Gurumobility also makes it easy to define and deploy network settings like wireless connectivity, security settings, and remote VPN access to

all devices on your network at once. Instead of manually provisioning devices for network connectivity, or relying on end users to do so, configure settings such as WPA2-Enterprise in the dashboard, and let the cloud push the settings to end-user devices.

## ON-DEVICE CONTENT MANAGEMENT

- Gurumobility lets you deliver and manage documents, images, apps, and other files on Android devices. Bundle documents and files into a backpack and deliver it over-the-air to one device or thousands of devices, right from the dashboard. Built-in file synchronization keeps the content on the device up-to-date with the latest version of the file in the administrator's backpack. Prepare separate backpacks to be delivered to different classrooms, departments, or groups. Use tags to selectively deliver content to the appropriate devices.

## SECURE SUPPORT FOR BYOD INITIATIVES

- While user-owned devices have exploded onto networks everywhere, it's imperative to keep network access secure without causing an undue IT burden. Improve the security of BYOD initiatives by enforcing data encryption, remotely wiping lost devices, and even restricting network access to managed devices. gurumobility has built-in support for BYOD, making it easy to securely support BYOD — without extra appliances, licenses, or complex configuration.

## AUTOMATIC DEVICE CLASSIFICATION

- Layer 7 client fingerprinting

technology integrated into gurumobility lets you see all the devices on your network, with no configuration required. Client devices are automatically identified and classified, letting you distinguish between mobile devices, desktop PCs, see device operating systems, and even see device hardware manufacturers.

## AUTOMATICALLY APPLY NETWORK POLICIES BY DEVICE TYPE

- Device-specific policies can be automatically applied by gurumobility wireless APs to restrict, quarantine, or throttle user-owned devices.
- Gurumobility client fingerprinting technology immediately recognizes iOS, Android, Windows, and Mac devices, and even lets you apply more restrictive policies for unknown devices.

## AUTOMATICALLY APPLY NETWORK POLICIES BY DEVICE TYPE

- See how many BYOD clients have connected, measure the bandwidth they've used, and even see their percentage of total traffic.
- Network summary reports are delivered to your inbox at any time or on an automatic, monthly schedule.
- iOS, Android, Windows, and Mac devices, and even lets you apply more restrictive policies for unknown devices.