

# Ivanti Mobility Manager

Personal mobile devices enter your organization virtually every day—and that’s a good thing. The productivity gains that workers can achieve through anytime, anywhere access accelerate decision-making and response to business activities. Ivanti Mobility Manager lets you embrace mobility with the confidence that security measures are available to protect corporate information consistently across endpoints.



## Manage BYOD Alongside Corporate-owned Endpoints

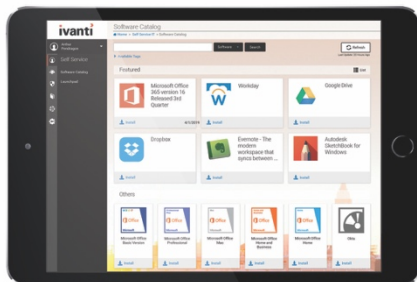
Corporate-managed devices are expected to have Enterprise Mobility Management features such as device enrollment, policy deployment, and remote device locking. Make your BYOD policies more successful by striking a balance with users of personal devices. Safeguard corporate information without invading the user’s personal mobile device space.

## True Unified Endpoint Management

Ivanti Mobility Manager is integrated within Ivanti Endpoint Manager, so IT teams can use a single system to manage all the devices users carry. Uniform delivery of policies is made easy and one-touch employee onboarding becomes a reality. You can administer policies once and propagate them across all the user’s devices, ensuring consistent security for IT teams and uniform user access across devices.

## Provide a Common Experience Across Devices

Role-based Workspaces provide users a secure place to access needed applications and corporate information. Your IT team can deliver a corporate app store experience, enabling mobile users to launch applications and stream access to corporate data—all through an interface and navigation experience that is consistent from the desktop to the tablet and smartphone.



## Scalable App Deployment and Enrollment

The capabilities found in Ivanti Mobility Manager scale with your business. No longer is individual application licensing required for every Apple-device user in your organization. Support for Apple’s Volume Purchase Program makes it easy for IT teams to procure and distribute instances of AppStore applications.

Even enrollment of devices is easy, with support for Apple’s Device Enrollment Program (DEP). Best of all, both VPP and DEP can be used across Mac OS and iOS devices.

## Mobile Application Management

Push applications to users’ devices and control access to documents and other content. You can also blacklist or whitelist applications and set rules for URL access. Wipe corporate applications selectively to maintain security in the event a device is lost or stolen

## MDM for Mac & Windows 10

Is MDM-style endpoint management more your style? You’re covered! With Mac MDM and Windows 10 MDM capabilities, you can extend your mobility management experience to your users’ laptops and more!

## Restrictions and Compliance Control

Maintain control of Android devices with Android for Work, including a robust list of Android restrictions such as camera, screen capture, and app uninstall, among others. Couple with compliance settings for both Android and iOS devices, and you can feel confident that mobile users are working within company policies.

## Don’t Forget About Mobile Security

When you add our Mobile Security Suite you gain several enhancements. For example, app-wrapping safeguards individual corporate applications. Secure mobile email enables users to access corporate email in their native app—whether the device is managed or not. And the secure mobile browser lets users safely access internal corporate websites. Be confident knowing that corporate applications are accessible and secured and that mobile users can access needed content easily via the user experience they demand.