Top Five Reasons to Leverage Ivanti UEM for Frontline Worker Enablement

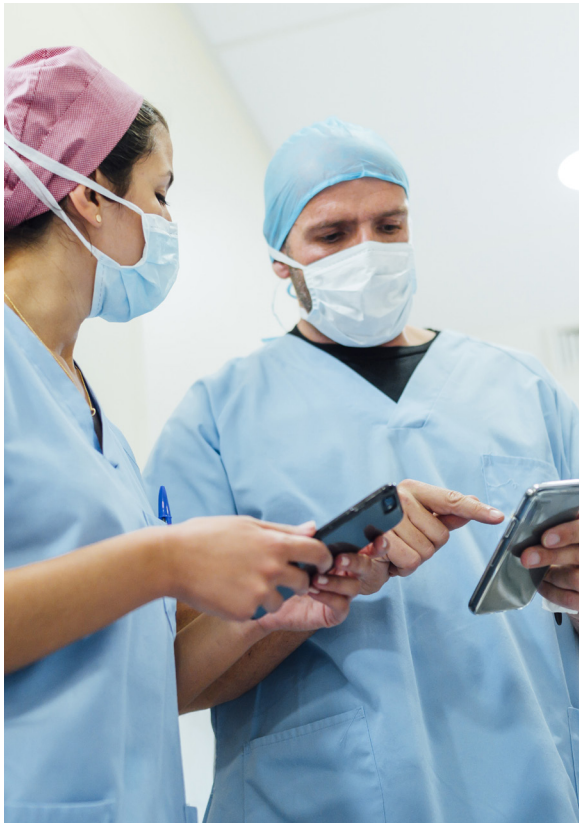
Why Ivanti UEM?

1. Streamline device enrollment and provisioning.
2. Grant secure access.
3. Allow only approved apps on corporate devices.
4. Enforce security policies.
5. Support shared devices.

Secure mobile productivity for frontline workers

Today's frontline workers are pushed to be more productive than ever before. That's why they need secure mobile devices and apps that allow them to access the information and workflows they need on any device, wherever they work. As traditional network perimeters become obsolete, secure productivity requires a zero trust approach that validates every frontline worker device, establishes user context, checks app authorization, verifies the network, and detects and remediates threats before granting secure access to a device or user.

With Ivanti unified endpoint management (UEM), organizations get a mobile-centric, zero trust security platform that supports frontline worker productivity in any environment, faster and more securely than ever before. Plus, IT has the confidence of knowing devices and apps are always in a consistent and secure state -- no matter how many users access them during the day.

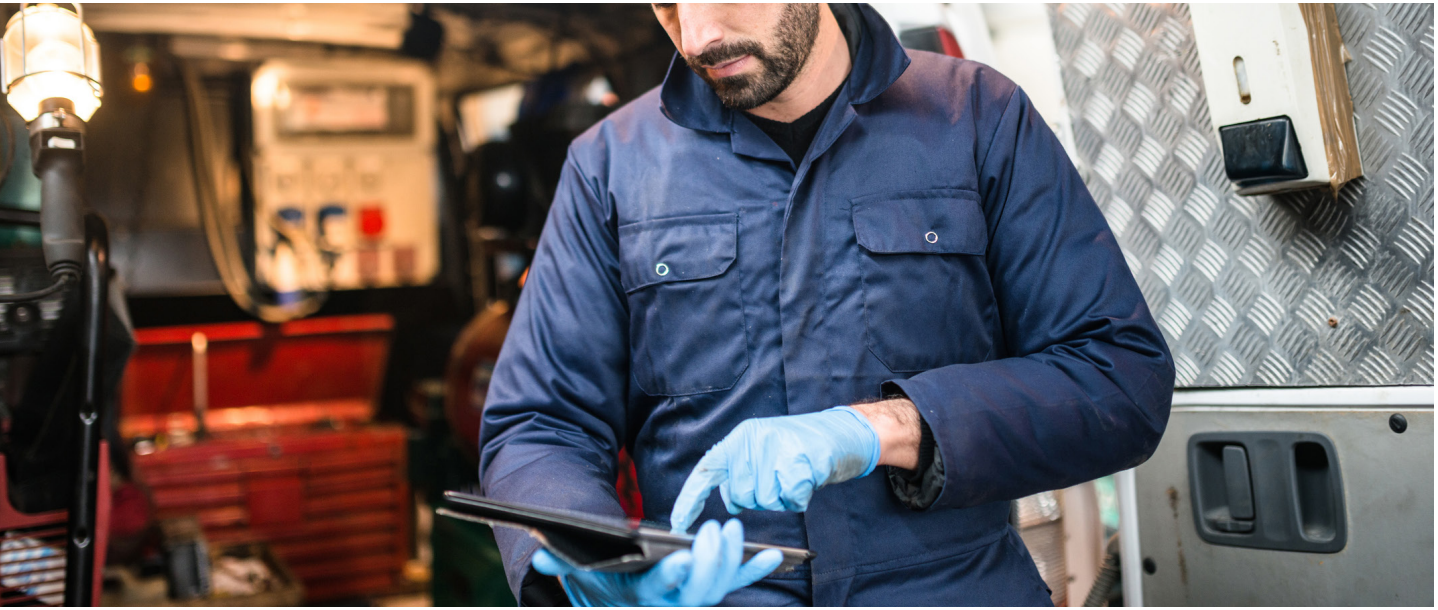


1 Streamline device enrollment and provisioning

Ivanti eliminates the time-consuming task of provisioning and configuring devices for new users. Admins can quickly set up devices over the air, with no manual configuration required. This not only saves countless IT hours, it ensures that workers in remote locations can quickly start using new devices provisioned with all the apps, configurations and security policies they need to be productive right away. Ivanti supports all major device enrollment programs, including Android zero-touch enrollment, the Apple Device Enrollment Program (DEP), Samsung Knox Mobile Enrollment (KME) and Microsoft Windows Autopilot.

2 Grant secure access

The Ivanti UEM policy engine grants secure access based on the context of the device, user, network or app. For example, a public utility worker can quickly access and update work orders in the field without returning to the office, which saves both time and money by eliminating extra trips. If the device is ever lost or stolen, or if a user tries to access an unauthorized network, the Ivanti policy engine can deny access and take appropriate compliance actions, such as notifying IT or quarantining the device.



3 Allow only approved apps on corporate devices

Frontline workers typically require only a few applications, such as inventory, maps, and point-of-sale (POS) apps on corporate-owned devices. Ivanti UEM makes it easy to deploy and update allowed business apps to devices and prevent users from installing denied apps such as social media, personal email and streaming music services. This helps keep business apps and data safe from potentially malicious apps and gives IT complete visibility and control over all apps and data on frontline worker devices. Ivanti UEM supports device management controls including:

- **Android kiosk mode:**
  Devices are restricted to an allowed set of apps only.

- **Android dedicated device:**
  Company-owned devices are restricted to a single use case, such as ticket printing or inventory management. This prevents users from enabling other apps or performing other actions on the device.

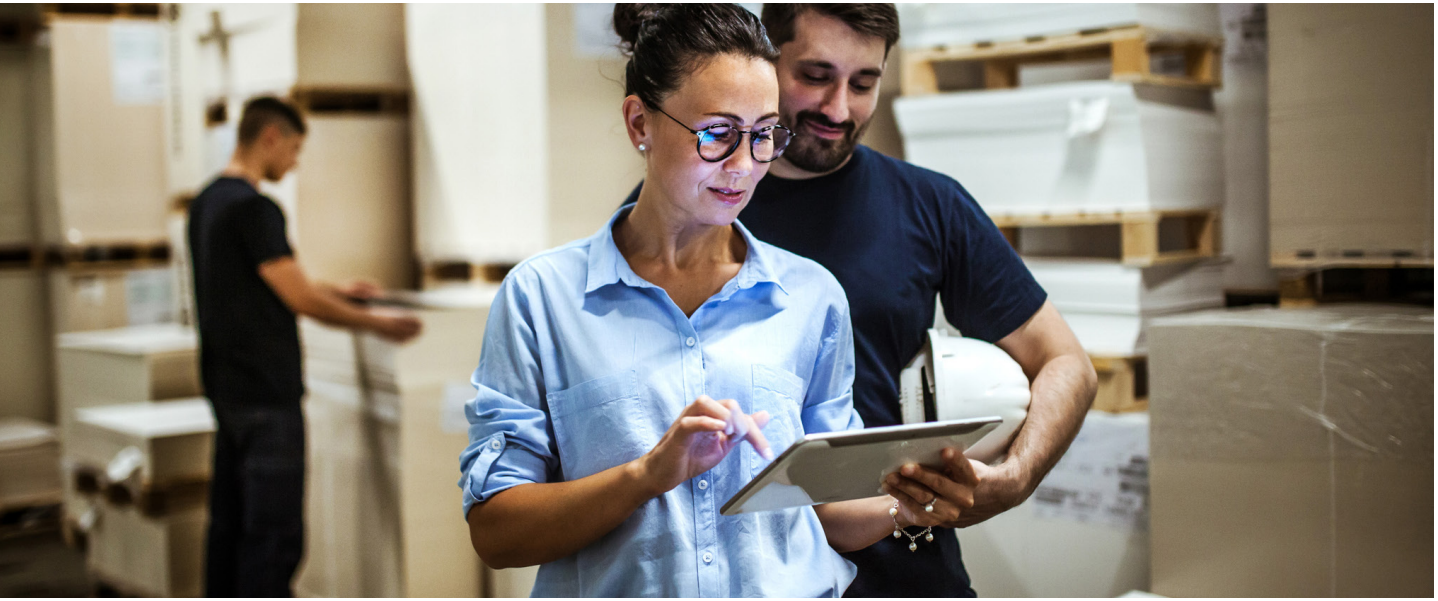
- **iOS supervised mode:**
  Device supervision allows admins to apply extra restrictions on corporate-owned devices, such as turning off AirDrop or preventing access to the App Store.

4 Enforce security policies

Ivanti helps IT ensure that frontline worker devices support only well-defined and regimented workflows, such as package delivery. Through Ivanti, admins can enforce certain device restrictions, such as disabling the camera and microphone, restricting Wi-Fi options, and more. Not only does this help to keep frontline workers productive, it also protects apps and devices from unsafe user behavior, such as accessing potentially compromised networks. Depending on the device OS and security requirements, admins can manage devices in a corporate-owned, single use (COSU) configuration or kiosk mode to ensure users can only access allowed apps and networks.

5 Support shared devices

Frontline workers frequently share devices, such as in a retail store where several assistants may access the same device to look up inventory or check out customers during the course of a shift. Each employee may have different responsibilities or job functions requiring access to different apps or content. For instance, a manager may have access to certain apps or approval functionality that regular employees do not. To securely support shared devices among multiple employees, Ivanti allows admins to assign role-based access to individual groups and users through a single management console.



ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com