導入Ivanti UEM支援一線員工生產力的五大理由

為什麼選擇Ivanti UEM？

1. 優化設備註冊及權限配置。
2. 授予安全存取權限。
3. 僅允許在公司設備上使用已被允許的應用程式。
4. 強制執行安全性原則。
5. 支援共享設備。

確保一線員工的行動生產力

今天的一線員工比以往任何時候都更有效率。這就是為什麼他們需要安全的行動設備和應用程式，讓他們無論在哪裏工作，都能在設備上存取所需資訊及工作流程。隨著傳統的網路界限已變得過時，安全生產力需要一種零信任方式，即在授予設備或使用者安全存取權限之前，驗證每個一線員工的設備、建立使用者框架、檢查應用程式授權、驗證網路並檢測和修復威脅。

通過Ivanti統一端點管理（UEM），企業可以獲得一個以行動為中心的零信任安全平臺，該平台支援一線員工在任何環境的生產力，比以往任何時候都更快速及更安全。另外，IT部門有信心知道設備和應用程式始終處於一致和安全的狀態——無論一天中有多少用戶存取它們。

1 簡化設備註冊及權限配置

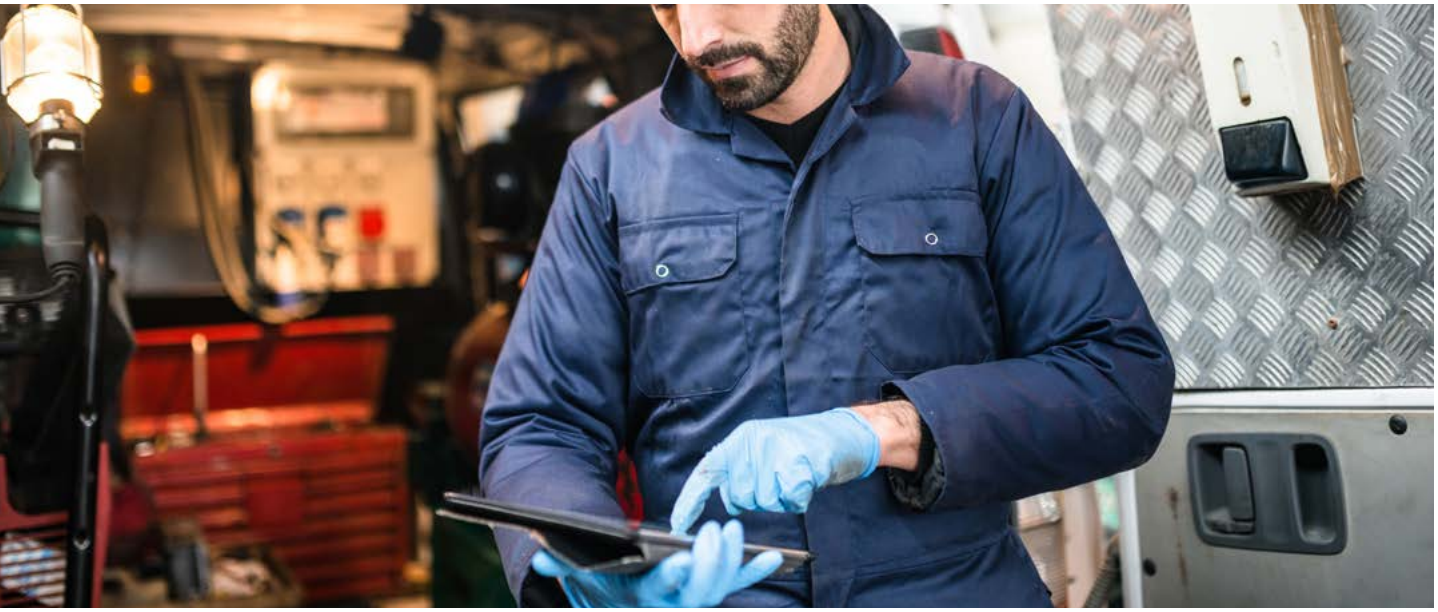
Ivanti移除為新使用者部署及配置設備的耗時任務。管理員可以通過無線方式快速設定設備，無需手動安裝。這不僅節省了無數的IT時間，還確保了遠程工作人員可以快速開始安裝並使用所有應用程式、配置和安全策略的新設備，他們需要立即有效率地工作。Ivanti支援所有主要設備註冊方案，包括Android 零接觸（Zero Touch），Apple裝置部署計畫(DEP), Samsung Knox Mobile Enrollment(KME),Microsoft Windows Autopilot。

2 授予安全存取權

Ivanti UEM策略引擎根據設備、使用者，網路，及應用程式的框架授予安全存取權限。例如，公共事業工作者可以在不返回辦公室的情況下快速存取和更新現場的工作指令，從而省去了額外的出差並節省了時間和金錢。如果設備遺失或被盜，或者使用者試圖存取未經授權的網路，Ivanti策略引擎可以拒絕存取並採取適當的合規性處置動作，例如通知IT部門或隔離設備。

3 只允許

在企業設備使用被允許的應用程式。線員工通常只需要一些應用程式，如庫存、地圖和企業自有設備上的銷售終端（POS）應用程式。Ivanti UEM可以方便地在設備上部署和更新允許使用的商業應用程式，並防止用戶安裝被拒絕的應用程式，如社交媒體、個人電子郵件和串流音樂服務。這有助於保護商業應用程式和資料免受潛在惡意應用程式的攻擊，並使IT部門能夠完全查看和控制一線員工設備上的所有應用程式和資料。Ivanti UEM支援設備管理控制，包括



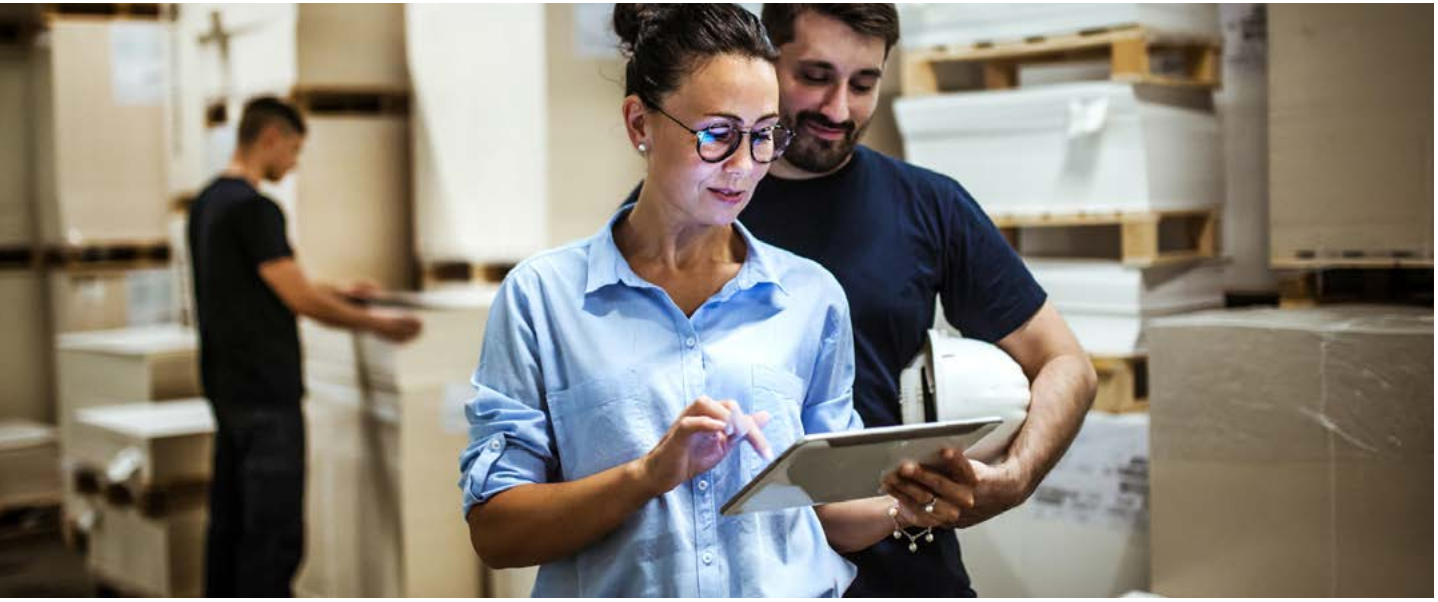
- **Android kiosk模式：**
  設備僅能安裝及運行特定App。
- **Android專用設備：**
  企業公發設備僅限於單一功能使用，例如票據列印或庫存管理。這會封鎖用戶在設備上啟用其他應用程式或執行其他操作 。
- **iOS監管模式：**
  設備監管讓管理人員擁有公發設備更多的限制權限，例如關閉AirDrop或封锁存取應用程式商店。

4 執行安全性原則

Ivanti幫助IT部門確保一線員工裝置僅支援已被完整定義且嚴格控管的工作流程，例如包裹递送。藉由Ivanti，管理人員可以強制執行某些設備限制，例如禁用相機和麥克風、限制WiFi選項等。這不僅有助於保持一線員工的工作效率，還能保護應用程式和設備不受不安全用戶行為的影響，例如訪問可能受到威脅的網路。根據設備作業系統和安全要求，管理人員可以將裝置配置成公發單一功能(COSU)設備，或啟用Kiosk模式確保使用者僅能存取被允許的應用程式及網路.

5 支援共享設備

一線員工經常共用設備，例如在零售店裏，店員們可以在輪班期間，共同使用一台設備查詢庫存或結帳。每個員工可能有不同的職責或工作職能，需要存取不同的應用程式或內容。例如，經理可以存取特定應用程式或審核功能，這是一般員工不需要的功能。為了安全地支援多個員工之間的共用設備，Ivanti允許管理人員透過單一管理主控台，依據工作職位存取權限，分配給單一群組或使用者。



ivanti.com
+886 975-125148
ContactChina@ivanti.com