

Ivanti® 移动设备管理器

在公司里，几乎天天都有人使用个人移动设备，这当然是件好事。因为员工可以随时随地访问快速的决策制定流程，并且响应业务活动，从而有助于提高工作效率。Ivanti® 移动设备管理器部署了各种安全措施，能够在各种终端间始终如一地保护企业信息，让移动设备的使用更加安全无虞。



管理 BYOD 以及企业拥有的端点

企业管理的设备应具有设备注册、策略部署和远程设备锁定等企业移动管理功能。想要更为成功地制定 BYOD 策略，需要平衡使用个人设备的用户人数。您需要保护企业信息，又不能侵入用户的个人移动设备空间。



真正的统一端点管理

Ivanti 移动设备管理器已与 Ivanti® 管理套件相集成。这样，IT 团队可使用单个系统来管理用户携带的所有设备。策略的统一交付变得简单，一键触控式员工入职成为现实。您可以只管理一次策略，并且将策略传播到所有用户设备上，从而为 IT 团队提供一致的安全性，确保各个设备之间的用户访问保持一致。



在各个设备上提供共同的体验

基于角色的工作区为用户提供访问所需的应用程序和企业信息的安全场所。您的 IT 团队可提供企业应用程序商店体验，使移动用户能够启动应用程序并精简对企业数据的访问。这一切，都通过从桌面到平板电脑和智能手机保持一致的界面和导航体验来完成。



可扩展应用程序的部署和注册

Ivanti 移动设备管理器中的功能随业务的发展而扩展。不再需要为组织中的每个 Apple 设备用户单独购买独立的应用程序许可。由于支持 Apple 批量采购计划，因此 IT 团队可以更轻松地采购和分发 AppStore 的应用程序。而支持苹果的设备注册计划 (DEP) 则让注册设备也变得非常轻松。最棒的是，可以跨 Mac 操作系统和 iOS 设备同时使用 VPP 和 DEP。



移动应用程序管理

将应用程序推动至用户设备，并控制对文档及其他内容的访问。您也可以创建应用程序黑名单或白名单，并设置 URL 访问规则。当设备丢失或被盗时，可以通过选择性清除企业应用程序来维护安全性。



限制和合规控制

Android 设备的维护控制，可利用 Android for Work，其中包括一份完善的 Android 限制清单，例如相机、屏幕截图、应用程式卸载等。配合 Android 和 iOS 设备的合规性设置，您可以放心让移动用户在公司策略允许的范围内工作。



移动安全记心上

添加我们的 Mobile 安全设备套件后，您将获得一系列增强功能。例如，应用程序封装保护单个企业应用程序。安全的移动电子邮件允许用户在其原生应用程序中访问企业电子邮件，而无论该设备是否受管理。此外，安全的移动浏览器还能让用户安全地访问内部企业网站。您可以看到，企业应用程序可访问并受到保护，而移动用户则可通过其需要的用户体验来轻松访问所需内容。

更多信息：

访问我们的网站：<http://www.ivanti.com>

与销售沟通：010-85153668 转产品咨询