Ivanti LANrev for Mobile Devices

Ivanti® LANrev allows you to manage and secure the mobile devices in your deployment remotely. The solution includes support for employee-owned devices and a web-based user interface so that IT can perform select administrative and security tasks working remotely or on the go.

Mobile Application Management

With Ivanti LANrev, policy management is not about policies but instead how they are applied. For example, a device can be part of a blanket security policy that applies to all devices, an app distribution policy that applies to one department, and a blacklist policy that applies only to company-owned devices. Ivanti LANrev policies are dynamic and can be reassigned whenever the applicable criteria changes on the device. This approach lets you manage dozens of policies versus thousands of devices. You can:

- Track and manage installed and in-house apps
- Build device records using custom data fields
- Employ a single-click download/install process for users
- Install/remove apps silently using management APIs
- Manage Apple Volume Purchase program(VPP) licenses easily
- Experience zero-touch deployment with full support of Apple Device Enrollment Program (DEP)

Security, Change, and Configuration Management

Set longer, more complex passwords for enterprise-level security. Lock a device, clear a password, and wipe a device clean to factory settings. Manage and deploy profiles to configure email, restrict apps, set up VPN, disable the camera, and deploy web clips. Use policy-locked configuration profiles to block non-compliant devices (jailbroken, blacklisted apps installed) from accessing company email and networks. Schedule policies so users have a defined window of time to access secured documents and corporate networks. Send customized messages and communicate with the end user wirelessly.

When it comes to user authentication, unlike device certificates, Ivanti LANrev generates unique certificates per user for Exchange email access. So instead of relying upon standard passwords, user authentication is a smooth process using certificates. This provides a much higher degree of security, an improved end-user experience, and a significant reduction in password-related security and help desk incidents.

Intelligent: Track and locate unauthorized apps. Block noncompliant devices from accessing the network. Control how and when users access sensitive corporate data.

Automated: Manage all of your in-house custom apps efficiently. Automate time-consuming configuration and profile work. Notify administrators with automated commands and remediate devices based on predefined conditions.

Cross-Platform: Enjoy ease of use and full cross-platform capabilities using a single console to manage PC, Mac, iOS, Windows Phone, and Android devices.

Mobile Content Management

Apply strict security controls for the sharing of files and media. Distribute sensitive or confidential files to devices without using email. Restrict content from being emailed, printed, or moved outside of the LANrev repository.

All content is managed with the same types of automated and dynamic policies used for configuration and provisioning. This includes scheduling the availability of

content on a device so that it can be deleted automatically based on date and time (down to the minute), no matter if the device is on or off the network. Mobile content management includes integration with the corporate SharePoint infrastructure to locate and assign content to the LANrev repository.

Asset Inventory

Gather hardware and software data points for analysis. Display data such as device serial numbers, MAC addresses, installed apps, telephone numbers, and other data with custom views, searches, and reports. Integrate your mobile device data with third-party applications such as Microsoft SCCM.

BYOD

Use the automated employee-enrollment process to onboard employees and their personally owned devices, eliminating the manual IT work associated with BYOD programs. Record employee opt-in and direct a copy of each confirmation to Human Resources. Assign BYOD-specific policies automatically to ensure these devices only access corporate networks and data if they are compliant.

System Requirements

- Servers
- Windows® Vista and later[i]
- macOS 10.6 and later[ii]
- Admin Consoles
- Windows Vista and later[i]
- macOS 10.10 and later[ii]
- Agents
- Windows XP and later[i]
- macOS 10.5 and later[iii]
- Mobile Client Platforms:
- - iOS 6.0 and later[ii] [iii]
  - Android 2.3.3 and later[iv]
  - Windows Phone 7 and later

www.ivanti.com

1.800.982.2130

sales@ivanti.com

i including Windows® Server 2012, Windows Server 2008, Windows 7®, Windows 8® & Windows 10®

ii including macOS Sierra and iOS 10

iii Previous agent software versions may be available to support older operating systems

iv Some Android systems without access to Google Cloud Messaging (GCM) services may not be supported.