Ivanti UEM for Android

The challenge

- Secure sensitive data on Android devices while maintaining user privacy.
- Ensure the right applications are available to users.
- Lack of technical expertise within an organization to onboard/scale Android deployments.
- Identify the right deployment modes to deliver critical business value with superior user experience.
- Consistent management across Android devices from different manufacturers such as Samsung, Pixel, Zebra and more at scale.

The Everywhere Workplace

Ivanti makes the Everywhere Workplace possible. Our comprehensive unified endpoint management (UEM) platform is purpose-built to secure Android environments. Manage devices, applications and content with ease – with access to our UEM technology and integration services around the world thanks to our global partner network.

Scalability. Security. Ease. Global Expertise. These are just a few of the reasons organizations trust Ivanti to help accelerate their Android adoption. With 2.5 billion monthly active devices, Android has become the number one mobile platform for consumers. For enterprises, Android powers the widest range of deployments including single-use, dedicated use cases, kiosk mode, rugged devices for frontline workers and high-end knowledge productivity tools.

As the first provider to deliver an enterprise app storefront, BYOD privacy controls and certificate-based identity management for Android, Ivanti is also one of the first UEM providers to support the Android enterprise platform.

A flexible fit

Ivanti UEM for Android supports a broad range of use case scenarios. Segment users by role and device ownership. Company-owned, personally owned (BYOD), Corporate-owned personally enabled (COPE) frontline and task- worker dedicated devices – with Ivanti for Android, select what's best for your organization and extend employee productivity with the right tools and the right devices for a secure mobile transformation.

Consistent IT management across disparate devices at scale

Android enterprise delivers a deeper and more consistent security model to enterprise customers while ensuring user privacy. Ivanti supports this model. Using Ivanti's UEM console, IT can securely distribute enterprise apps and push configurations to Android devices. These features not only simplify IT management, but they also reduce Android fragmentation by enabling more consistent app distribution and security.

Capabilities

- Broad multi-vendor support by securely enabling Android devices and apps.
- Streamline onboarding by using Samsung Knox Mobile Enrollment (KME) and Google Zero Touch Provisioning with Ivanti UEM solution.
- Separate security domains for work and personal data on the device.
- Enforce security and privacy policies.
- Protect data-at-rest through encryption and DLP controls.
- Preserve the native device experience and keep employees happy.
- Maintain granular app-level control over the entire lifecycle.

Key use cases

- **Ensure privacy and compliance inorganizations tasked with protecting sensitive data.** Secure business data on any endpoint and separate business and personal data on various endpoints including Android devices.
- **Enable multi-device, multi-OS, multi-app management from a single console.** In a mixed-device environment with Android based devices (Samsung, Google, Pixel, Zebra, Oculus, Honeywell etc.), iOS, macOS and Win 10 laptops, unified device management is top priority.
- **Empower Android frontline workers.** Support the field, fleet and mobile workers in healthcare, transportation, manufacturing and other industries who use rugged devices or devices in kiosk mode.
- **Provide superior end user choice and a seamless user experience.** Device choice and user experience are essential for productivity and compliance. Ivanti UEM provides streamlined onboarding and a superior on-device experience.
- **Industry security certifications for UEM.** Gain industry-standard security certifications such as FIPS 140-2 Validated Container, Common Criteria MDM PP V3.0, DISA STIG, FedRAMP and National Cryptologic Center – Assurance High.
- **Provide security automation for device compliance.** Automated tier compliance quarantines or deletes all business data or apps on compromised devices without manual IT actions.

A secure foundation for Android in the enterprise

How does Ivanti UEM address enterprise security concerns so well? By enabling a containerized enterprise persona that separates personal and professional apps and content – all while preserving the native user experience. Whether the device is corporate-owned or employee-owned as part of a BYOD program, IT has full control over the enterprise container. The administrator can set and manage app and data-level policies and perform selective or complete wipes of the container.

Long story short: Ivanti UEM for Android gives IT comprehensive data security controls while the user retains a seamless experience across devices.

Features include:

Device security

- Work profile on company-owned employee enabled devices for better user privacy.
- Secure Android devices with passcode and biometric policies.
- Protect unauthorized access by locking down hardware access.
- Kiosk mode lockdowns, with support for shared devices.
- Control what wi-fi networks the device can connect to

Data security

- Separate app and user data encryption.
- Individual certificate-based security for email, Wi-Fi, and VPN.
- Secure via single or Ivanti Zero sign-on.
- Selective quarantine/wipe of business apps and data.
- 5G slicing support

Data loss prevention (DLP)

- Encrypted attachment control.
- Screen capture control.
- Copy/paste control.
- Control what information is shared between device and work profile

Secure network access

- Sentry acts as an email and content in-line gateway that manages, encrypts and secures traffic between the Android device and back-end enterprise systems.
- Tunnel is a multi-OS per-app VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.

Complete device lifecycle management

Onboarding a fleet of Android devices manually is a tall order. This is made especially challenging by the long list of Android device vendors including Google, HTC, LG, Samsung, Zebra, Honeywell and more. Zero touch enrollment with Ivanti UEM for Android automates onboarding, user provisioning, configuration, application deployment and security and control of Android endpoints for users, including remote workers. With Ivanti for UEM enrollment you can also:

- Provision the devices in specific modes based on the privacy/security requirements.
- Deploy and preconfigure apps customize to your needs.
- Reduce IT needing to physically preconfigure each device while giving the user a white glove experience.

Using corporate-owned devices?
Maintain both security and the native user experience with Ivanti UEM. Here's what's possible:

- Automate user provisioning when users log into the device.
- Support provisioning of corporate-owned, kiosk or single App mode, and shared device use cases across your organization.
- Centrally configure and push user email, Wi-Fi and VPN settings.
- Set device-security standards.
- Track device inventory and details.
- Seamlessly install business applications to the device.
- Automate application and Android updates.
- Wipe corporate data off a device at the end of the device lifecycle, employee termination or loss of device.
- Unattended remote-control capabilities to support devices even when the user is unavailable.

Examples of zero touch enrollment for Android vendors:

- Google Zero Touch Provisioning (ZTP): Enables an IT administrator to mass deploy configured, managed, and corporate-owned devices.
- Samsung Knox Mobile Enrollment (KME): Provides automated enrollment of Samsung Galaxy devices capable of Android Enterprise (AE).

Comprehensive XR and VR device management including next-generation AOSP devices

- Support file transfer for business apps, firmware files and any type of files up to 10GB
- Seamless in-house app distribution
- Support multiple versions
- No limits on APK size
- Apps distributed via Content Delivery Network (CDN)
- Support deployment in-house and preconfigured applications and updates
- Secure apps with per-app encryption with Ivanti Tunnel
- Support certificates and certificate authentication
- Over-the-air updates, control and VPN configuration
- Remote lock and wipe

Application management

App productivity is key to worker productivity, and that's why Ivanti offers the most comprehensive platform for mobile application management on Android devices. Ivanti supports managed Google Play or Apps@Work for app distribution and discovery, data security with native enterprise containers or AppConnect and AppConfig for an industry-standard means of delivering secure configurations to enterprise apps.

With Ivanti UEM for Android, business apps are inside a secure container with data encrypted, protected from unauthorized access and wipeable. A single container passcode secures access to business apps, and users can easily access and share data between apps. The Ivanti platform manages all containerized apps for centralized policy management, supporting native Android workflows and a productive mobile experience for users.

Additional highlights include:

- Secure, identity-based delivery of in-house and Google Play Store apps through the Apps@Work private app storefront.
- Improved productivity via secure user apps:
  - Email+ for containerized corporate email, calendar and contacts.
  - Docs@Work for secure document storage.
  - Help@Work to provide remote access for faster helpdesk resolution of issues.
- Selective wipe of business apps and apps data on the Android devices.
- Allow/deny list of apps to protect against inappropriate access.
- Containerization and dynamic policy to protect data-at-rest and enable compelling app-based user experiences through AppConnect.

Ivanti unified endpoint management

Device management and security	Ivanti Neurons for MDM	Ivanti Neurons for MDM Premium
Security and management. Secure Secure and manage endpoints running Apple iOS, macOS, iPadOS, Google Android, and Microsoft Windows operating systems. Available on-premises and as a cloud service.	✓	✓
Mobile application management (MAM). Secure business apps with AppStation on contractor and employee devices without requiring device management.	✓	✓
Easy onboarding. Leverage services such as Apple Business Manager (ABM), Google Enrollment and Windows AutoPilot to provide users with automated device enrollment.	✓	✓
Secure email gateway. Sentry is an in-line gateway that manages, encrypts, and secures traffic between the mobile endpoint and back-end enterprise systems.	✓	✓
App distribution and configuration. Apps@Work is an enterprise app storefront that combined with Apple Volume Purchase Program (VPP, facilitates the secure distribution of mobile apps. In addition, capabilities such as iOS Managed Apps and Android Enterprise allow for easy configuration of app-level settings and security policies.	✓	✓
Secure Connectivity		
Per app VPN. Tunnel is a multi-OS VPN solution that allows organizations to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.		✓
Conditional access		
Trust Engine. Combine various signals such as user, device, app, network, geographic region and more to provide adaptive access control.		✓
Passwordless user authentication. Passwordless multi-factor authentication uses device-as-identity for a single cloud or on-premises application.		✓

Ivanti unified endpoint management (continued)

Scale IT operations	Ivanti Neurons for MDM	Ivanti Neurons for MDM Premium
Helpdesk tools. Help@Work lets IT remotely view and control a user's screen, with the user's permission, to help troubleshoot and solve issues efficiently.	✓	✓
Reporting. Gain in-depth visibility and control across all managed devices via custom reports and automated remediation actions.	✓	✓
Secure productivity		
Secure email and personal information management (PIM) app. Email+ is a cross-platform, secure PIM application for iOS and Android. Security controls include government-grade encryption, certificate-based authentication, S/MIME, application-level encryption and passcode enforcement.		✓
Secure web browsing. Web@Work enables secure web browsing by protecting both data-in-motion and data-at-rest. Custom bookmarks and secure tunneling ensure that users have quick and safe access to business information.		✓
Secure content collaboration. Docs@Work allows users to access, create, edit, markup and share content securely from repositories such as SharePoint, Box, Google Drive and more.		✓
Mobile app containerization. Deploy the AppConnect SDK or app wrapper to provide an additional layer of security for your in-house mobile apps, or choose from our ecosystem of AppConnect integrated apps.		✓
Derived Credentials. Support two-factor authentication using common access cards (CAC) and personal identity verification (PIV).		✓

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

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