



Mobile Management for Android Smartphones and Tablets

Advanced security, reliability and scalability for Google Android smartphones and tablets in your mobile enterprise infrastructure.

Now IT departments can ensure that users have consistent, reliable and secure access to enterprise data and applications while avoiding costly delays, downtime and compliance violations. Zenprise helps you provision Android smartphones and tablets; proactively monitor and troubleshoot Android user and infrastructure problems; and manage Android policies and configurations. Zenprise also supports Apple iOS, BlackBerry, Windows Mobile, Windows Phone and HP Palm OS devices.

Greater insights for end-to-end control

With Zenprise, you know when devices connect to your corporate network, whether these devices are employee- or company-owned and if they are missing security policies or have the incorrect policies applied. Zenprise keeps you informed of critical system details to help you manage every step of the mobile device lifecycle, from Exchange ActiveSync provisioning to the decommissioning of devices.

Fast, sure-fire protection

With Zenprise device management capability, you can proactively monitor the Android smartphones and tablets in your mobile enterprise. When problems occur, Zenprise performs automated diagnostic tests to quickly identify the root cause of Android device issues for faster troubleshooting.

Immediate locks and wipes

When smartphones or tablets are lost, Zenprise gives you the ability to avert potential corporate data security breaches. IT help desk representatives can immediately remotely wipe clean an Android device to prevent access to unauthorized corporate data.

Zenprise automates and eases the management of Google Android smartphones at every stage in the mobile lifecycle.

Mobile Device Lifecycle Stage	Feature	Benefit
Configure	<p>Applications & Device Settings</p> <ul style="list-style-type: none"> • Wifi settings (WPA, personal, WEP, WPA2) • Enable/Disable application installs 	<p>Enforces Sarbanes Oxley and HIPAA requirements to Android smartphones and tablets.</p> <p>Protects enterprise from loss of confidential data</p>
Secure	<p>Device Security</p> <ul style="list-style-type: none"> • Enforce passcodes (simple, complex) • Auto-lock device after inactivity • Auto-wipe device after certain number failed attempts • Configure APN • Restrict ports used by mobile apps on device • Data loss protection—identify all files installed on device • Track lost or stolen devices <p>Application & Infrastructure Security</p> <ul style="list-style-type: none"> • Encrypt data between mobile apps & enterprise infrastructure • Audit & log all mobile app traffic • Remotely kill rogue app processes • Remotely remove malicious apps 	<p>Enables organizations to document compliance with HIPAA, SOX and other global standards</p> <p>Mitigates risks and averts potential security breaches</p>
Provision	<p>Roles based provisioning integrated with LDAP</p> <p>Profile-lock: Ensures that profiles remain on device</p> <p>Enterprise App Store</p> <ul style="list-style-type: none"> • Provision applications • Provision application updates 	<p>Quickly activate thousands of users</p> <p>Maintain consistency across all deployed devices for corporate compliance</p> <p>Quickly deploy enterprise applications</p>
Maintain	<p>Proactively detect user or infrastructure problems (e.g., mail outage, LDAP problems, carrier outages)</p> <p>Return real time device statistics</p> <ul style="list-style-type: none"> • Processes running • Device memory & CPU • Signal strength • Battery level • OS version number • Carrier • Available storage • SD card details • Applications installed 	<p>Reduce support calls from end users</p>
Track	<p>Assets</p> <ul style="list-style-type: none"> • Employee owned & corporate provided devices • Hardware versions • SIM IDs • IMEI/Serial # <p>Expenses</p> <ul style="list-style-type: none"> • Detect roaming users • Detect inactive users • Track expense plans of employees • Require roaming users to connect applications through Wifi only 	<p>Reduce overall wireless bill</p> <p>Facilitate device refreshes/ updates</p>
Decommission	<p>Full wipe of device- returns device back to factory default</p> <p>Select wipe of device—only removes corporate data and leaves personal data on device</p> <p>Lock device</p>	<p>Protect corporate data on device should device be lost or stolen</p>

