Technical Review

Android Enterprise Essentials: Easy, Automatic Mobile Device Security

Date: January 2021 **Author:** Jack Poller, Senior Analyst

Abstract

This ESG Technical Review documents testing of Android Enterprise Essentials with a focus on assessing the speed and simplicity of automatically securing Android devices.

The Challenges

Protecting an organization from a cyber-attack has become more difficult as attackers gain sophistication and knowledge through experience, developing stealthy attacks targeting key personnel in weakly protected organizations. These attackers threaten organizations with automated tools, reducing the adversary's cost and effort and enabling the attacker to target a larger population at scale. And attackers are progressing from large, heavily defended organizations to smaller organizations that may be perceived to be less well protected—a perception arising from the reality that SMBs are often resource constrained, especially for cybersecurity. This is why almost half (47%) of organizations believe that cybersecurity will be one of the most important considerations for justifying IT investment in the next year (see Figure 1), making it the most-cited response.[1]

Figure 1. Most Important IT Investment Justifications

Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results: *2021 Technology Spending Intentions Survey*, December 2020.

With 48% of organizations facing a problematic cybersecurity skills shortage, SMBs are searching for security solutions that are easy to deploy and manage, requiring no training and minimal investments in time and effort.[2]

Android Enterprise Essentials

Leveraging Google's experience building Android Enterprise device management and security tools for the world's largest organizations, Google designed Android Enterprise Essentials to be a simple, secure management service providing integrated, automatic security to protect business devices and data for small and medium businesses. Android Enterprise Essentials enables an organization of any size to:

- Require a lock screen to prevent unauthorized access to company data.
- Enforce mandatory malware protection by ensuring that Google Play Protect is always on and users cannot download apps outside of the Google Play Store.
- Remotely wipe all company data from a device in case it is lost or stolen.
- Remotely reset screen locks.

Android Enterprise Essentials automatically applies these core features that remain in place even when an employee resets their device. There is no device configuration required by either the company or the employee.

To further simplify and lighten the workload on the business, Google is partnering with distributors and resellers to enable businesses to drop-ship managed devices directly to employees at remote offices or their homes and have the devices automatically appear in the management portal.

The benefits of using Android Enterprise Essentials include:

- Protection for all mobile devices and their data
- New devices added automatically after purchasing from a reseller
- No additional IT training or resources required
- Seamless and easy for employees to use
- Extension of core protections to devices that may not need advanced device management

ESG Validated

ESG represents a typical SMB with 45 employees of varying technological skill levels from novice to expert. As is usual for a small organization, ESG's single IT manager is responsible for all IT services from mobile devices to cloud applications and cybersecurity.

ESG purchased devices from a reseller for four distinct roles: managing partner, executive vice president, knowledge worker, and IT administrator. The reseller shipped devices to each employee's home address. Each employee was directed to unbox the phone and proceed through the device's guided installation and setup process. During setup, because the devices were managed by Android Enterprise Essentials, each employee was forced to use a PIN to protect the lock screen.

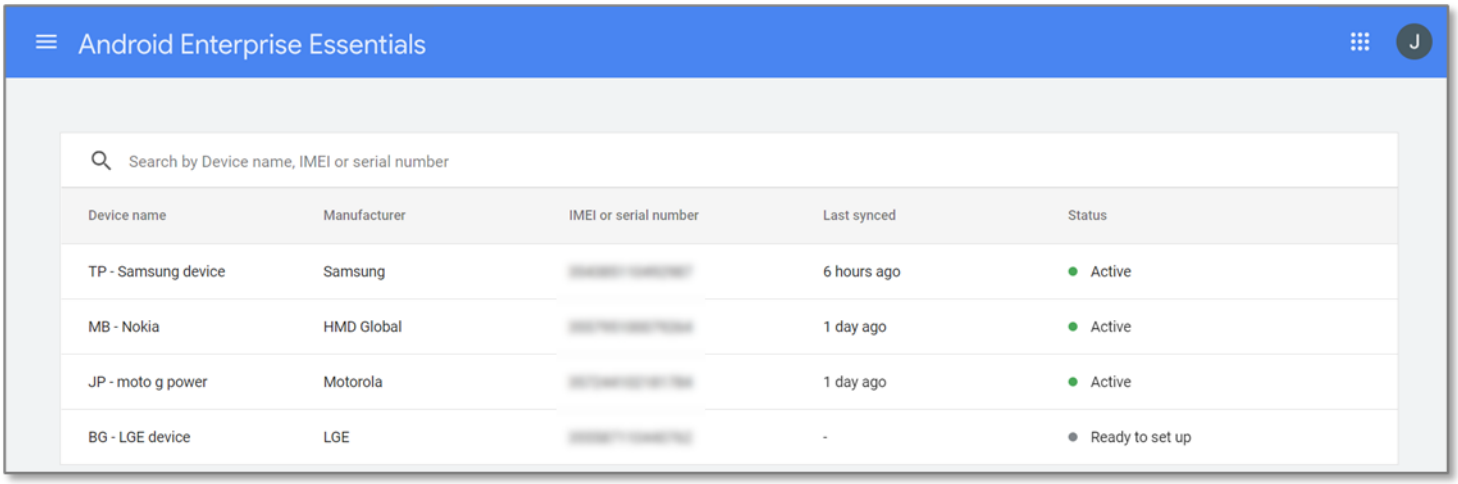
"The out-of-the-box experience and initial setup was seamless, as I was able to access business and personal applications within minutes."

-Knowledge Worker

Next, ESG logged in to the Android Enterprise Essentials management portal. As shown in Figure 2, the portal provides a filterable, sortable list of all managed devices, detailing the device name, manufacturer, IMEI or serial number, last synced date and time, and status.

[2] *Ibid.*

Figure 2. Android Enterprise Essentials Management Portal



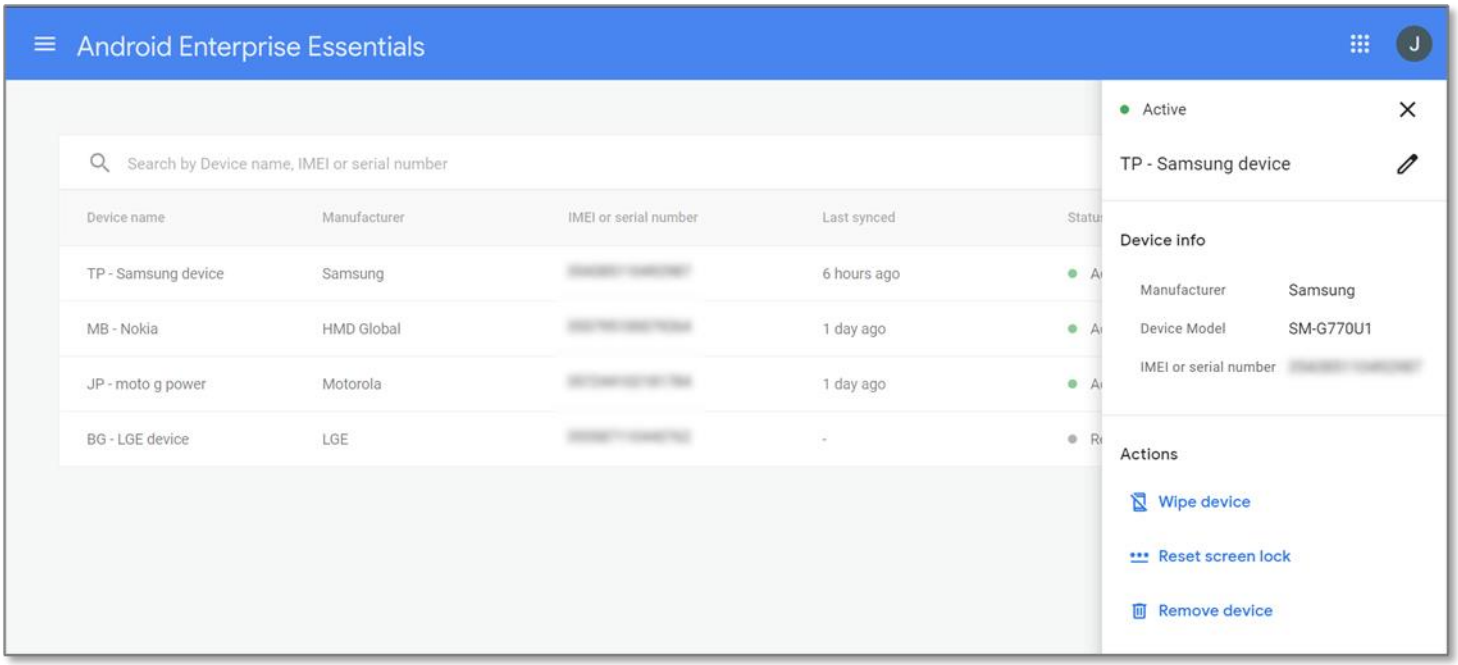
Source: Enterprise Strategy Group

We clicked on the first device in the list and a popup window displayed the device details and provided options to wipe the device, reset the screen lock, or remove the device from the management portal, as shown in Figure 3. We could also access the device management options by hovering the mouse over a line in the list of devices and clicking on the "3-dot" menu that was displayed on the right side of the line. This second method also provided an option to rename the device.

"I was pleasantly surprised how simple and easy it was to manage devices and perform tasks without having to go through a steep learning curve and specialized training."

-IT Manager

Figure 3. Device Details



Source: Enterprise Strategy Group

Next, we selected ***Rename*** and renamed the device.

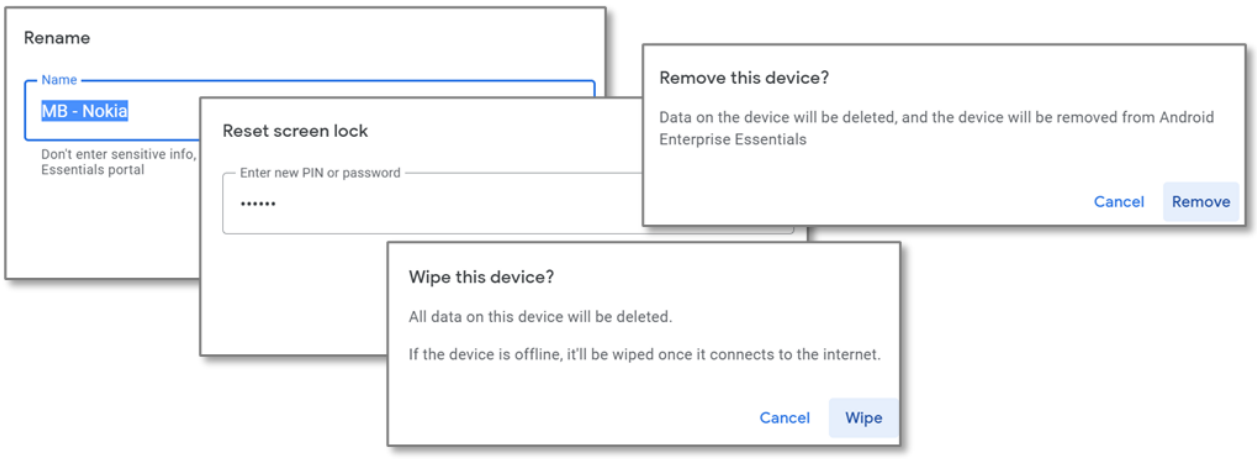
We also selected ***Reset screen lock*** and changed the screen lock PIN for each device. Each user verified that the screen lock PINs changed instantly for their device, and they were immediately able to use the new PIN.

Next, we selected ***Wipe device***, and verified that as soon as the device connected to the network, it erased all data and reset to factory defaults. We proceeded through device setup a second time and verified that all secure features remained in place after reset.

"I watched as the device was wiped and reset to factory defaults. There is a peace of mind knowing that the device is protected and that the company has taken steps to secure and protect its employees"

-Executive Vice President

Figure 4. Popups to Rename, Remove, Reset, or Wipe a Device



Source: Enterprise Strategy Group

Why This Matters

SMBs face two simultaneous challenges: a large number of unsecured devices with access to company applications and data and a lack of IT resources to manage and secure devices. As SMBs accelerate the transition to the always-on, always-available mobile workforce and their dependency on mobile devices increases, they need simple, effective, and automatic device and data security without increasing the IT workload..

ESG validated that Android Enterprise Essentials provides a simple solution for mobile device security. The interface is easy and intuitive, and non-technical users can quickly wipe lost or stolen devices or reset PINs. Device security—including enforcing screen lock PINs, device encryption, and malware protection, as well as preventing app downloads outside of the Google Play Store—is enforced across wipes and resets. Businesses can deploy Android Enterprise Essentials without dedicated administrative resources and gain confidence that employee devices and data are protected.

The Bigger Truth

Businesses are increasingly indicating that their top considerations for investment are security and increased user productivity. These considerations are especially important for small and medium businesses with limited resources to support an ever-increasing mobile workforce.

ESG found that devices enrolled in Android Enterprise Essentials are automatically secured. Resellers ship devices, preconfigured with security policies, directly to remote locations. The devices are encrypted, require a PIN on the lock screen, and ensure Google Play Protect is always on for malware protection and prevention of downloading apps outside of the Google Play Store. These security features are enabled by default, and neither IT administrators nor employees have to take any additional actions.

"It was very cool to see the 'managed by Android Enterprise Essentials' displayed on the device, as it is actually comforting for a user like me knowing the device is protected."

-Managing Partner

ESG found Android Enterprise Essentials to be easy to use and simplified securing and managing mobile devices and device data. Without any training, we used the management portal to quickly and easily rename devices, remotely reset lock screen PINs, and remotely wipe devices. Android Enterprise Essentials enforced all security features after a device was wiped and reset. We anticipate that IT administrators will only use the portal for the rare instance of wiping a lost or stolen device.

ESG looks forward to seeing how customers respond to these simple management and automatic security features. At this point, Google is in the process of opening up availability of Android Enterprise Essentials to the field, and Google has invested heavily in testing and integration to ensure smooth operation.

If your organization is looking for a seamless employee experience and simple, automatic device security, then ESG believes that you should consider how Android Enterprise Essentials can provide confidence in security for your business and a safer work environment for your employees.