SAMSUNG

Making every vote count

Samsung's end-to-end solution helps government agency safeguard election integrity

Challenge

The election oversight agency of a Latin American country needed a mobile solution to help employees transmit vote counts from the country's voting districts. The agency was concerned, however, that mobile devices offered too many opportunities for fraud and data leakage. The agency wanted rigorous controls to help ensure transparency and maintain security.

Solution

The agency chose an end-to-end solution from Samsung that met all its requirements. With the Knox Manage enterprise mobility management (EMM) solution, the institution can restrict device usage, monitor and track devices remotely, and troubleshoot issues. And agency devices now come with defense-grade Knox protection to minimize device-level vulnerabilities.

Results

The government agency gained confidence in the Samsung solution through repeated trials. By choosing a complete solution from a single partner, the agency has gained one-stop support for peace of mind in case of issues, efficient device set up that benefits employees and IT, and government-grade security that starts at the device level.

Knox

SAMSUNG

MAINTAINING VOTE-COUNT INTEGRITY

Election compliance requires strict control over people, systems, and technology. One government agency responsible for collecting millions of votes during elections wanted a mobile solution that would meet these requirements:

- High security standards.
- Ability to prevent unauthorized activities.
- Transmission only over a secure network.
- Rapid troubleshooting capabilities.
- Big screen for ease of use.
- Biometrics authentication.

> "With high-profile, politically charged elections ahead, the government is confident in its ability to maintain control over devices that will transmit vote counts."

Samsung manager
in Latin America

Challenge

Maintaining clear oversight using mobile devices

The election oversight agency of a Latin America country wanted to improve the productivity and effectiveness of its team during the 2019 elections by providing mobile devices to workers in the country's voting districts.

The agency's major concern was the security of sensitive data transmission. First, the agency helped raise security standards for carriers to help ensure transparency and minimize election fraud.

To protect against data leakage and hacking, the agency knew it also needed to retain maximum control over all devices distributed. This meant regulating who used the devices and which apps they accessed. The goal was to prevent unauthorized activities such as sending text messages and emails, as well as misuse in case of theft or loss. To thwart hacking and prevent data leakage, the agency needed employees to use a proprietary application to transmit votes over a secure network.

Other requirements included the ability to track device location and monitor usage. And if employees ran into issues during the elections, the agency needed rapid troubleshooting capabilities.

The high-profile project was so complex and sensitive that the agency hired an IT security consulting firm to help find the best solution.

Solution

Samsung solution enables granular control over devices

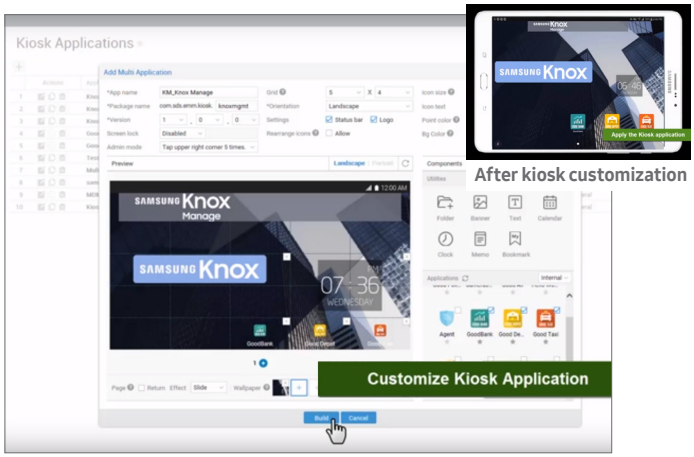
Working with its security consultant, the election agency chose a complete solution from Samsung that met all its requirements. Samsung offered a proven management solution and devices built on a defense-grade security platform.

MANAGEMENT SOLUTION

To maintain control over devices once they were in the hands of remote employees, the agency chose Knox Manage, an enterprise mobility management (EMM) solution. Knox Manage helps the agency restrict device use, monitor and track the devices, control devices, and troubleshoot issues remotely.

Restricting device usage. The election agency used the Kiosk Wizard feature to customize a kiosk mode that would allow only certain features and applications to work. The agency prohibited certain activities to minimize data leakage, including SMS texts and access to apps at the Google Play store, and used the EMM to configure the Virtual Private Network (VPN) and Access Point Name (APN) needed to transmit vote counts securely.

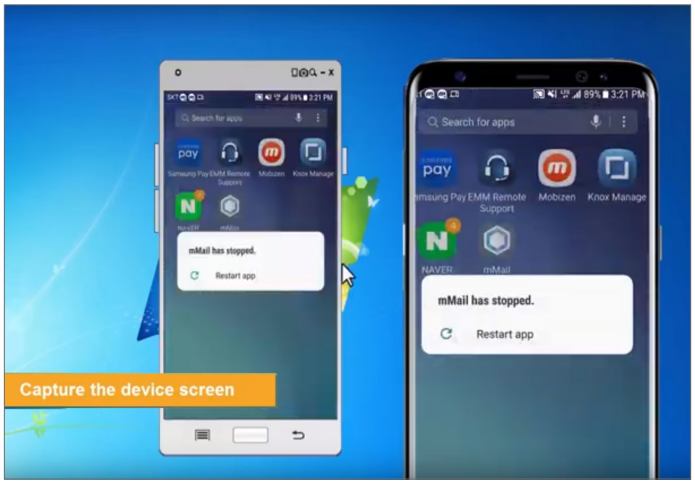
Knox Manage application management features enables the agency to install and update apps without user intervention and disable app uninstallation to ensure devices are in appropriate condition for use. The agency also requires biometrics authentication to make sure only the authorized employee can use a given device.



Using Kiosk Wizard to create a kiosk mode without coding. Organizations use Knox Manage to customize a kiosk mode that restricts devices to specific purposes. With Kiosk Wizard's drag-and-drop controls, they can easily customize the home screen, for example, adding only apps they want to enable.

Monitoring and tracking devices. Device location tracking provides the geographical locations of devices. The agency can also view device inventory in real-time, which enables IT admins to audit devices and receive early warning of equipment misuse. The agency is also able to use the EMM to locate the last position of a device, remotely block or wipe devices, even selectively delete information from a device and authorize or deny access to an application.

Troubleshooting remotely. The Knox Manage Remote Support tool helps the agency address user issues immediately. The feature provides full access to the devices as if the IT admins are using the devices themselves. IT administrators gain the ability to view the home screen and run an app, for example.



Using Remote Support to gain control over devices.

MOBILE DEVICES

Election employees receive either a cost-effective smartphone or a rugged tablet, based on their role and the needs of the election center. The agency uses the Knox Mobile Enrollment portal to simplify device set up and register the devices with the Knox Manage EMM.

Both devices come with the government-grade protection of the Knox platform and include biometric authentication. Although EMM solutions can restrict device usage, security can easily be compromised if the devices themselves are vulnerable. Knox adds protection with a multi-layered platform built into the hardware and software. Knox continually verifies the integrity of the device through a chain of security checks that begin at the hardware level and extend through the operating system.

> "The election agency selected Samsung based on its ability to provide an end-to-end solution—from software and devices to support."

Samsung manager
in Latin America

Results

End-to-end solution streamlines operations, support

Despite initial concerns about using an unfamiliar EMM to carry out its mission, the government agency gained confidence in the solution through a series of demonstrations and trials. In fact, the agency gained additional benefits by selecting an end-to-end solution with hardware, software, and support from the same partner:

Streamlined, one-stop support. With an end-to-end solution that includes devices, a management solution, and support, the agency is able to simplify lifecycle management and resolve issues faster. Instead of spending time trying to understand each issue, the agency can turn to Samsung for comprehensive support.

Efficient device set up for employees and IT. With the help of Samsung's streamlined EMM installation, enrollment services, and professional support, the government agency has simplified the setup process for both employees and its IT team. With Knox Mobile Enrollment, IT admins can make sure each device includes all appropriate security policies without physically touching it. When the employee receives the device, all that's needed is to open the box and connect the device to a network. Immediately, the Setup Wizard launches the EMM agent and the EMM automatically applies correct security settings and configurations. The device is then ready for controlled, secure use.

Government-grade security. The agency selected two Samsung devices built on the Knox platform, renowned for its security features. Knox received 25 of 28 "Strong" ratings in a December 2017 Gartner report and is approved by government and security organizations worldwide. Samsung manufactures and configures its devices in its own factories, and builds the Knox platform into device hardware and software. Knox security complements the Android operating system security and makes Samsung phones, tablets and wearables the most reliable on the market.

About Samsung Electronics Co., Ltd.

Samsung Electronics inspires the world and shapes the future with transformative ideas and technologies that give people the power to discover new experiences. With a constant focus on innovation and discovery, we keep redefining the worlds of TVs, smartphones, wearable devices, tablets, digital appliances, network systems, and memory, system LSI, foundry and LED solutions.

For more information

For more information about Samsung Knox Manage, visit: www.samsungknox.com/km.

Copyright © 2019 Samsung Electronics Co. Ltd. All rights reserved. Samsung and Samsung Knox are either trademarks or registered trademark of Samsung Electronics Co. Ltd. Samsung is not liable for errors or omissions. All brand, product, service names and logos are trademarks and/or registered trademarks of their respective owners and are hereby recognized and acknowledged.

Knox

SAMSUNG