

White Paper:

The Ultimate Guide to Customizing Tablets

Using Samsung's Knox Configure to create a secure, highly customized platform for your business applications



Tablets Have Become a Tool for Business Transformation

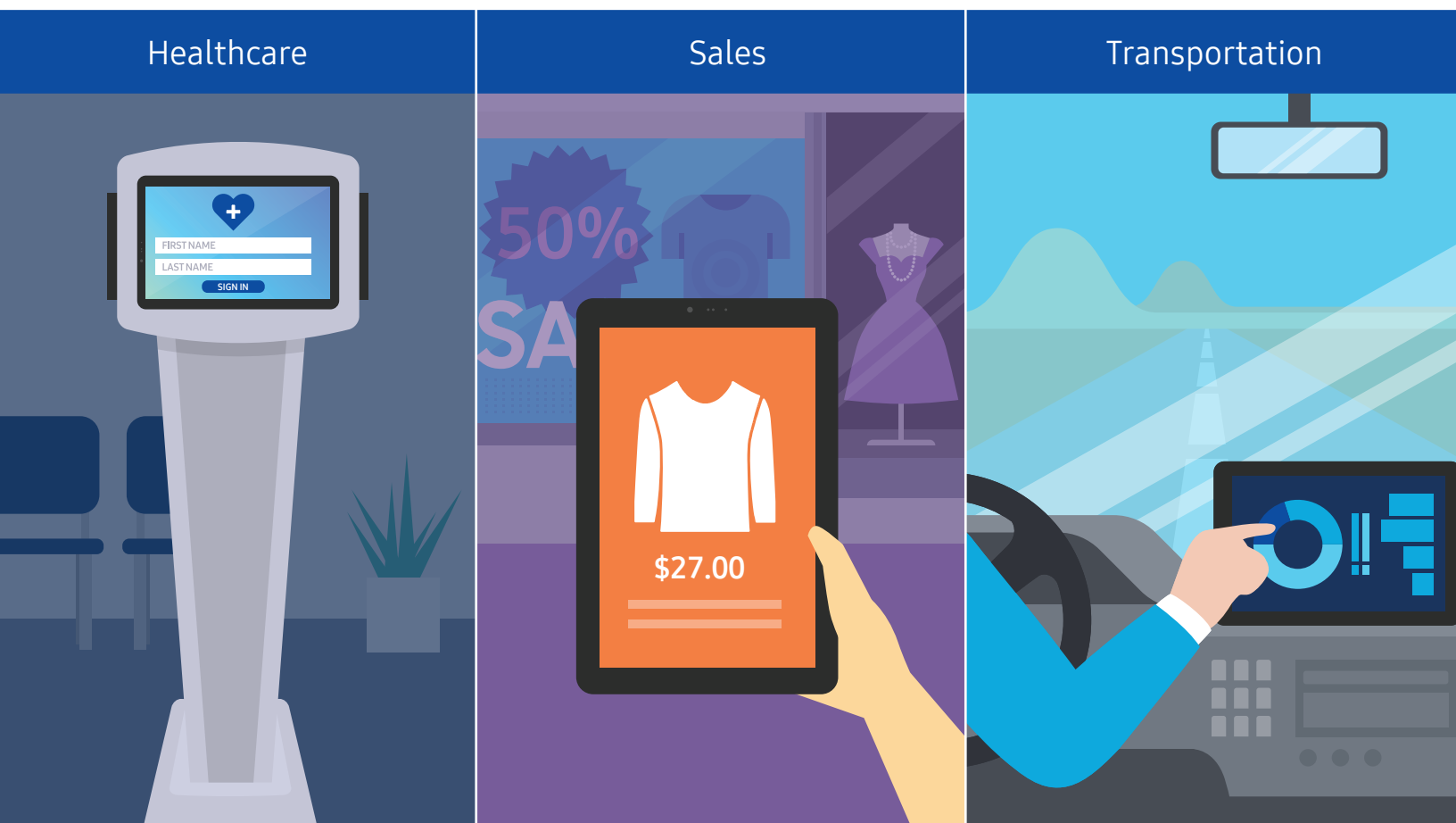
Tablets have established an important niche in both personal and enterprise computing. Lightweight with long battery life, a large display, fast processor and wireless connectivity, the unadorned tablet is an ideal device for browsing the web, reading documents, streaming video or video conferencing.

Business leaders and IT innovators, however, see the tablet as more than an inexpensive browser. With the right application(s) and accessories, tablets provide a flexible and affordable platform for digital transformation. From patient in-take forms in healthcare and customer kiosks in retail, to hospitality order-taking, trucking hours of service logging and more, a tablet offers an ideal replacement for pen-and-paper processes or legacy technology. These new digital processes vastly improve speed and accuracy of data capture while creating a more positive customer experience and reducing costs.

However, IT managers tasked with transforming an off-the-shelf tablet into a dedicated workforce tool

encounter one key challenge: the sheer flexibility that tablets provide to the user. Why? Because, as in many of the business use cases described above, the tablet is intended to perform just one clear task. Access to other preloaded apps or features such as the camera, microphone or Bluetooth connectivity could distract from the tablet's core purpose and may even pose a security risk. What's needed is a way to easily reconfigure off-the-shelf tablets to create a customized device with only the desired applications, features and connectivity options.

This white paper maps out how Samsung's Knox Configure solution provides businesses the ability to fully customize tablets and other mobile devices to meet diverse industry needs. It will outline questions that will help determine if a customized tablet is the right solution to achieve your business objective, discuss the key planning steps prior to device configuration, and then walk through the customization process with Knox Configure, presenting several typical use cases.



Making Sense for Your Business

Configuring and deploying tablets for dedicated applications may look like an easy decision for IT managers, but it has to make sense for the business. When looking at tablets for dedicated applications, IT managers should answer four specific questions to be sure the deployment makes sense.

1

Will this improve my staff and customer experience?

Every IT project, especially those using mobile devices, should improve the experience of staff and customers. Taking a tablet into the field without the right applications or accessories can make things worse rather than better. IT managers should be prepared to answer not just if it will improve the experience, but how it will improve the experience.

2

Will this create a competitive advantage?

While making customer and staff experiences better is necessary and good, it's not sufficient to justify a dedicated application tablet deployment. The project also has to create a competitive advantage that results in increased revenue, time- or money-saving. Digitization for the sake of digitization isn't a good reason. IT managers should be able to describe how the new solution will create a competitive advantage for the enterprise.

3

Is it cost effective in terms of time and money?

Dedicated application tablets are almost always more cost effective than purpose-built hardware, so IT managers are already on the right side of the budget. But even with inexpensive hardware and efficient customization tools, there are other costs to consider. Quantifying time and money savings for these types of projects can be difficult. For example, if the app satisfies a regulatory requirement, the price of noncompliance is hard to gauge. Still, IT managers should be able to quantify the resource cost of a tablet project, and identify where this will save the enterprise time and money.

4

Does this project create a new security risk?

The answer to that question is almost always "yes." Any time you put enterprise data on a mobile device, you're increasing the risk of data loss or compromise. However, good deployment design will mitigate these risks, and you should even reduce the overall risk of data loss by eliminating paper-based systems or by increasing data collecting and monitoring. IT managers should identify the new security risks that a project creates, and show how these risks will be mitigated.




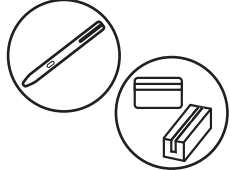
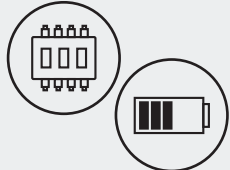

It Starts With the Right Apps

The app or apps running on your customized tablet are ultimately the key to your business case. While this guide does not attempt to tackle the subject of application development for such a diverse set of potential business purposes, that doesn't mean it should be overlooked. There are important strategic decisions to be made, such as whether to license or build, how your apps will integrate into back-end systems, and how they will be updated over time. Once you have the right applications, the customization of the tablet will ensure the optimal presentation of those apps on the device, ensuring adoption and compliance.

The Big Picture of Dedicated Applications

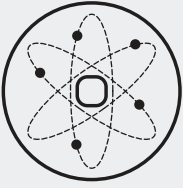
Most tablet customization projects begin with an idea: a particular experience you want to create for staff, for customers, for passers-by — for whomever. Getting from the idea to the execution is not nearly as difficult as it might seem. Yes, there are a number of steps, but each one is fairly straightforward and easy to complete.

The table below highlights the six main steps that happen before you hand out your first tablet, and provides some hints on the main issues you'll be reviewing and resolving.

Step	Main Issues and Questions
<div data-bbox="40 745 68 793">1</div> <div data-bbox="138 751 295 814">Identify your application(s)</div> <div data-bbox="129 829 308 1008">  </div>	<p>The app(s) are the first and most central concern when developing dedicated mobile devices. Fortunately, IT managers searching for ideas need not work too hard; options will come flooding very quickly. Software vendors are aggressively moving to add mobile solutions to their existing application suites, while startups and developers are making use of tools that help accelerate and reduce the cost of developing custom business apps. It's important to take a considered approach, taking advantage of trial periods, discussing the deployment process in detail and conducting security reviews. If building your own app, be conservative in developing your timeline. Build in a brief proof of concept (PoC) period, in the field and with real constraints.</p>
<div data-bbox="40 1087 68 1136">2</div> <div data-bbox="138 1087 430 1119">Select "add-on" hardware</div> <div data-bbox="129 1129 357 1297">  </div>	<p>When deploying tablets for special-purpose apps, there are almost always accessories and options needed to complete the picture, and these should be among first considerations. These may be as simple as a ruggedized case or mount to help prevent damage or theft, but could also include special data collection devices, such as electronic styli, credit card or barcode readers, keyboards or extended batteries. The accessories and options that are needed for the application should be identified early because they can drive tablet selection.</p>
<div data-bbox="40 1360 68 1409">3</div> <div data-bbox="138 1360 397 1423">Select your base tablet hardware</div> <div data-bbox="129 1434 357 1602">  </div>	<p>Many dedicated tablet projects are based on economical hardware rather than premium devices, as the apps do not require the latest processors or large amounts of RAM or storage. Of course, if you have particular needs that are best met by a high-end tablet, or a small screen device, this is the time to identify the right hardware. When picking the right tablet, keep in mind add-on hardware compatibility, battery life and connectivity requirements and lifecycle. If the deployment will be conducted in phases or on an ongoing basis, ensure that the model selected will be available for the duration of the transition or purchase replacement units in advance.</p>
<div data-bbox="40 1665 68 1713">4</div> <div data-bbox="138 1644 438 1738">Identify and resolve any InfoSec, legal and physical security issues</div> <div data-bbox="129 1749 308 1927">  </div>	<p>It's a good idea to bring InfoSec staff to the table at the project start, even before a PoC is fully designed. New mobile technology under consideration may be at odds with established security architectures. For example, if the application is not currently internet-accessible, mobile devices may need to start up a VPN tunnel before they can connect. Similarly, legal and security teams responsible for data protection will definitely want to get involved early any time protected company data starts moving out of the building on easily stolen and misplaced mobile devices. Their concerns and requirements (for example, encryption or other hardware protection features such as biometric authentication) need to be addressed early on.</p>

5

Link applications to your network and authentication infrastructure



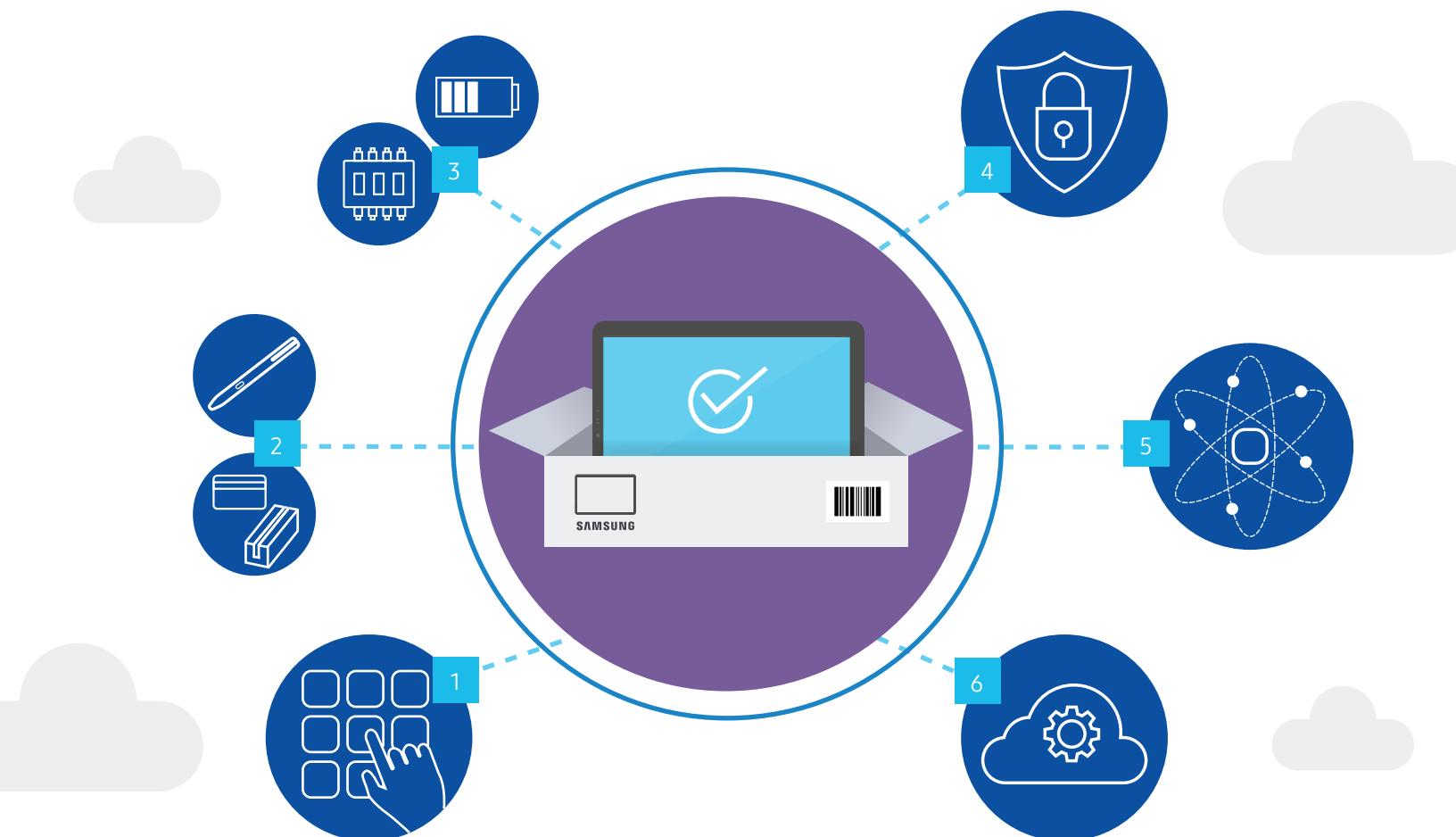
Most tablet applications require some network connectivity, and this should be worked out early in the process. If they're always used on-site, connecting them to a new or existing Wi-Fi network is the best choice, avoiding trusted corporate nets. When the tablets roam off-campus, cellular connectivity will patch up the gaps, but should probably be combined with a VPN if the application touches any sensitive data. Authentication choices are an important security consideration. Sometimes the answer is obvious. For example, when a tablet is providing digital signage or is being used in a display-only mode, there may be no authentication needed at all — power-on all the way to application launch can be a one-key operation. However, it's not always so clear-cut. In the Android world, there are two clear points at which authentication might occur: when logging into the tablet, and when running the individual application. Deciding which of these authentication methods to use, and how to link the tablets to your existing authentication infrastructure, will have an effect on both security and usability.

6

Configure the tablets to meet your needs



If selecting applications and tablets is the most visible, high-profile work, configuring and managing the tablets is the submerged iceberg that can sink a ship without proper navigation. Unless you're designing your project for a single tablet, you'll want to use a configuration tool to create a tested and approved "golden master" for your tablets. With a good configuration tool, you can deploy quickly and repeatedly with a minimum of resources required. One of the competitive differentiators that Samsung has to offer is Knox Configure, which can simplify the configuration stage and allow more granular controls to be put in place, reducing deployment time and support costs. The use of Knox Configure will be the focus of the remainder of this guide.



Customization With Knox Configure

In the Android world, getting a mobile device from the box to the user generally requires two passes. The first is used to get the proper operating system version and any initial applications loaded, set up basic device settings (most often connectivity settings, such as Wi-Fi networks and VPN settings) and enroll the device in a mobile device management (MDM) or enterprise mobility management (EMM) tool. The second pass is controlled by the MDM/EMM tool and fine-tunes device and application settings, while bringing it under tighter control for reporting, patching and enabling security controls such as remote lock and remote wipe.

Dedicated application tablets are slightly different animals. In many cases, they are not attached to enterprise MDM/EMM tools — which means that a good configuration tool is needed to get the tablet set up properly.

With Samsung's Knox Configure, enterprises can fully customize the device — applying connectivity settings, deploying apps, enforcing security controls and much more — right out of the box. The IT manager creates a profile or gold master in the Knox Configure portal and assigns it to a list of devices. When users unbox the device and connect to Wi-Fi or a cellular network, the configuration profile is automatically pushed to the device.

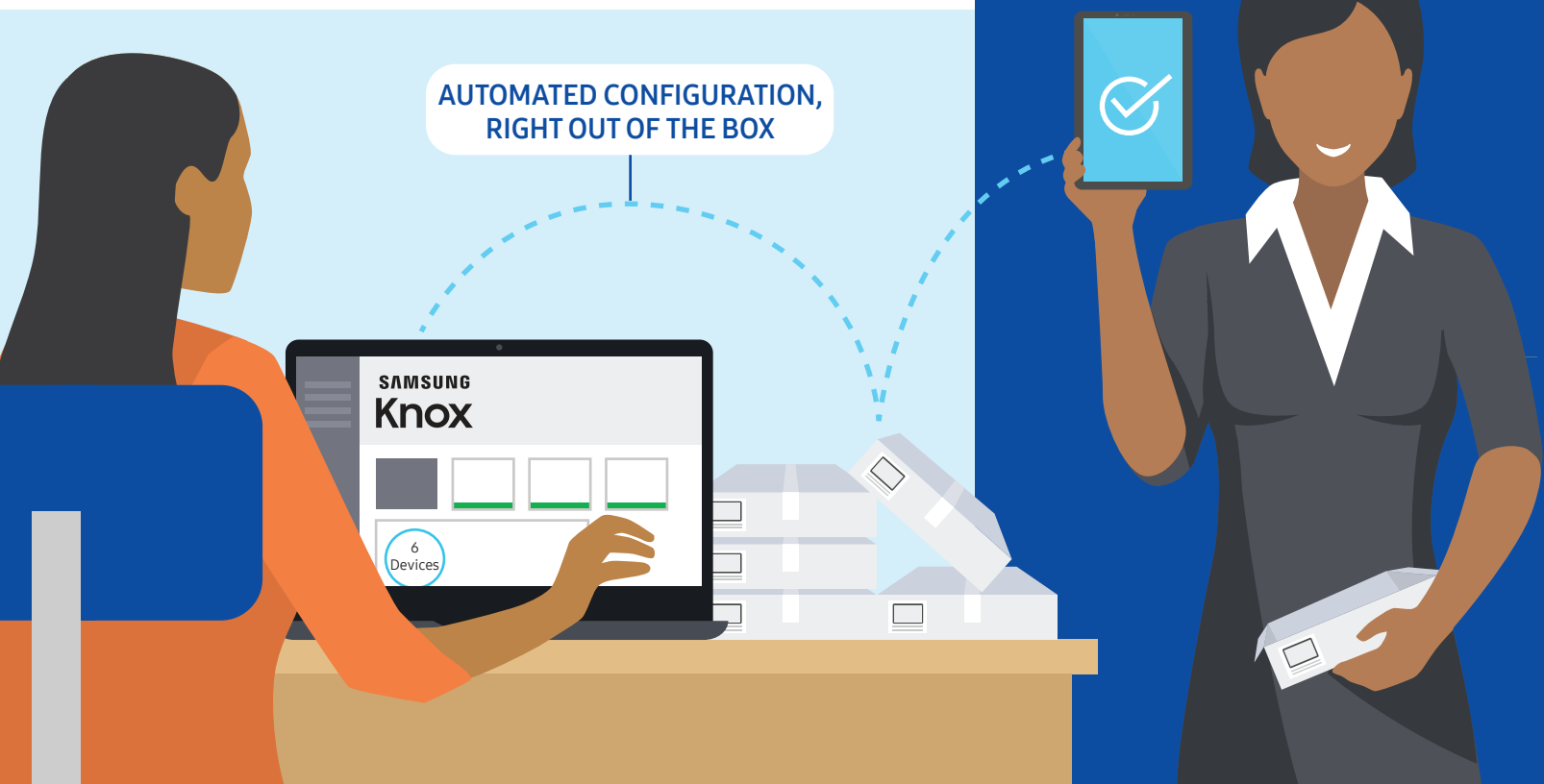
If the tablet is known and associated with an enterprise configuration profile, Samsung's Knox Configure servers can strictly control the device boot (such as removing factory reset options); deliver software licenses; preload applications and widgets (and associated settings); push initial security configuration; control home, lock screen, settings and system button functions; download content and contacts; and load up initial connectivity settings.



Enhanced Time to Market

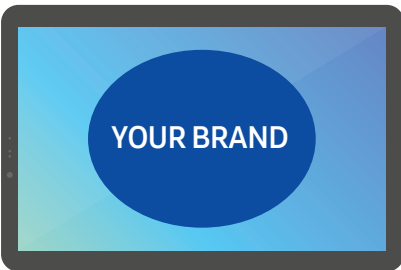
When customizing with Knox Configure, devices can reach their intended end user or location still in the box, without requiring several passes from the IT administrator. Quick configuration settings include:

- Preconfiguring one or multiple Wi-Fi connections before entering network's range
- Whitelisting, blocklisting, and installing workflow-specific applications
- Preinstallation of necessary company data, including contact lists and employee-specific content



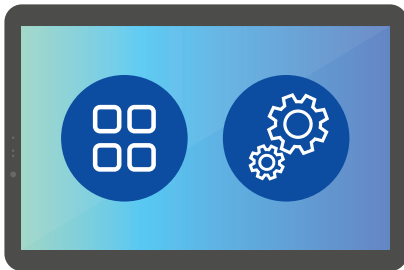
What's in a Knox Configure Profile?

Knox Configure is based on profiles, which are collections of settings that are applied to devices. Each profile has five major categories of settings that together control how the tablet will be configured.



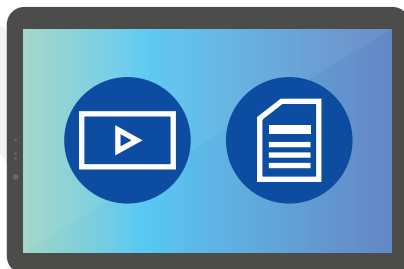
User Experience

Wallpapers, favorite applications and shortcuts, screen layout, sound levels, display brightness and rotation, fonts, custom booting and shutdown animations, language, country, time settings, kiosk mode



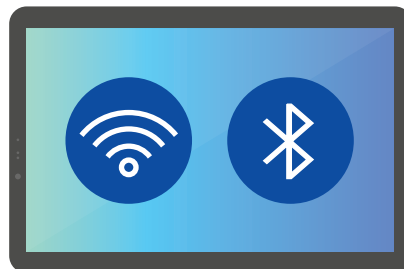
Applications and OS Controls

Applications to be immediately loaded, list of disabled applications (such as browsers and app store), application install/uninstall controls, application autolaunch, application settings (such as names and icons), browser and Samsung DeX settings



Content

Content such as documents or videos to be preloaded, contacts to be preloaded, widgets to be preloaded



Connectivity

Settings for Wi-Fi, Bluetooth, location sharing, Near Field Communications (NFC) readers, cellular data controls



Security

Settings for software updates, safe mode, multiuser mode, USB connectivity and debugging, disabling other configuration tools, application permissions

Using Knox Configure to Build a Dedicated Application Tablet

These four common use cases show how Knox Configure can get you from shrink wrap to deployment. They might not match exactly what you're planning, but most deployments look like one of these four. Each use case includes Knox Configure features that can help you to create the user experience you want.

1

One-time tablets.....pg. 9

These are devices that are deployed once and never updated. A typical example would be a single-event deployment, such as for a concert, special meeting, professional conference or temporary museum exhibition. Some of these devices may not even be network-connected when they are deployed, if all the data is local. Of course, one-time tablets are not really One-time: one of the challenges is retrieving them after the event and then getting them ready, quickly, for the next event.

2

Restricted-use devices.....pg. 10

These devices are locked down to a single application or set of applications. They're usually handed to a staff member to help with their day-to-day job responsibilities, but with a very restricted set of applications, preventing use as a general-purpose tablet. Restricted devices are usually network-connected, often including both Wi-Fi and cellular networks. A typical example would be a field service technician with one or two custom applications, plus some very specific (whitelisted) web-based applications, or a warehouse worker with a tablet wrapped in a special case and with barcode and RFID readers. These devices are usually tightly locked down and carefully configured, but because they aren't allowed to browse the internet or download new applications, they aren't managed to the same level of detail as the enterprise's bring- or choose-your-own-device (BYOD or CYOD) devices.

3

Enterprise devices.....pg. 11

These tablets have a clear primary purpose: to run a specific application. But they are still usable for other functions, such as web browsing. As with restricted devices, they're usually network-connected. A typical example would be a caregiver in a home health scenario, or a retail staff member running point-of-sale on a showroom floor. These devices aren't that different from a tablet that someone might buy off-the-shelf, except that their configuration has been optimized to speed their assigned application, while extraneous uses, such as personal email, are blocked. They are usually managed using the same tools as the enterprise's other mobile devices, such as those covered by a BYOD or CYOD program.

4

Digital kiosks.....pg. 12

These tablets are network-connected and generally mounted in a secure, fixed location, such as a cabinet or locking bracket. This is the traditional digital kiosk where the typical user is casual and may be looking for information, or otherwise engages in gentle interaction with the tablet. Some typical examples would be a digital concierge in a building or another public/private location such as an airport or meeting room.

1 One-Time Tablets

A one-time tablet doesn't get updates or changes — once it's deployed, it lives out its life and then gets recycled for the next project. Knox Configure has two types of profiles: "Setup Edition" and "Dynamic Edition." The first, Setup Edition, is perfect for this use case as it sets the device up once. (Dynamic Edition, which will appear in other use cases below, allows Knox Configure to dynamically change the configuration of connected devices over-the-air.)

The edition of Knox Configure (Setup or Dynamic) you select doesn't change what you can configure; it just changes whether or not the device tries to change its configuration once deployed. If you're making changes to a profile each time you host a new event and you don't want old devices to accidentally pick up new profile updates, Setup Edition ensures that the device stays configured the way you left it.

Individualized User Experience

One-time tablets tend to be constrained in what they do, so a typical profile would include particular applications to be installed, while other applications are locked (such as setting the web browser home screen). For this use case, Knox Configure lets you control the user experience and lock settings down tightly. From the start of the boot, where you can control branding and animations, to basic Android layout such as wallpapers and appearance of the lock screen, Knox Configure lets you apply your own visual style to the tablet.

Event Guide Tablet

If you are customizing a set of tablets for handing out to attendees as an event guide, consider the following configurations:

- Apply a branded event wallpaper to your boot and home screens
- Preload your event apps for dedicated schedules and real-time updates
- Preconfigure Wi-Fi connection to the event venue's network
- Disable/hide other preloaded apps not relevant for event attendees
- Disable installation of other applications from Google Play



2 Restricted Tablets

Restricted tablets are a great way to build an application experience on inexpensive off-the-shelf products and avoid the costs and delays of purpose-built hardware.

Knox Configure Dynamic Edition profiles are perfect for these types of projects. Although the same settings are available in Setup and Dynamic edition, a tablet with Knox Dynamic Edition profile will periodically try to “phone home” over its network connections. If its profile has been updated, it will automatically apply any updated settings, download any new apps and bring itself into conformance with any profile requirements.

Improving Workforce Efficiency

As well as determining which business apps will be preloaded, IT managers can also define a certain app or apps to automatically launch at boot. Additionally, if users frequently access web-based resources, it can be helpful to set the Internet browser home page and add a set of bookmarks. Small configurations like this can lead to big productivity gains when viewed across the entire field force, and also drive uniformity in business practices.

If the tablet is being used within the Samsung DeX environment, all of DeX’s settings can also be controlled through Knox Configure profiles. In this way, businesses using the Galaxy Tab S4 for both mobile and desktop productivity can customize both experiences for optimal efficiency.

Managing Business Contacts and Data

When a tablet project includes locally stored data on the tablet, Knox Configure profiles can be used to preload the data and even a contact directory for the tablet’s address book. Or, IT managers can define an application to be launched immediately after configuration that can take responsibility to preload data or update data caches on the device.

Although Restricted Tablets are normally used in a well-defined environment, IT managers who want to roll out new features gradually or conduct field testing before a big deployment can easily move devices between different Knox Configure profiles to change settings and push updates to a subset of users. The dynamic nature of Knox Configure’s updates, working over both cellular and Wi-Fi networks, means that users are almost always up-to-date with the latest settings.

Retail Inventory Management Tablet

When designing a restricted-use tablet for inventory management, consider this set of task-focused configurations:

- Preload your inventory management and scanning apps
- Configure these core apps to launch automatically upon boot
- Disable web browsers, or limit internet access to a set of preloaded bookmarks
- Preconfigure and limit connectivity to warehouse Wi-Fi
- Disable/hide other preloaded apps not relevant to retail workers
- Disable installation of other applications from Google Play



3

Enterprise Devices

An enterprise tablet comes with a heavy dose of preconfiguration, but because these devices often have a mixed business/personal or enterprise/internet use, security is also top-of-mind.

A dynamic profile in Knox Configure for enterprise devices will often concentrate on locking down the security aspects of the device, while allowing more freedom to run different applications or operate in home/work mode. Knox Configure lets the IT manager control software and firmware updates, multiuser mode, safe boot mode, applications and application store choices and even USB and SD card access.

Mobility is tied tightly to communications, which means IT managers will want to keep clear control on communications options as well. Tightly defined Wi-Fi profiles, cellular APN configurations and VPN settings are all important in preventing data breaches. These are all part of Knox Configure profiles.

Working With Existing Solutions

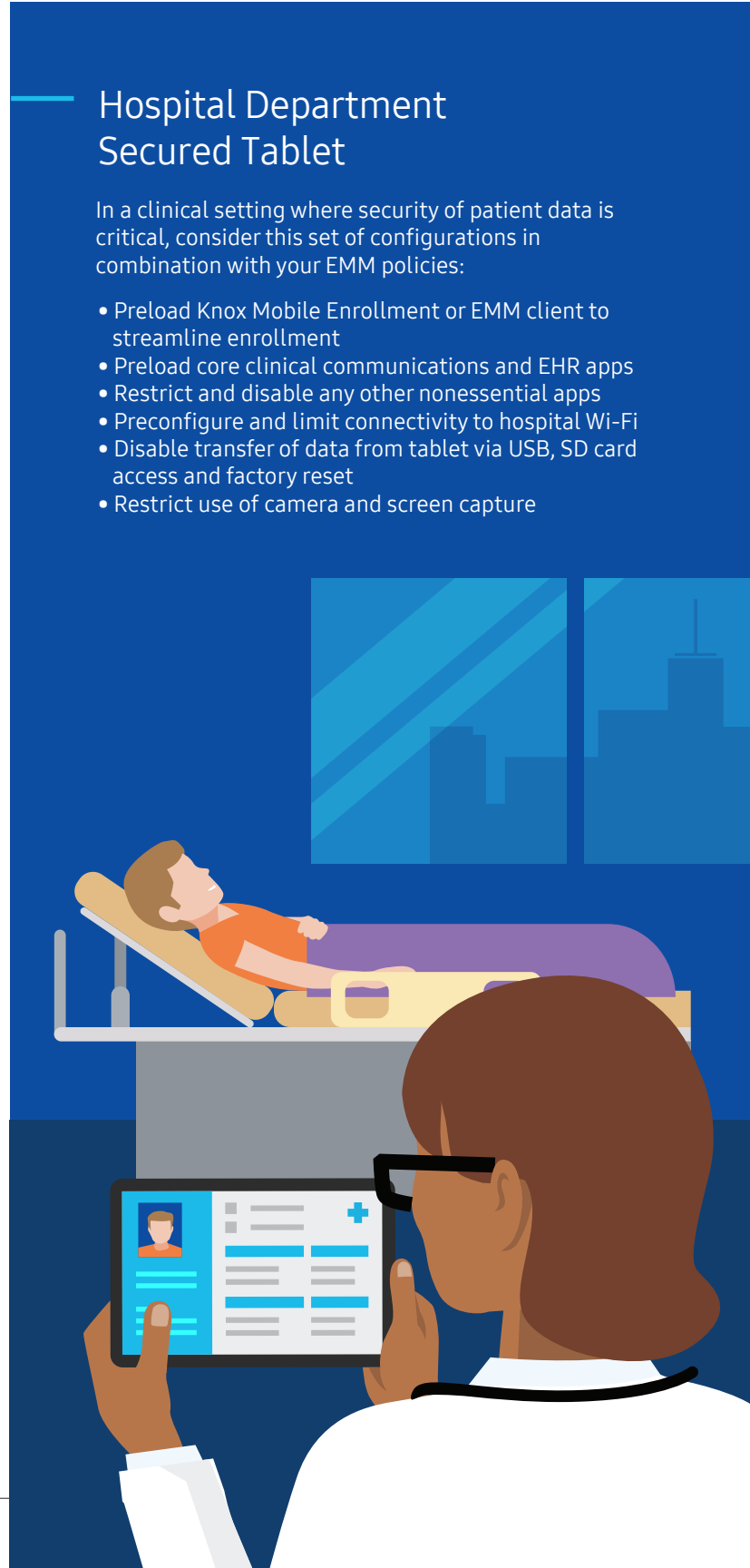
Although Knox Configure controls many of Samsung's and Android's underlying security features, Enterprise Tablets are often also enrolled into the organization's MDM/EMM tool as well as Knox Configure. In these environments, Samsung's Knox Mobile Enrollment takes the next step from Knox Configure by loading the MDM/EMM client software and launching it so the end user (or deployment team) can add the new device to the MDM/EMM system — which then finishes configuration so the tablet is ready to go.

IT managers can use their own EMM/MDM console as well as the Knox Configure dashboard to help in reporting compliance. As soon as a profile change requires device updates, Knox Configure starts reporting how many devices need the update, which ones are not compliant and the reasons why — such as a user cancelling an update. Knox Configure also logs profile changes and updates so that an audit trail, tied to each individual user, is always available.

Hospital Department Secured Tablet

In a clinical setting where security of patient data is critical, consider this set of configurations in combination with your EMM policies:

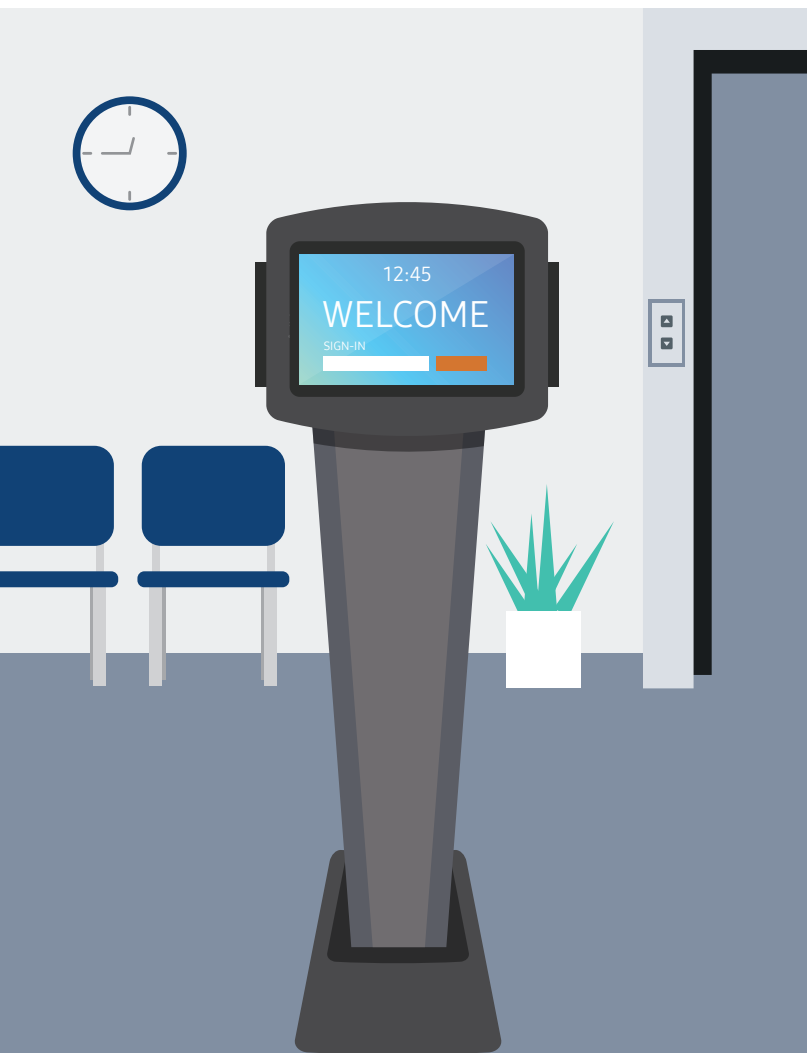
- Preload Knox Mobile Enrollment or EMM client to streamline enrollment
- Preload core clinical communications and EHR apps
- Restrict and disable any other nonessential apps
- Preconfigure and limit connectivity to hospital Wi-Fi
- Disable transfer of data from tablet via USB, SD card access and factory reset
- Restrict use of camera and screen capture



4 Digital Kiosks

Sometimes the line between a kiosk and a restricted tablet isn't completely clear. Generally, kiosk mode restricts a tablet to running a single application (or set of applications), limits the ability of the end user to change settings on the device, and hides some of the notification and status information about the tablet. For example, the traditional status bar at the top of the screen might be removed or autorotation might be disabled. With Knox Configure, a profile can be designated as "ProKiosk," which guides the IT manager through settings that create a locked-down device.

Although kiosk applications are available for managing tablets, Knox Configure's ProKiosk solution has the advantage that it can dive into the hardware in a way that may not be supported in the general Android APIs or even a standard Knox Configure profile.



Major ProKiosk-Specific Settings



User Experience

Kiosk application; hiding notifications and status bars; passcodes to exit kiosk mode; hiding different setting options and power/restart options or even the entire settings menu; blocking "hardware" keys (such as the home button or volume)



Applications and OS Controls

Enrollment restrictions (skipping setup for Google; Samsung and carriers); application installation; updating whitelists and blocklists



Connectivity

Restrict send/receive SMS, roaming and tethering features; control screen capture; disable different connectivity modes (in addition to setting up profiles); special APNs to separate enterprise billing from personal bills per application



Security

URL whitelists and blocklists; blocking screen capture, microphones, audio recording, clipboard; disabling different types of biometric authentication and password viewing from the lock screen

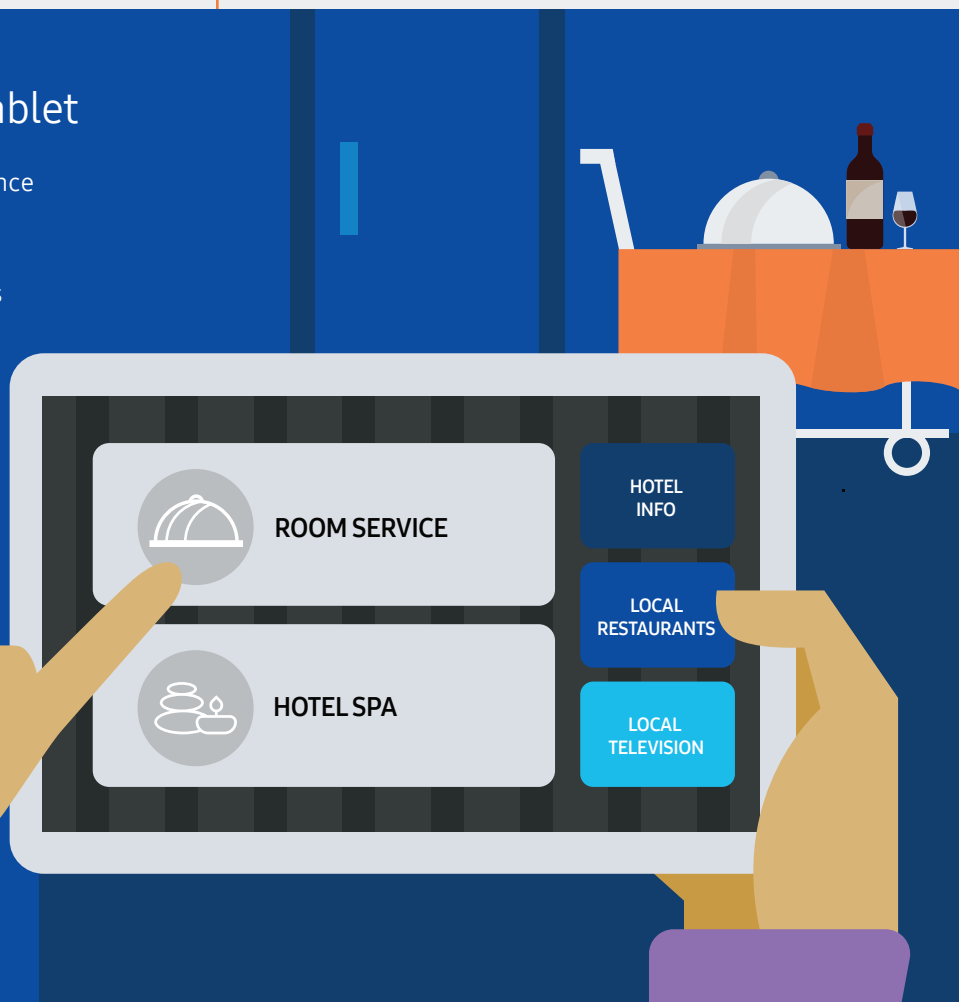
Does ProKiosk Mode Fit Your Usage Objectives?

Usage Criteria	Kiosk Mode Pros and Cons
Will the tablet be used by untrained end users, such as customers in a retail environment?	Kiosk mode reduces the likelihood of a user accidentally or intentionally “breaking” the tablet, avoiding rebuilds that take a device out of service or interrupt operations.
Will the tablet be permanently mounted and not movable, such as a product information display?	Kiosk mode helps ensure that the device is running the correct application at all times and is ready to go when users need it.
Will the tablet run more than one application, such as in a field service environment?	Kiosk mode may be unnecessarily restrictive, keeping the end user from taking advantage of Android tablet features.
Will the tablet be used exclusively to display information, without any user data input, such as in a signage or guided tour application?	Kiosk mode can streamline device booting and keep the display and application functioning as intended for best performance and user experience.

In-Room Hotel Concierge Tablet

An in-room tablet to improve guest experience could be enhanced with the following configurations in ProKiosk mode:

- Preload your guest services app and set as home screen
- Require a passcode to exit ProKiosk mode
- Hide standard device status bar and notification messages
- Disable power off and volume controls
- Set a branded lock screen wallpaper
- Set screen timeout to 60 seconds and disable screen rotation
- Preconfigure to Wi-Fi network



Create Your Customized Tablet Experience

For businesses pursuing digital transformation, tablets offer an ideal platform for streamlining workflows, empowering workers and better engaging customers.

Tools like Knox Configure give IT managers and line of business leaders the ability to customize tablets to meet their specific needs, while enhancing data security and simplifying user experiences. Knox Configure is a solution designed for device customization at scale for any size of mobile fleet, offering significant time-saving benefits.

How do you get started?

Take advantage of the Knox Configure free trial:

Sign up for a free trial of Knox Configure to understand its full capabilities and how they can support your objectives.

[Learn more](#)

Get help from Samsung Business Services:

For complex or time-sensitive projects, reach out to Samsung Business Services or get in touch with a Samsung reseller partner for expert help.

[Learn more](#)

Choose the right tablet:

Samsung's Galaxy tablet portfolio offers a wide variety of options, from affordable models to high-end, productivity tools that address a multitude of business needs. Tablets come in a range of sizes, from a compact 7-in. up to 10.5-in., and include rugged options such as the Galaxy Tab Active2.

[See the full portfolio](#)

© 2019 Samsung Electronics America, Inc. All rights reserved. Samsung is a registered trademark of Samsung Electronics Co., Ltd. All products, logos and brand names are trademarks or registered trademarks of their respective companies. This white paper is for informational purposes only. Samsung makes no warranties, express or implied, in this white paper.

Learn more: samsung.com/knox | insights.samsung.com | 1-866-SAM4BIZ

Follow us: [youtube.com/samsungbizusa](https://www.youtube.com/samsungbizusa) | [@samsungbizusa](https://twitter.com/samsungbizusa)

SAMSUNG