Samsung Electronics America, Inc.
Enterprise Business Division
85 Challenger Road
Ridgefield Park, NJ 07660
201-229-4000
samsung.com/printer

SAMSUNG BUSINESS

Subject: Samsung Printing Security Guide for: MX7, MX4, M4583, M4580, M5370 series

When Samsung introduced the Smart UX Center, the industry's first Android-based user interface for printers, we brought a new printing paradigm with unparalleled usability and convenience. One way we achieved this was with the intuitive user interface design, familiar to smartphone and tablet users. Another key achievement was the unlimited possibility of expanding existing printer functions with apps and widgets.

While some are hesitant to fully utilize the Smart UX Center due to its Android platform, "Android" does not translate to a lack of security. The Smart UX Center **only provides "user experience "**and operates in a framework of robust, multi-layered security features and user access control settings that protect data. Here's a close look at how security works in the Smart UX Center.

Samsung Electronics America, Inc.
Enterprise Business Division
85 Challenger Road
Ridgefield Park, NJ 07660
201-229-4000
samsung.com/printer

System Security

Printer systems equipped with the Smart UX Center are composed of two platforms: the Android UI platform (closed platform) and the main internal system platform (**Samsung Propriety Firmware)**. The UI platform runs the GUI (graphics user interface), providing users with that intuitive experience of smart "touch" operation, while the latter stores print and user data which is **completely separate from the UI platform** .

The two platforms communicate with each other, but the only direct access that the UI platform has to the main system platform is through the Smart UX Center's special folder. All other data stored in the main system platform is encrypted, and requires decryption every time the UI platform requests permission. The UI platform's communication with other network devices (PCs, servers) is possible only through the **internal**, secure, main system network.

Samsung Electronics America, Inc.
Enterprise Business Division
85 Challenger Road
Ridgefield Park, NJ 07660
201-229-4000
samsung.com/printer

User Interface Security

Security risks associated with an Android platform can arise from unapproved writing of unverified data. The Smart UX Center is protected from this risk in two ways: a rigorous quality assurance process at Samsung, and user control over Smart UX Center settings.

Samsung's Security QA Process

Official apps and widgets provided in-house or by our partners undergo a multi-step QA process before registration for quality and security verification. Only the ones that pass our software quality engineering (SQE) process are registered on our authorized Samsung Printing App Center channel and recommended for our customer to use.

Firmware updates are guaranteed secure as well. The only way to update the Smart UX Center's firmware is with the official Samsung upgrade, which goes through user authentication and signature verification. This eliminates the possibility of hacking through firmware attacks.

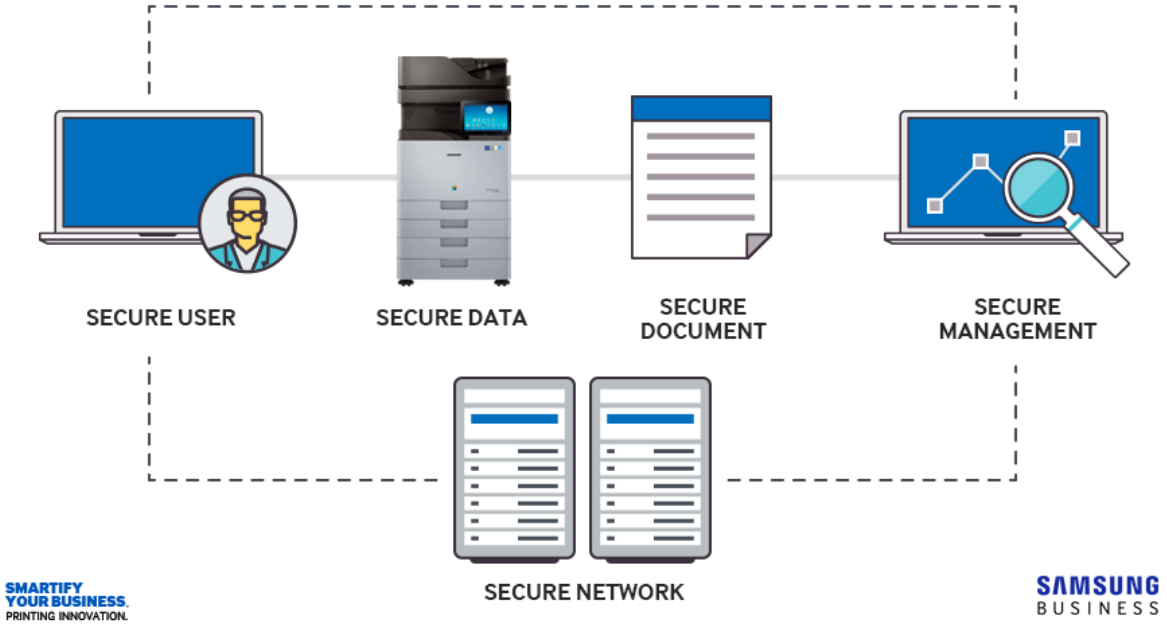
User Control – Administrative Settings

The Smart UX Center settings can be configured to only give the administrator the authority to install or remove apps, thereby regulating installation of third party apps. To further tighten security, the administrator can choose to block USB memory access including installation via USB, or disable app installation via all routes by any user, including the administrator himself. The administrator can also limit users' browser usage.

Samsung Electronics America, Inc.
Enterprise Business Division
85 Challenger Road
Ridgefield Park, NJ 07660
201-229-4000
samsung.com/printer

The Samsung Security Framework

All Samsung Printing Solutions products operate within the multi-layered Samsung Security Framework, built to protect information throughout the document life cycle, from all the way from data encryption to document management.



The Five Components of the Security Framework

- ***Secure User*** This feature includes authentication, authorization, and accounting to limit MFP access to verified users, assign varying levels of access, and keep track of MFP usage data by device, group, or individual users, respectively.
- ***Secure Data*** Data that stays in or passes through the MFP is protected with encryption and hard drive image overwrite technology.
- ***Secure Network*** Only the devices connected to the authorized network have access to the MFP with industry-standard TLS/SSL protocols, IP security, and network security protocols.
- ***Secure Document*** One of the primary features of this feature is password assignment to individual print jobs, ensuring safe and authorized delivery of printouts and faxes.
- ***Secure Management*** With the job auditing feature, the administrator can track events and actions for logged-in users including data requests, changes made to security audit functions, image overwrite results, and inquiries/changes to the security audit configuration. System backups ensure quick data recovery in case of loss.