M600 Security Overview

The M600 incorporates physical security, software security, and payment security features.

M600 device

BIOS

Setting	Description
Password	All access to the BIOS is password-protected, including all access via a function key.
USB Booting	Disabled

Software and Image

The operating system and software reside on a single solid-state drive (SSD) within the M600.

Setting	Description
Operating System	Windows 10 IoT Enterprise, containing minimum OS components for the application.
Safe Mode	Booting to Windows Safe Mode has been disabled in the embedded image.
Image Integrity	Operating System partition is 'frozen' in a read-only state using Microsoft's Unified Write Filter (UWF). Any changes to the registry or files on this partition are made in memory only and are not written to the disk. On the next reboot, the device is restored to the known 'frozen' image on the OS partition. The M600 is configured to automatically restart daily.
Firewall	Microsoft Firewall is enabled to block all incoming ports, except ping.
Logon Shell	The default Explorer logon shell has been replaced with an EFI application. There is no desktop, taskbar, or Start Menu. In addition, Task Manager has been disabled.
Keyboard Access	Disabled
USB Drive	The USB drive (aka USB flash drive) is mounted as a read-only device at the OS level. Write access is only enabled when scan-to-USB is used.
Auto-Launch	Disabled
Other USB Devices	Disabled through removal of all USB drivers from the OS, except mass storage (i.e. USB flash drive) and internal USB devices identified by unique device ID. In addition, a filter will actively monitor and remove any unauthorized USB devices that appear.
Remote Access	None
Anti-Spyware	Windows Defender is installed and running.

Physical - Inside Locked Compartment

Port	Description
Network	Ethernet connection to the store network. Microsoft Firewall is enabled as follows: • Block all incoming ports, except ping • Block all outbound ports from all applications, except the EFI client applications WiFi and Bluetooth are not present.
Copier	Foreign Interface connection, used for copy interface to the MFP.
Client	Additional Ethernet connection, used only for 'direct printing' where the printer is connected directly to this Ethernet port.
USB1/USB2	Allows certified card terminals only. Additional USB devices are disabled within the OS.
Serial	RS-232 port, used for copy with Vendor 2 interface only.

Payment security

The M600 device processes credit cards using a validated point-to-point encryption (P2PE) solution. A P2PE solution is defined by the PCI Security Standards council as follows:

"A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI-approved point-of-interaction (POI) device through to decryption, assessed in accordance with PCI's P2PE standard and included on PCI's list of Validated P2PE Solutions."[1]

The M600 uses as its POI a card terminal that is PCI PTS certified, ensuring secure data management and secure electronic transactions. The card terminal encrypts credit card data when the card is inserted or swiped, and the data remains encrypted until it reaches the P2PE solution provider's gateway for processing.

The M600 does not require PA-DSS validation.

References:

https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf

https://www.pcisecuritystandards.org/documents/P2PE_Program_Guide_v2.0.pdf

https://www.pcisecuritystandards.org/documents/PCI_PED_General_FAQs.pdf

[1] *PCI P2PE Glossary of Terms, Abbreviations, and Acronyms* Version 2.0, published by the PCI Standards Council, June 2015

Cloud printing and scanning security

Following are the security elements of access to cloud services for printing and scanning from the M600, specifically PrintMe, Box, Dropbox, Google Drive, and OneDrive.

1. **Controlled Workflow:** The user has restricted access to the Internet limited to logging on to their account. All other user interfaces are controlled by the EFI application. The logon credentials are not stored or retained in any way.

2. **File Transfer:** All communication between the M600 and the cloud services is encrypted using TLS 1.2, including the file download and upload.

3. **File Storage:** The document is temporarily stored on the M600 during the customer's session. The document is securely deleted from the M600 at the end of the session.