

MFP Security Overview



Introduction

Multifunction Printers (MFPs) are complex network devices that require careful consideration regarding security. Samsung's printing and networking products include a wide array of security related features. This document discusses those features and provides an overview of their benefits and their implementation.

Any device that is placed on a network must be evaluated with respect to security. How does the device protect itself from unauthorized access? Does the device expose the network to any form of vulnerability? What sort of information does the device process, and what are the security considerations related to that data? These and many other questions are appropriate to ask of any networked device, including networked printers.

Networked printers operate independently on the network and can be focal points for sensitive information. Securing them is sometimes comparable to securing other conventional networked devices such as computers: the need for controlled network access and the need for secure remote management are largely the same for printers and workstations. In other areas, the security considerations around printers are substantially different: they generally don't run conventional operating systems, they don't have network file shares that need to be secured, they probably don't need or support antivirus software, etc.

This document will define the major areas of security concerns related to printers, and provide an overview of the Samsung printer security features that allow these devices to be deployed, managed and used in a secure manner.

Security Policy

Samsung security policies are based on industry standard requirements set forth by several regulatory organizations. By using the guidelines from these organizations, Samsung has developed a set of security goals that meet the standardized security requirements and the needs of Samsung customers.

Regulatory Standards

The following are regulatory standards that are used to provide security guidelines:

- Common Criteria
- FIPS 140-2
- HIPPA
- SOX
- GLBA
- IEEE Std 2600™ 2008
- DoD 5200.28-M

Security Goals

The Samsung MFPs use standard security protocols to protect assets such as image files, stored documents, system audits, and Samsung MFP configuration data. The following are descriptions of the various assets that require security.

Components on the Internal Network

Components of the internal network include the user's PC, web administrator's PC, and the authentication servers. Malicious attacks on the internal network can be attempted through a networked Samsung MFP, which could have devastating results on the customer's internal network components. For this reason the Samsung MFPs must be capable of withstanding malicious attacks on the network.

File Preservation

Samsung MFP users save files on the MFP hard drive for future work. An attacker will want to access these files. For this reason MFP hard drive files must be protected from unauthorized external access.

System Audit Logs

The Samsung MFP system audit logs include system security information. Because attackers can use this information to gain access to the secured systems on the MFP, the system audit logs must be securely protected.

Image Files

An image file from copying, printing, faxing, or scanning may include important information that a client does not want to disclose. For this reason the image files must be securely protected.

Samsung MFP Configuration Data

If a hacker were to acquire Samsung MFP configuration data, which includes the Samsung MFP security, the Samsung MFP should be able to be compromised. System administrators must securely protect the Samsung MFP configuration data.

User Roles

Users can be divided into two categories: administrator and general user. The role of each user is as follows:

Administrator

- Local administrator
 - The local administrator role manages the Samsung MFP through a local user interface. The tasks performed by this role include confirming MFP status information and setting system configurations. Moreover, local administrators activate or deactivate *Immediate Image Overwrite* (IIO) and *On Demand Image Overwrite* (ODIO), start or stop ODIO, and change PINs for security.
- Web administrator
 - The web administrator role manages the web site (embedded in the Samsung MFP) by using the web user interface. This role performs the following:
 - Creates, modifies, or deletes NetScan service user accounts.
 - Modifies web administrator accounts and passwords.
 - Activates or deactivates security audit.
 - Downloads the security audit log.

General User

The general user accesses the Samsung MFP through the Local User Interface (LUI) or the user's PC. From the local user interface, users can perform copy, fax, or scan jobs. From the user's PC, the user can access the Samsung MFP from the internal network and print documents. When using SmarThru Office, the user can also scan.

A user granted network scanning privileges can perform scan jobs through the local user interface. Network scanning services include scan-to-email, scan-to-server, and scan-to-network.

When a user stores documents as Secured, the user who stores the document via client PC can assign PIN to the document. The PIN should not be exposed to others. When accessing the file, the user must get permission by entering the PIN through LUI and then access to the file.

Samsung MFP Models with Security Features

The following Samsung MFPs use the latest security features:

- SCX-5635FN - Black and White MFP
- MultiXpress 6545N - Black and White MFP
- MultiXpress 6555N - Black and White MFP
- CLX-6240FX - Color MFP
- MultiXpress C8380ND - Color MFP

User Access Control

One of the primary security features for any device is access control. Samsung MFPs employ system authentication and network authentication access control mechanisms.

System Authentication

The MFP requires the system administrator to enter authentication before permitting access to the system management items. System administrators include SyncThru™ Web Service administrators and the local system administrators. The authentication process for the SyncThru™ Web Service administrator uses an account and a password on the user interface, the authentication process for the local MFP system administrator uses a PIN number on the MFP user interface.

The system administrator must enter a PIN to access the system administration functions. The SyncThru™ Web Service administrator must enter their account and password in to the SyncThru™ Web Service UI, and the local administrator must type their PIN number in to the MFP UI. The security software displays asterisks instead of characters to hide what they enter.

The authentication process will be delayed at the MFP UI for three minutes when 3 wrong PINs are entered in succession. When 3 wrong PINs are entered in the SyncThru™ Web Service UI from one particular browser session, the security software will send an error message to the browser session screen.

Network Authentication

The Samsung MFP prevents unauthorized use of the installed network options (network scanning, scan-to-email, and scan-to-server); the network options available are determined by the system administrator. To access a network service, the user is required to provide a user name and password, which is then validated by the designated authentication server.

Overview

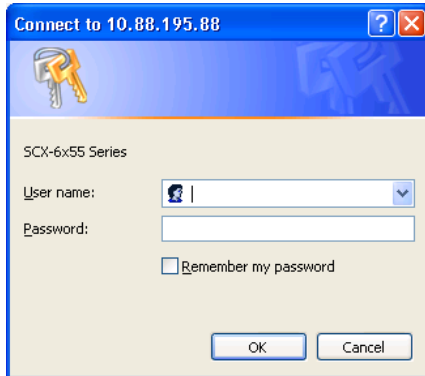
User Authentication can protect MFP from unauthenticated user access. Un-authenticated users can see the basic status of the MFP, but cannot configure MFP settings. It needs to authenticate users that users want to change MFP's settings or to use functions like Copy, Fax, Scan and Printing. User Authentication can be configured by Local Authentication or LDAP Authentication.

Details

When User Authentication is enabled, Copy, Fax, Scan, and Printing functions require a user account.



When User Authentication is enabled, modifying printer settings or viewing printer configuration requires a user account through SWS (Samsung Web SyncThru).



Local Authentication

The user password can be up to 15 characters in length, and it can include alphabetic, numeric and special characters. The password complexity consists of upper case letters, lower case letters, numbers and special characters.

LDAP Authentication

LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

User Data Protection

It is no longer surprising to find MFPs/Printers equipped with hard drives. The hard drive stores various types of hardcopy information such as: user information, copy/scan/fax/print images from processed jobs, and device logs. Some or all of the information on the hard drive needs to be protected securely. Hard drive overwriting technology (eShredding) and encryption are the safest mechanisms available to achieve this goal.

Encryption

To protect confidentiality of data stored on a computer disk, disk encryption is used. Although you have a device that is equipped with a HDD wiping protocol, the data on the HDD is still written in plain text which makes it available for everyone to read. In order to prevent this, HDD encryption is required.

Samsung MFP protects data by using encryption technology, especially AES-128. The following table lists types of data that potentially require encryption.

Feature	Description	Encryption
User credential	Account information for each user	Yes
Logs	Audit, Job, LDAP, and other logs	Yes
Printing	Spoiled Printing image	Yes
Scan	Scan job template	Yes
Email	Connectivity logs and address book	Yes
Fax	Fax Tx/Rx, mail box, and Phonebook	Yes
MIB	Certification	Yes
Fault History	Fault History	No

eShredding

To remove data from a hard drive completely, you must degauss the drive with a powerful magnet. Another method used to protect hard drive data from being recovered is to physically shred the hard drive. These are both methods used to protect hard drive data from recovery when a hard drive device is removed from a secure location. Deleting files or formatting the drive is not sufficient to delete files in a secure manner. Even if you delete files or format the hard drive, information on the hard drive is still recoverable by an advanced tool.

When a hard drive device remains in a secure location, a triple overwrite algorithm is used to electronically shred the data. The triple overwrite algorithm is used because it takes more than two overwrite operations to ensure that information is no longer recoverable.

The eShredding feature overwrites files created during print, scan service, copy, and fax by using the triple overwrite algorithm. This process is implemented in accordance with DoD 5220.28-M and will be activated at the completion of each copy (landscape/stapled type only), print, network scan, or scan to e-mail jobs, whenever the MFP is turned back on after power failure, and *on demand* when executed by the MFP system administrator.

Secure Print

Print data may be one of the most overlooked areas when it comes to network security. Printed jobs routinely contain sensitive information—financial data, information that personally identifies customers or employees, account information, etc. Printers are commonly located in high-traffic areas with only basic physical security. In this environment, it's very easy for printed information to end up in the wrong hands, either accidentally or intentionally. Samsung printers include standard features that can substantially reduce this vulnerability.

The Confidential Print feature addresses the basic concern of printed pages lying on the printer for anyone to pick up. With Confidential Print, the printer holds submitted jobs until the intended recipient is present at the device. By producing the printed job only when the proper PIN code is entered on the printer's operator panel, the job is delivered securely into the right hands.

User Data Access Control

Documents stored on the MFP can be stored using a public method or a secured method.

Public Method

A document stored using the Public option allows all users to access and use the file.

Secured Method

A document stored using the Secured option restricts access to only the user who stored the file.

During storage, the user must create a PIN number for accessing the file. Later, when the user wants to access the file, they must enter the correct PIN number or the MFP denies access.

Network Security

HTTPS

HTTP is an easy and general method for management of network devices. It supports most MFP configurations including network configurations. But network data including the administrator's information can be acquired through sniffing the network traffic.

HTTPS protects network data without using encryption. When HTTPS is enabled, user connections are redirected into HTTPS automatically.

HTTPS ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

The connection uses port 443 (unsecured HTTP typically uses port 80).

For HTTPS to work, key pairs of a Public Key and a Private Key are necessary. They can be generated by the following methods:

- Self Signed Certificate: Machine generates Public Key and Private Key pair through RSA algorithm and signed by itself.
- Certificate Signing Request: Machine generates Public Key and Private Key pair through RSA algorithm and requests to sign by a certificate authority (CA).

Machine Digital Signatures are generated by using these algorithms.

SNMPv3

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMPv3 is not a stand-alone replacement for SNMPv1 and/or SNMPv2. SNMPv3 is SNMPv2 plus security and administration.

SNMPv3 security features support authentication and encryption. SNMPv3 used on Samsung MFPs can support authentication by using the MD5 or SHA algorithm and can support one account to read and write. Samsung MFPs with SNMPv3 can support encryption by using the DES algorithm.

IP Security (IPSec): IPv4, IPv6

IPSec is an important element between the other network nodes in IP communication. It supports authenticating and encrypting IP packets between network devices using IPv4 or IPv6. IPSec is used widely without upper layer security protocols like TLS/SSL or SSH because of the existing layer 3 based on the OSI layer. When IPSec is used between a user PC and an MFP, print job security and scan job security can be enhanced. When IPSec is used between the Administrator and an MFP, management data security can be enhanced. IPSec can be used to protect IP-based network traffic.

IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

IPSec uses two protocols to provide traffic security – Authentication Header (AH) and Encapsulating Security Payload (ESP). Both protocols are described in more detail in their respective Internet Society™ RFCs:

- 4302 - IP Authentication Header
- 4835 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)

IPSec supports only pre-shared key method for IPSec authentication. Users can setup pre-shared key values through a Web server.

IKE protocol is used in order to establish and manage Security Association (SA) between a printer and a user node in AH and ESP service.

In IPSec and IKE protocol, the supporting algorithms are:

- Diffie-Hellman algorithm : modp 768, modp 1024, modp 1536, modp 2048, modp 3072, modp 4096, modp 6144 and modp 8192
- Hash algorithm : MD5 and SHA1
- Encryption algorithm : DES, 3DES, AES128, AES192, AES256, CAST and Blowfish
- Integrity algorithm : MD5 and SHA1

802.1x Support: MultiXpress 6555N Model Only

802.1x network security is a protocol to authenticate network access for 802.1x enabled port. Generally it is used in wireless security communication. Wired communication also is used in a 802.1x enabled port. A switch network device called 'Authenticator' requires the 802.1x authentication to be connected to the MFP and that the MFP responds with its credentials. The authenticator transfers the MFP's credentials to a authentication server called 'RADIUS' and finally RADIUS decides whether to permit the connection or not.

802.1x security adopts some Extensible Authentication Protocols (EAP), Samsung MFPs support the following EAPs:

- EAP-MD5
- PEAPv0
- EAP-MSCHAPv2

Server Certificate Validation is not supported. Each EAP requires a user ID and Password as a credential.

Protocol/Port Management

Protocol Management can select whether a network protocol is used or not. According to a user's network policy, some protocols can be disabled and this can protect an MFP from an external network attack like a port scan. Additionally it can reduce network traffic.

Samsung MFPs can support Protocol Management for the following protocols:

- EtherTalk
- FTP
- HTTP/HTTPS
- IPP
- LPD
- mDNS
- Network Scan
- Raw TCP/IP Printing
- SETIP
- SLP
- SMB
- SMTP
- SNMP
- SNMPv3
- Telnet
- T4Net
- UPnP
- WINS

IP Filtering

Samsung MFPs can support IP Filtering to configure available IP Address Ranges. Only registered IP devices can print or scan through a network. Samsung MFPs support IPv4 Filtering and IPv6 Filtering. This can protect MFPs from unknown network devices.

Samsung MFPs can support 10 IPv4 Address ranges and 10 IPv6 Address ranges.

Network/Fax Separation

Samsung MFPs use RAM memory to store data. The memory is divided into fax memory that the fax board can only access and network memory that only the network port in main control board can only access. Separation between the PSTN port on the FAX board and the network port on the main controller board is established through the architectural design of the main controller software. Samsung MFPs control and restrict the information flow between the fax board and the network port in main controller. Direct communication between a client PC and the fax modem through the internal network is impossible; the communication can only be passed through the Samsung MFP. Using the fax-to-email function, the fax image is received from the PSTN line and is translated and sent through the internal network. The fax image received from the PSTN line is stored first in the MFP fax memory, and then the data goes through a verification process. When the fax image data is standardized with MMR, MR, or MH of T.4 specification, the Samsung MFP copies the data to network memory. Then the fax image can be transmitted to the SMTP server through the network card. All data received sent to the internal network has been verified by the MFP, it does not threat or modify Samsung MFP component of the internal network.

Security Management

Security Function Control

The MFP security management features allow authorized administrators to manage the MFP security features locally or remotely.

Local administrators can manage the following security features:

- Enable or disable security functions
- Start or stop security functions
- Change the local administrator PIN

Remote administrators using SyncThru™ Web Service can manage the following security features when using local certification in network scan service authentication:

- Create/Change/Delete user account for network scan service.
- Configure the authentication option for the network scan service (*No Authentication, Require Network Authentication, or Require Local Authentication*)
- Enable or disable Security Functions
- Change the local administrator's name and password.
- Enable or disable system audit logs.
- Download system audit report.

Managing Security Data

The MFP security management features allow authorized administrators to manage the MFP security data locally or remotely.

Local administrators can manage the following security data:

- Authentication data for local administrators
- Configuration data for security functions

Remote SyncThru™ Web Service administrators can manage the following security data:

- Authentication data for web administrators.
- Configuration data for enabling or disabling system audit logs.
- Configuration data about network security.
- System audit logs.
- User information for network authentication service

Audit Log

The Samsung MFP tracks events/actions (e.g., print/scan/fax job submission) for login users. Audit logs are created for each event in fixed size. Each audit log provides the user's identification, event number, date, time, ID, description, and data. The audit logs are available to web administrators and can be exported for viewing and analysis by using the web user interface.

Table : Security Events

Event ID	Event Explanation	Input Data
Audit log consists of the following fixed-size input data. <ul style="list-style-type: none"> Input Number (An integer number from 1 to the number of log data) Event Date (mm/dd/yyyy) Event Time (hh:mm:ss) Event ID (Specific number – Refer to the following table) 		
1	System startup	Device name, Serial number of the device
2	System shutdown	Device name, Serial number of the device
3	ODIO started	Device name, Serial number of the device
4	ODIO complete	Device name, Serial number of the device, Completion status
5	Print Job	Job name, User name, Completion status, I/O job status, SyncThru user's account
6	Network scan job	Job name, User name, Completion status, I/O job status, SyncThru user's account, total number of the destination address, Destination address
7	Server fax job	Job name, User name, Completion status, I/O job status, SyncThru user's account, Total number of the fax number to receive , Fax number to receive, Destination address
8	IFAX	The Samsung MFP does not support this function.
9	Scan-to-email job	Job name, User name, Completion status, I/O job status, SyncThru user's account, Total number of SMTP receiver , SMTP receiver
10	Audit Log Disabled	Device name, Serial number of the device
11	Audit Log Enabled	Device name, Serial number of the device
12	Copy job	Job name, User name, Completion status, I/O job status, SyncThru user's account
13	Embedded fax job	Job Type (Sending fax, Receiving fax), Job name, User name, Completion status, I/O job status, SyncThru user's account, Total number of the fax number to receive , Fax number to receive, Destination address
14	PC-Fax job	Job name, User name, Completion status, I/O job status, SyncThru user's account, Total number of the fax number to receive , Fax number to receive, Destination address

The audit log traces decisions that allow requested data flow, changes about security audit function, image overwriting start/completion, inquiry/change about security audit configuration, and recovery from failure of image overwriting job. Because the audit records are only available to the authorized web administrators, unauthorized users cannot change or delete them. Audit records can be downloaded by using the Web interface for viewing and analysis. When storage is full of log data, the latest records overwrite the oldest audit records.

Summary

Printer security is about protecting the printers, the network and the data that is involved in the use of the printers. Printer security is a complex issue with many elements to consider.

Samsung's printers are equipped with an array of security features that allow you to secure networked printer devices and their use. These features include the following:

- Samsung printers can be managed securely with device passwords, HTTPS, SNMPv3, and IPSec
- Samsung printers can be hardened with Port control, Protocol control and Hard Drive Encryption
- Samsung printers support secure printing through Secure Print and IPSec

About Samsung Electronics America, Information Technology Division

Samsung's Information Technology Division (ITD) markets the award-winning line of Samsung printers including; black & white laser printers, black & white multifunction printers, color laser printers, and color multifunction printers. Samsung ITD is committed to supporting the needs of its channel partners in the professional, commercial, corporate, and small/home markets. ITD is a division of Samsung Electronics America (SEA), a U.S. subsidiary of Samsung Electronics Company, Ltd. (SEC). The SEA organization oversees the North American operations of Samsung, including Samsung Telecommunications America, LP, Samsung Electronics Canada, Inc. and Samsung Electronics Mexico, Inc. For more information, please visit www.samsung.com, or call 1-800-SAMSUNG.

About Samsung Electronics

Samsung Electronics Co., Ltd. is a global leader in semiconductor, telecommunication, digital media and digital convergence technologies with 2007 consolidated sales of \$103.4 billion. Employing approximately 150,000 people in 134 offices in 62 countries, the company consists of five main business units: Digital Media Business, LCD Business, Semiconductor Business, Telecommunication Business and Digital Appliance Business. Recognized as one of the fastest growing global brands, Samsung Electronics is a leading producer of digital TVs, memory chips, mobile phones and TFT-LCDs. For more information, please visit www.samsung.com.



Samsung MultiXpress C8380ND

For more information, please visit www.samsung.com

Printing solutions
as easy as



WP_MSO_Rev0A, 17 April 2009