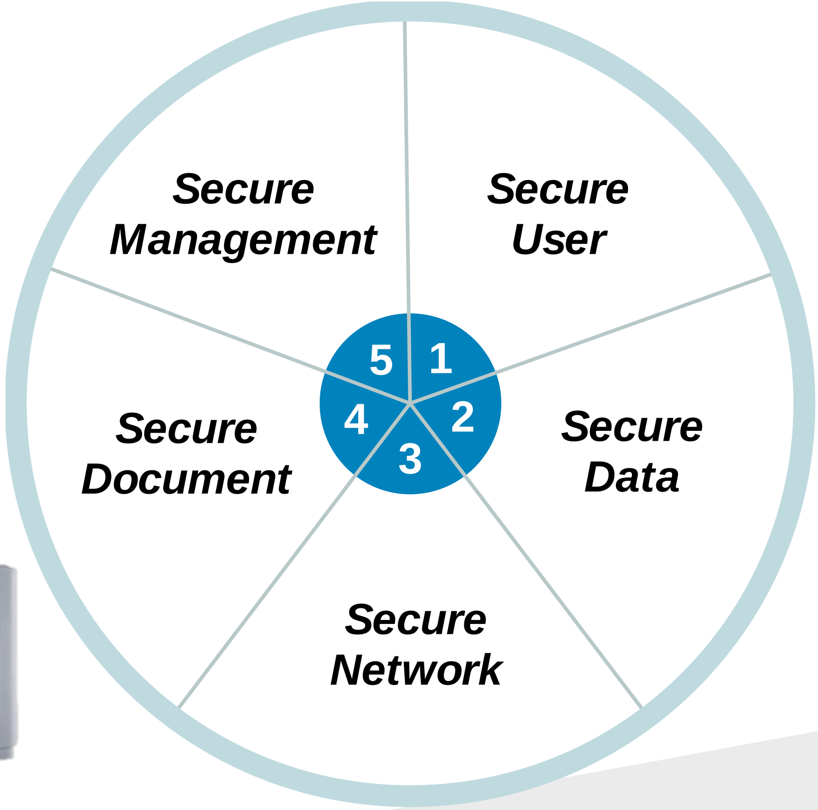
Samsung MFP Security

White Paper: Samsung Security Framework



© 2015 Samsung Electronics Co., Ltd. All rights reserved.

Samsung Electronics provides this guide for information purposes only. All information included herein is subject to change without notice.

Samsung Electronics is not responsible for any direct or indirect damages that may occur when you use this guide or that you relate to the use of this guide.

Samsung and Samsung logo are trademarks of Samsung Electronics Co., Ltd.

All other brand or product names are trademarks of their respective companies or organizations.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Table of Contents

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Introduction

Securing valuable information was an easy process back in the early days of computing. All of the data was kept on tapes and disks, which were not accessible to anybody outside of the building. However, now with networks connecting everything to the outside world, security leaks can occur anywhere.

IT professionals are faced with managing an assortment of devices that can allow security breaches. This overwhelming burden of device management has led IT managers to demand better security features from the manufacturers of the devices they use.

Samsung has responded to the requests from our IT customers and created MFP security features that protect valuable data from unauthorized access.

1.1 Information Security

In our digital information-based society, we have become more aware of the perils associated with sharing information. In the name of productivity we have created increasingly easier ways to share information, at faster speeds and with higher bandwidth. The downside to this increase in share is the decrease in our ability to secure our information. Search engines and sniffers are constantly monitoring networks for information, usually for innocuous purposes, but sometimes the reasons are malicious.

To address this situation we need to understand the path information travels and then we can identify the vulnerabilities the information can encounter. A simple path is one that uses a single connection such as the path from a computer to a printer:

A complex path can include several connections over various wired and wireless networks such as sending an email from a cell phone to several distant locations.

In the Information Technology field, our goal is to make information highly available, but only to the desired recipients. The tools we use to achieve this goal include data encryption and user authentication.

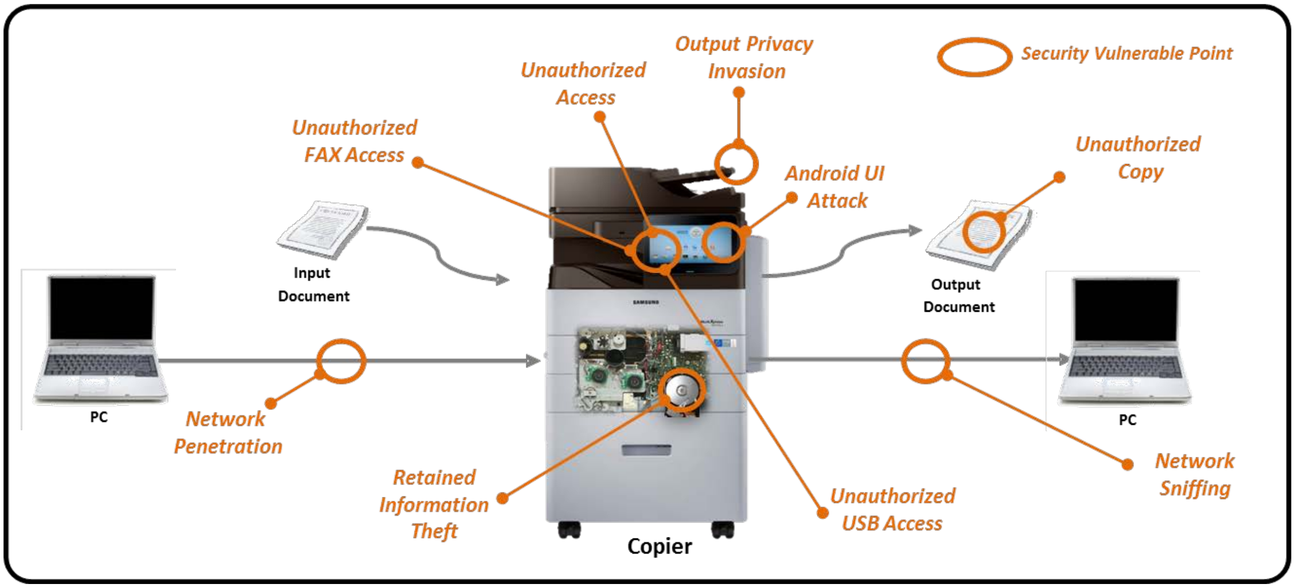
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

1.2 The Objectives of Multifunction Printer (MFP) Security

Information is a resource that by its nature is most valuable when it is being shared with a group working together to achieve a goal. It is this ability to share information over great distances at the speed of light that has created the technological world we live in today. Unfortunately the creation of so many ways to access information has also resulted in more ways for unauthorized access to information. So the dilemma IT professionals are faced with is "how do I balance high availability of information with high security?"

Many formulas and strategies have been developed to determine the level of security that is required, and the amount of harm that would result from breaches in security. These formulas and strategies are useful for accounting purposes to determine the cost of security. However these accounting tools do not help the IT professional implement security.

Samsung has targeted the MFP security as the area of information security where we can add the most value for our IT customers. MFPs offer many features that processing information electronically and on paper. This means that the security objectives for MFPs must address and target the vulnerabilities of these features.



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

1.2.1 MFP Hardcopy Vulnerability

The primary task of an MFP is to print documents. Printed documents are vulnerable to both unintentional and intentional security breaches. Potential document security issues include the following:

- Unintentional removal
- Paper jams
- Intentional removal
- Copying.

1.2.2 MFP Electronic Vulnerability

The additional tasks an MFP performs (Copy, FAX, Scan, Email, Network, Document Storage), create more opportunities for security breaches. These tasks all share a common process – electronic routing of the information. During this electronic routing, the information can be stored on and transferred through many vulnerable locations on the MFP. These locations can include the following:

- Phone line (FAX)
- Ethernet (network connection)
- Hard Drive (stored documents from fax, email, network, and scan)
- USB.

1.2.3 Common Results of Having an Unsecured MFP

Some of the most common results associated with an unsecured MFP include the following:

- Unauthorized use by a malicious user
- Identity theft
- Stolen information
- Lawsuits from stolen information
- Loss of access
- Loss of productivity.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

2. Security Regulatory Requirements

The importance of the information that flows through private and public devices has resulted in the need for broad regulations to protect this information. Some of these regulations were directly developed to protect information such as medical records. Other regulations are indirect effects from other sources such as the need for document audit trails for SOX financial regulation compliance.

Samsung is continuously working with our industry partners to create compatible MFPs that meet the regulatory requirements of today's information infrastructure. The MFP security features presented in this paper are able to meet or exceed the current regulatory requirements of our customers.

GENERAL REQUIREMENTS	The government puts an emphasis on simplifying processes and improving cross-agency collaboration. To do so, the government employs the latest technologies, while implementing strict regulations.	Financial services have critical issues in IT security because more business is being conducted electronically than ever before.	With innovative technological advances, Healthcare now needs to share important medical data and patient information electronically, creating a major security concern.	Education institutions are adopting the online environment in their service area – applications, class notes, medical records, etc.. This electronic environment is vulnerable to security threats.
EXAMPLES OF INFORMATION SECURITY BREACH CASE	Department of Workforce Development (Indianapolis) accidentally disclosed 4,500 Social Security numbers due to a printing error made by a printing vendor.	At Jax Federal Credit Union, client account numbers and Social Security numbers were accidentally posted on the Internet because the printer did not encrypt the data being transmitted on the network.	California health regulators fined Kaiser Permanente's Bellflower Hospital $250,000 for failing to keep employees from viewing the medical records of a patient.	At Tennessee Tech University, Social security numbers of 990 students have been lost due to a misplaced portable flash drive.
REGULATIONS	**Federal Information Security Management Act of 2002 (FISMA)** requires that all networked devices meet strict information assurance. •**CC-ISO15408** •**FDIC** •**IEEE 2600-2008** •**IEEE 2600.1-2009** •**DoD 5200.2** •**HSPD-12** • Information Technology Management Reform Act of 1996	**For Gramm-Leach-Bliley Act of 1999 (GLBA)** compliance, organizations must complete a risk analysis on their current processes and implement firewalls, user access, monitor printing, and more. • National Institute of Standards and Technology Publication 800	**Health Insurance Portability and Accountability Act of 1996 (HIPAA)** forces all healthcare organizations to uniformly manage data to protect patient information and privacy at all times. • Health Information Technology for Economic and Clinical Health, 2009	**Family Education Rights and Privacy Act (FERPA)** prohibits the disclosure of personally identifiable education information without the written permission of the student or their guardian.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

3. Security Business Requirements

Businesses today are constantly creating new ways to use information. IT professionals have the demanding task of protecting that information from new ways of abuse. The most successful strategy for protecting this information is by implementing best practices for user authorization and to use devices that provide a high level of security.

Samsung MFP devices employ high levels of security to meet or exceed today's business security requirements. We are also working with our business customers to continuously improve our MFP security features.

3.1 Public Sector (Government / Education / Healthcare) Security Requirements

Public sector entities have very specialized security needs. The military must be able to protect sensitive information from foreign interests. Schools need to be able to protect the integrity of their student's grades. Healthcare systems must protect the privacy of their patients.

3.1.1 Government

U.S. government requirements include hard drive overwriting schemes that digitally shred the latent document information from the hard drive of a device. When devices with hard drives are removed from secure sites, the hard drives must be removed and physically destroyed.

Regulatory requirements that require these practices include the following:

- **FISMA**
  This regulation requires a mandatory set of processes that must be followed for all information systems used or operated by a U.S. federal government agency.
- **HSPD-12**
  A common identification standard used to ensure that government facilities and sensitive information stored in networks remain protected.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

3.1.2 Education

Education requirements include protecting data from teachers, students, or other staff who engage in unauthorized behavior, either knowingly or inadvertently. These activities can include: improper storage of passwords, students practicing their hacking abilities, and individuals attempting to access the system to modify their grades. Many of these risks can be avoided by implementing usage policies. These policies can add clarity to the tasks required of the network administrator. The policies should include the following:

- Password Policy
- Acceptable Use Policy
- Anti-Virus Procedures
- Email Policy
- Remote Access Policy
- Encryption Policy
- System Audit Procedures
- Confidentiality and Data Distribution Procedures
- Copyright Compliance Policy.

Regulatory requirements that require these practices include the following:

- **FERPA**
  A federal law that protects the privacy of student education records.
- **FISMA**
  Requires a mandatory set of processes that must be followed for all information systems used or operated by a U.S. federal government agency.
- **HSPD-12**
  A common identification standard used to ensure that government facilities and sensitive information stored in networks remain protected.

3.1.3 Healthcare

The healthcare industry is required to manage highly sensitive and private information for all of the patients in the system. Advances in IT have allowed them to manage this data more efficiently and cost-effectively, and it has allowed patients to be more proactive in managing their personal healthcare data. Now medical records are documented electronically in the exam room, patients can request their records over email, and health records can be accessed online. All of these advances in management, distribution, and storage of health records also make them vulnerable to unauthorized access. Regulations requiring the healthcare industry to protect this information from unauthorized access include HIPAA compliance.

HIPAA Compliance
Electronically-distributed patient information requires strong data security. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires that Protected Health Information (PHI) remain secure at all times. In addition, recent regulations and mandates from the Department of Health and Human Services apply to HIPAA covered entities and any of their business associates that “access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI.”

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

3.2 Private Sector Security Requirements

Private sector security requirements include authorization and encryption which is standard across all business sectors. However, private businesses have the added requirement of SOX compliance.

SOX

The Sarbanes-Oxley Act of 2002 (SOX) was enacted in response to several high-profile financial scandals. The SOX act is aimed at enforcing corporate responsibility by improving financial disclosures, and avoiding corporate and accounting fraud. The SOX contains many requirements aimed at standardizing financial reporting procedures. The requirement that targets IT policies is section 404 of the act, “Management Assessment of Internal Controls.”

COBIT

The Control Objectives for IT (COBIT) is a framework that is commonly used by IT departments to comply with SOX. COBIT is set of standard IT policies and procedures that can be adopted by all businesses. By using COBIT, an organization can quickly design IT controls to comply with SOX. This includes deploying the following security solutions in the right areas:

- **Identity Management**
  Each user must be uniquely identifiable. User identities and access rights must be maintained in a central repository.
- **User Account Management**
  Account management procedures must exist for requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user privileges, as well as performing regular management reviews of all accounts and related privileges.
- **Logs, Alerts, and Reports**
  Logging and alerting policies require recording and notification of abnormal access events. Reporting policies require authorized managers to generate periodic event and log reports.
- **Network Devices**
  This regulation requires secure network devices to be used to ensure authorized system access, and to preserve information integrity to and from networks. Network devices should be capable of central management from remote locations. Devices should deliver a high level of data security by providing strong, full-disk encryption and access control to ensure the secure exchange of sensitive data by ensuring the integrity and authenticity of data.

SOX section 404 compliance provides the momentum for most IT organizations to develop and document the IT security controls and processes needed to support financial reporting. Protecting the integrity of information and controlling access to resources are not only essential elements for the preservation of a company but are also requirements for compliance.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

4. Common Criteria Security Validation

Information systems are growing every day and the IT professionals that manage these systems need to keep up with this growth. As with all other aspects of business these days, they are trying to achieve more without adding any new personnel. To streamline the process of choosing network devices, a standard has been developed for certifying the security features/claims of a device. The process is known as Common Criteria.

Only when each of the security features passes Common Criteria testing does the device security level get rated and do they issue a Common Criteria certificate.

Products validated under the Common Criteria program provide customers with a high degree of confidence that they address the security issues described in the posted evaluation documents. CCRA posts the claims and evaluation reports on their Web site. Listings can be accessed by going to the Common Criteria Portal: http://www.commoncriteriaportal.org/

The Common criteria conformances were either to Samsung Security Target [1] or to IEEE-2600 Protection Profile.

[1] Samsung Security Target includes a set of security claims that have been validated by a Common Criteria certified lab. For more details, refer to the listings on the following web page: http://www.commoncriteriaportal.org/.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

5. IEEE 2600™-2008, IEEE 2600.1™-2009, IEEE 2600.2™-2009

The Institute of Electrical and Electronics Engineers (IEEE) Standards Association (IEEE-SA) is a recognized standards sanctioning body responsible for creating, developing, integrating, sharing, and applying knowledge about information technologies and sciences. The IEEE SA developed new security standards focused on modern network printers and hardcopy peripherals (such as copiers and multifunction devices) with the goal of preventing unauthorized access.

The IEEE 2600™-2008, "Standard for Information Technology: Hardcopy System and Device Security standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users and others on the selection, installation, configuration and usage of hardcopy devices and systems; including printers, copiers, and multifunction devices.

For more information about IEEE 2600™, go to: http://standards.ieee.org/getieee/2600/index.html

This standard identifies security exposures for these hardcopy devices and systems, instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

Prior to IEEE 2600, there were no standards to guide manufacturers or users of hardcopy devices in the secure installation, configuration, or usage of these devices and systems.

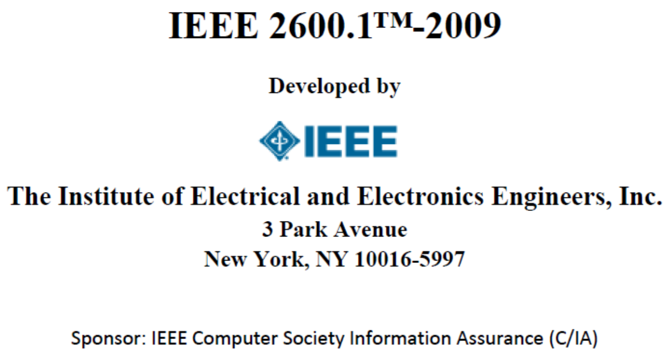
Based on the IEEE 2600-2008 standards the IEEE developed the following standards:

- IEEE 2600.1-2009
- IEEE 2600.2-2009

These standards provide a set of criteria/security requirements for Common Criteria labs, so they can verify that an MFP meets the IEEE standard requirements.

For more information, refer to the listings on the following IEEE website:

http://grouper.ieee.org/groups/2600/conforming_products.html.



IEEE 2600.1™-2009

Developed by

IEEE

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue
New York, NY 10016-5997

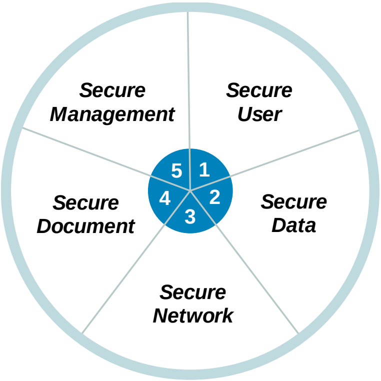
Sponsor: IEEE Computer Society Information Assurance (C/IA)

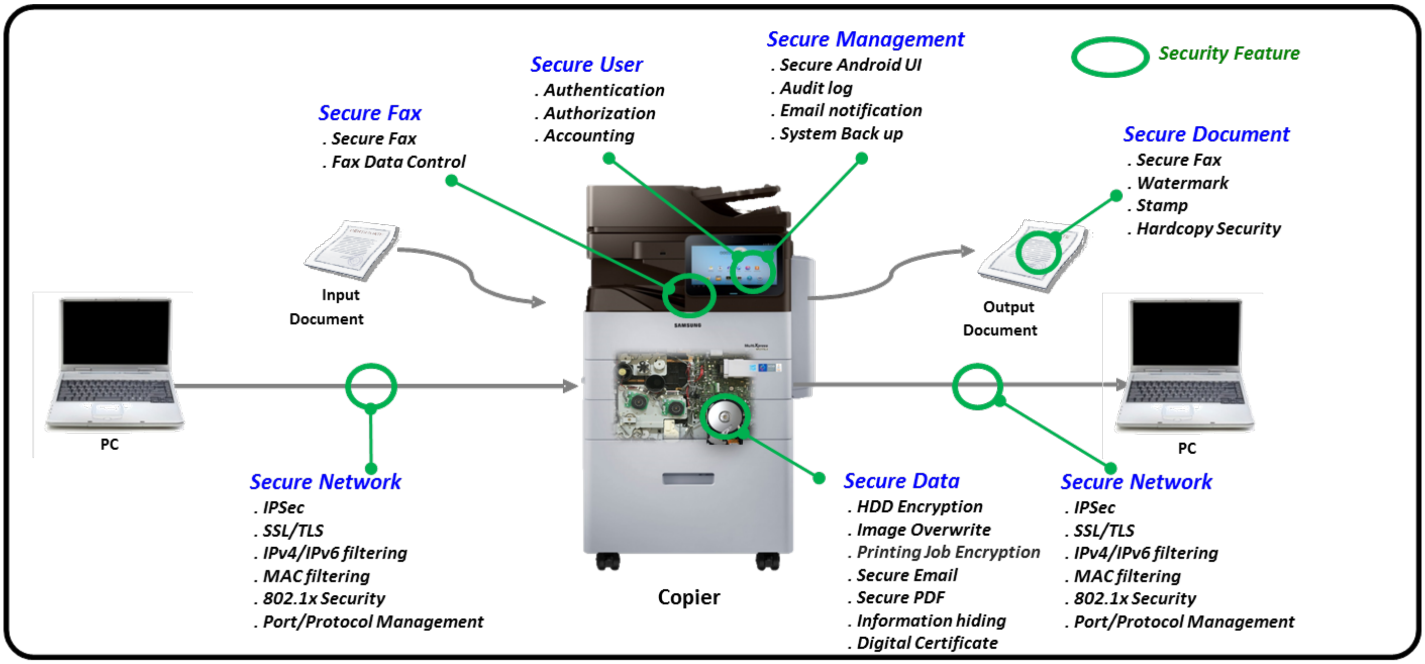
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

6. Samsung's Security Framework

Samsung defines its security framework with five security categories to cover all areas of security in the business environment. This framework is built to protect your most important information and keep your documents safe throughout the document life cycle. The categories of this framework include the following:

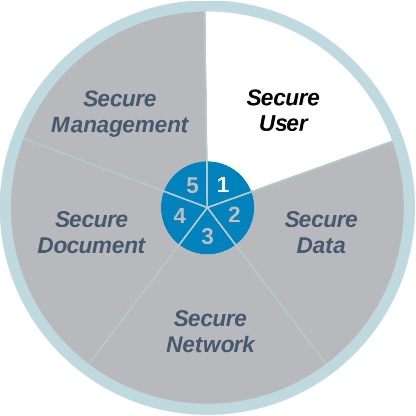
1. Secure User
2. Secure Data
3. Secure Network and Fax
4. Secure Document
5. Secure Management





Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

7. Secure User



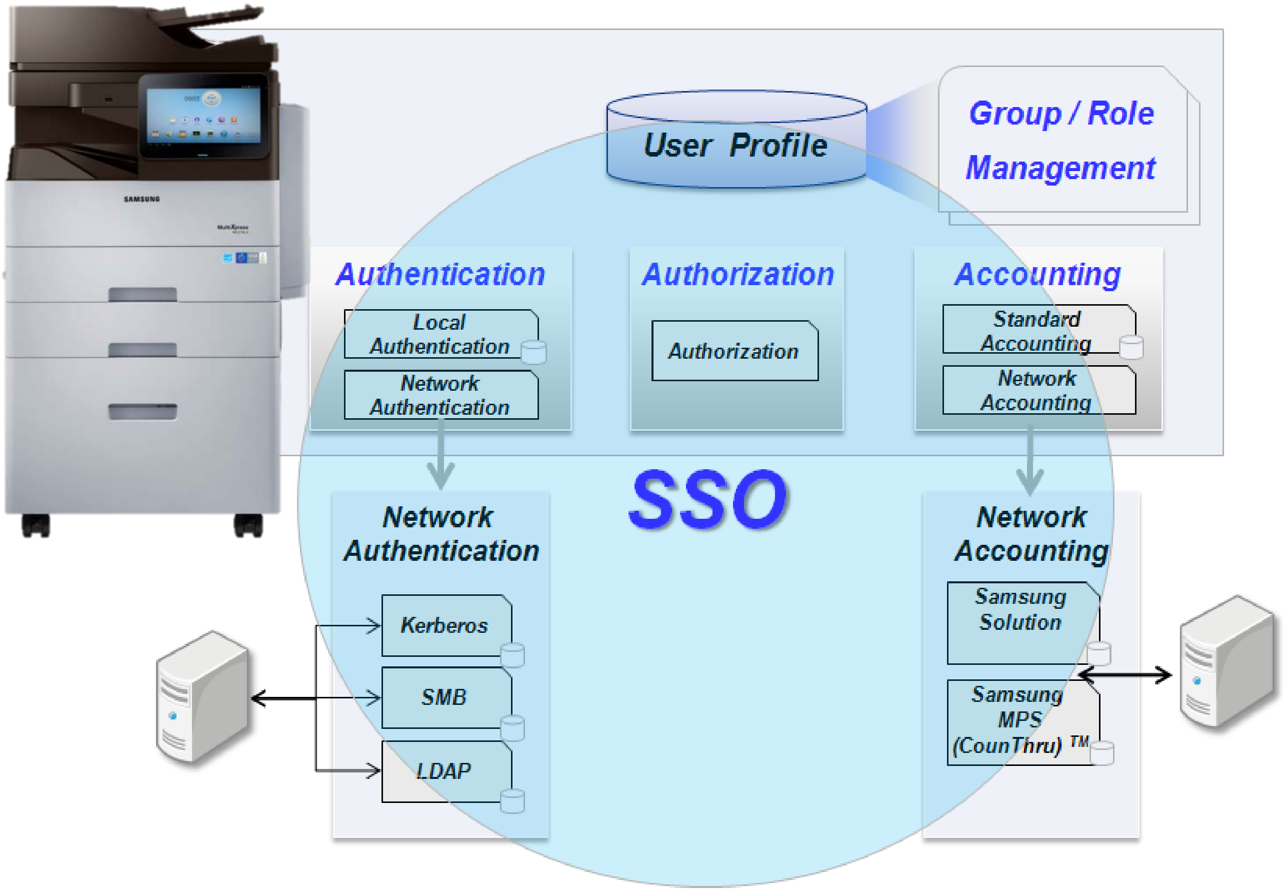
The Secure User category of the Samsung Security Framework includes the features needed to protect the MFP from access by unauthorized users.

These features include the following:

- System Authentication (for Administrators)
- Authentication (Local, Network)
- XOA-E / XOA Web Authentication
- Authorization (Group/Role Management)
- Accounting
- Single Sign-On (SSO).

The Secure User feature is designed to allow only authorized users to access the MFP, protecting your valuable information from unauthorized access.

Both large office groups and small to medium size offices can use our secure user features to easily enhance their secured environment.



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

7.1 Authentication

Authentication is used by Samsung MFPs to confirm that a user has rights to access the MFP. MFP authentication includes the following security checks:

- System Authentication
- Local Authentication
- Network Authentication
- Employee Badge / HID Proximity Card
- Smartcard Authentication / Common Access / PIV Card

7.1.1 System Authentication

Samsung MFPs require the system administrator to enter their authentication information before allowing access to the system management menus. The System Administrators role includes SyncThru^{TM} Web Service administrators and the local system administrator. The authentication process for the SyncThru^{TM} 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^{TM} Web Service administrator must enter their account and password in to the SyncThru^{TM} 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 the characters they enter.

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

7.1.2 Local Authentication

When the Authentication mode is enabled, a local MFP user must enter a password to access the menu. The password for a local MFP user 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.

7.1.3 Network Authentication

The Samsung MFP prevents unauthorized use of the network options (network scanning, scan-to-email, and scan-to-server). The MFP System Administrator sets the network options available for each user. To access a network service, the user must provide a user name and password, which is then validated by the designated authentication server.

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

7.1.4 XOA –E / XOA Web Authentication

The Samsung MFP additionally provides XOA-E / XOA Web authentication to prevent unauthorized use of the network options (network scanning, scan-to-email, and scan-to-server). XOA-E authentication server is located inside the MFP and XOA Web authentication server is located outside the MFP. That is, the Samsung MFP provides various authentication methods which are implemented by ISVs.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

7.2 User Authentication Scenarios

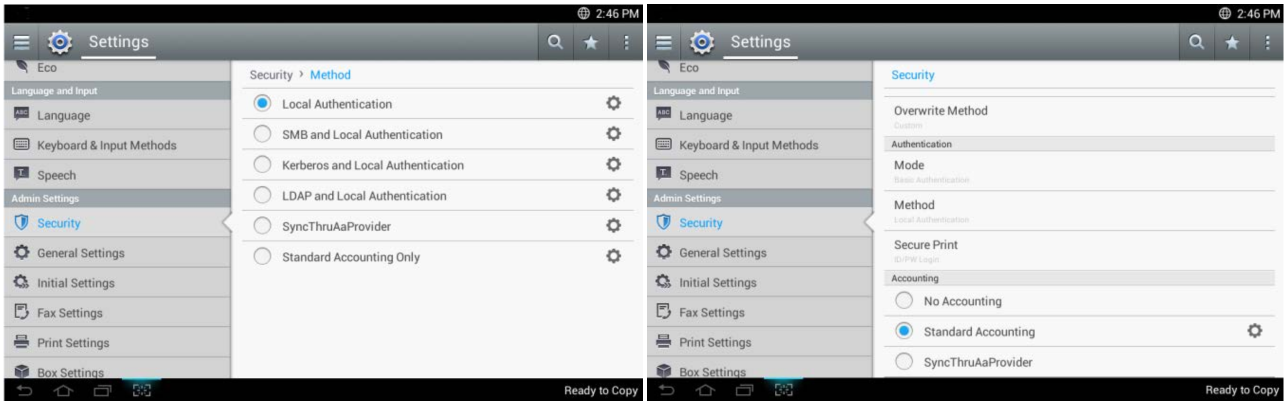
The following are examples of different user authentication configurations.

7.2.1 For Administrators

Method Setup

The Authentication Method can be set up by using the Local UI and the Web-UI. Only administrator can use these functions, after logging in to the MFP. The administrator can select from the following methods: Local Authentication, Network Authentication (Kerberos, SMB, and LDAP), and XOA-E/XOA Web Authentication.

Local UI:



Security › Method

- ● Local Authentication
- ○ SMB and Local Authentication
- ○ Kerberos and Local Authentication
- ○ LDAP and Local Authentication
- ○ SyncThruAaProvider
- ○ Standard Accounting Only

Security

Overwrite Method: Custom

Authentication

Mode: Basic Authentication

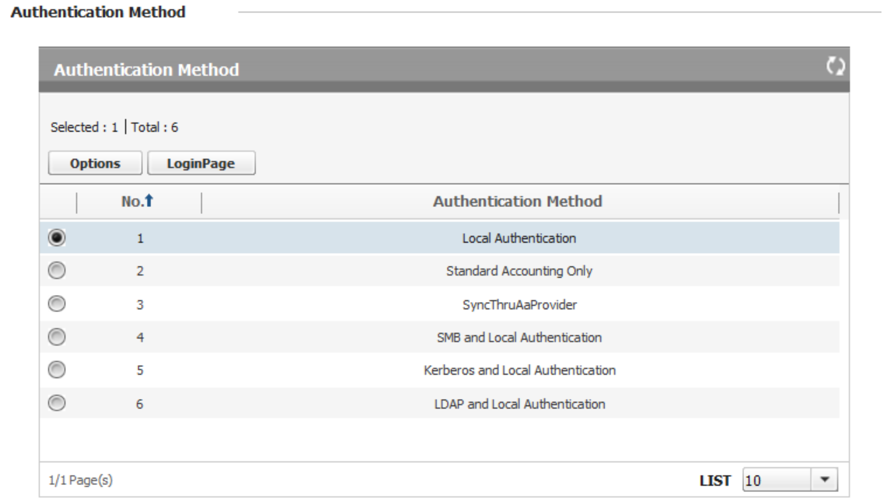
Method: Local Authentication

Secure Print: ID/PW Login

Accounting

- ○ No Accounting
- ● Standard Accounting
- ○ SyncThruAaProvider

SyncThru^{TM} Web Service UI: Security Settings → User Access Control → Authentication



Authentication Method

Authentication Method

Selected : 1 | Total : 6

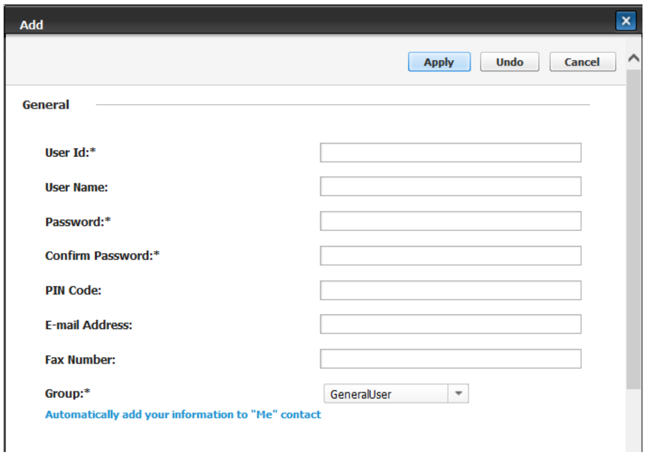
	No.	Authentication Method
●	1	Local Authentication
○	2	Standard Accounting Only
○	3	SyncThruAaProvider
○	4	SMB and Local Authentication
○	5	Kerberos and Local Authentication
○	6	LDAP and Local Authentication

1/1 Page(s) LIST 10

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

ID and Password Setup

The system administrator can create each user's ID and Password by using the Web-UI.



Add

Apply Undo Cancel

General

User Id:*

User Name:

Password:*

Confirm Password:*

PIN Code:

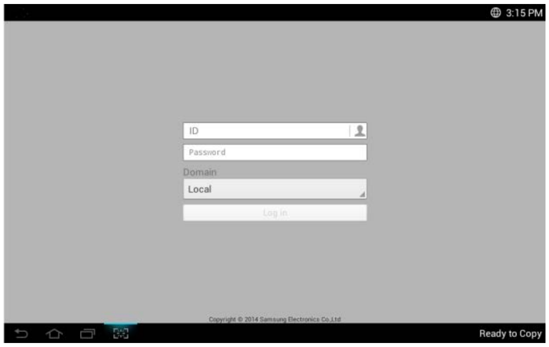
E-mail Address:

Fax Number:

Group:* GeneralUser

Automatically add your information to "Me" contact

When the Authentication mode is enabled, a User can log in to the device through the Local UI or through a Network connection. Only authorized users can access the device after successfully logging on. The following are examples of Local and Network login screens:



3:15 PM

ID

Password

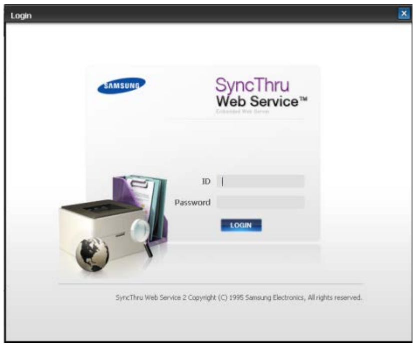
Domain

Local

Log in

Copyright © 2014 Samsung Electronics Co.,Ltd

Ready to Copy



Login

SAMSUNG

SyncThru Web Service™

ID

Password

LOGIN

SyncThru Web Service 2 Copyright (C) 1995 Samsung Electronics, All rights reserved.

7.3 Authorization (Group/Role Management)

A common form of user management is known as Role-Based Access Control (RBAC). By using a defined set of roles, an administrator can easily assign access to a user by assigning them to a role. Adding a user to a group also allows the administrator to manage access for large groups of users. Examples of Roles for the MFP are Print Only, Scan Only, Copy Only or any combination of these, and others.

7.3.1 Using Group and Role-Based Authority

The Administrator can create several groups with different user roles by using SyncThru^{TM} Web Service. With this function, the user property of Authorization, Authentication, and Accounting can be controlled by Group/Role definitions. For example, when Group "A" has only "Copy" authority, a user in that group can only use the Copy feature but not other features like Faxing or Scanning.

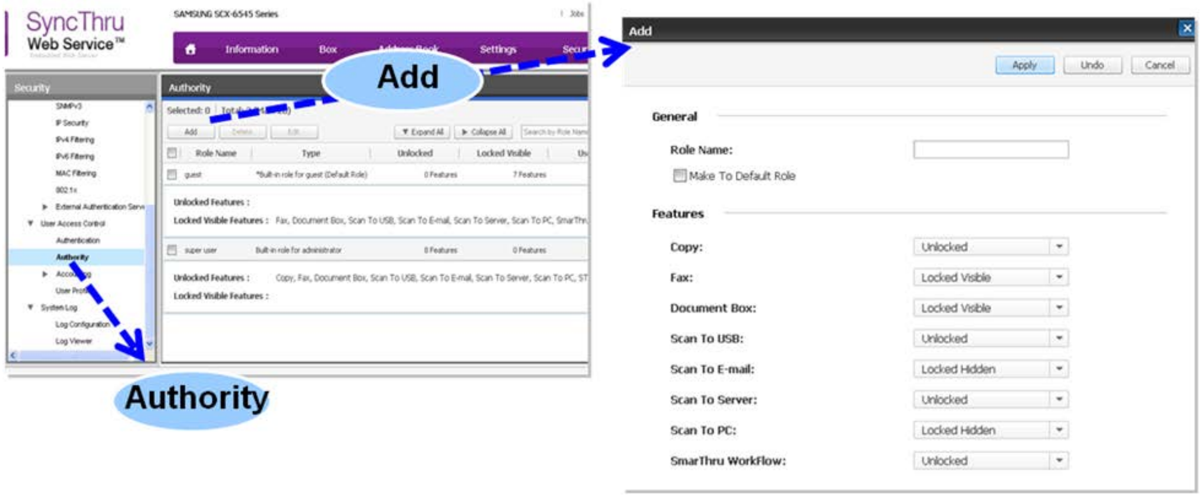
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

7.4 User Authorization Scenarios

The following are overviews of User Role and Group menus.

7.4.1 Administrator Menu

The Administrator uses the Web UI to set up the Role and Group Authorization modes. This feature is only accessible to the Administrator and it requires an ID and password.



☐	Role Name	Type	Unlocked	Locked Visible
☐	guest	*Built-in role for guest (Default Role)	0 Features	7 Features
☐	super user	Built-in role for administrator	8 Features	0 Features

guest — Unlocked Features :
Locked Visible Features : Fax, Document Box, Scan To USB, Scan To E-mail, Scan To Server, Scan To PC, SmarThr

super user — Unlocked Features : Copy, Fax, Document Box, Scan To USB, Scan To E-mail, Scan To Server, Scan To PC, ST
Locked Visible Features :

General

Role Name:

☐ Make To Default Role

Features

Copy: Unlocked
Fax: Locked Visible
Document Box: Locked Visible
Scan To USB: Unlocked
Scan To E-mail: Locked Hidden
Scan To Server: Unlocked
Scan To PC: Locked Hidden
SmarThru WorkFlow: Unlocked

The features that can be assigned to Users and Groups include the following:

- Color
- Copy
- Fax
- Document Box
- Scan To USB
- Scan To Email
- Scan To Server
- Scan To PC
- Address Book
- Job Queue
- Admin Setting.

Each feature can be given one of the following permissions:

- Unlocked
- Locked Visible
- Locked Hidden.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

7.5 Accounting

Accounting is the process of collecting MFP usage data by Device, Group, and User. This section describes the accounting features used by the MFP.

7.5.1 Standard and Network Accounting

Samsung MFPs track User Accounting for each impression of each job. Based on the User's ID, the Administrator can count each job for Users and Groups. This allows you to see the cost for MFP usage by User and Group.

The system supports the following types of accounting methods to support this functionality:

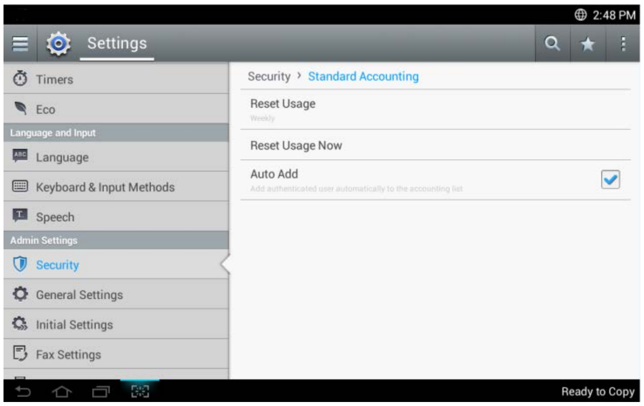
- Local User for Standard Accounting
- Network User for Server based Accounting (Fleet Admin Pro^{TM}, CounThru^{TM}).

7.6 User Accounting Scenarios

7.6.1 For Administrators

Accounting modes can be set up by using the Web-UI or the Local UI. When Network Accounting is enabled, you can use the Fleet Admin Pro^{TM} and CounThru^{TM} solutions. Standard Accounting allows the Administrator to manage the Accounting IDs list and the Login Settings (ID/Password or ID only). Detailed Accounting can be set up with the Web-UI, allowing the Administrator to manage limitations on Copying, Printing (Color, Black), Fax, and various Scanning options.

The following are examples of the Standard Accounting menus on the Local UI:



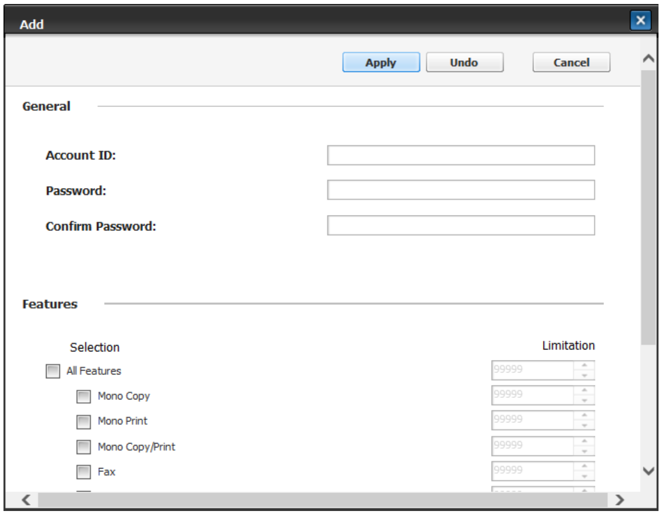
Security › Standard Accounting

Reset Usage
Weekly

Reset Usage Now

Auto Add ☑
Add authenticated user automatically to the accounting list

The following is an example of a Standard Accounting menu on the Web UI:



General

Account ID:

Password:

Confirm Password:

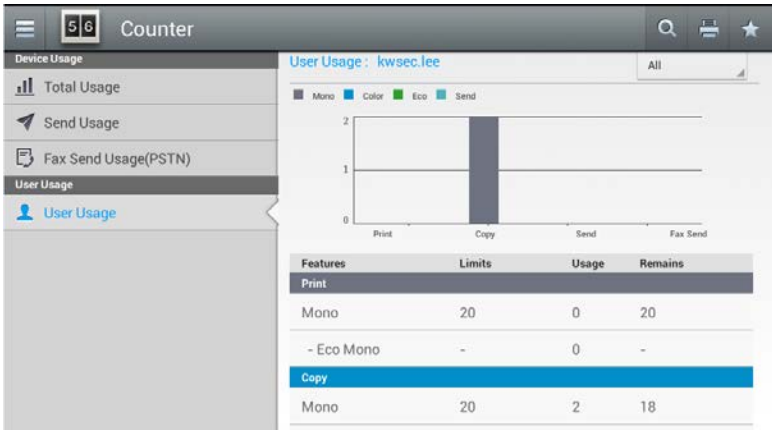
Features

Selection	Limitation
□ All Features	99999
□ Mono Copy	99999
□ Mono Print	99999
□ Mono Copy/Print	99999
□ Fax	99999

7.6.2 For Users

When a user logs on to the MFP, they can view their own usage accounting statistics.

The following is a User Accounting view on the Local UI:

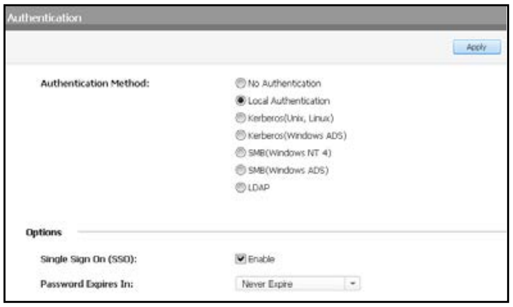


User Usage : kwsec.lee

Features	Limits	Usage	Remains
Print			
Mono	20	0	20
- Eco Mono	-	0	-
Copy			
Mono	20	2	18

7.7 Single Sign-On (SSO)

The SSO feature allows the user to only log-in to the system (Local and Network) once. SSO remembers the authority and authentication automatically based on initial user ID/Password input values. The SSO feature controls all of "Secure User" functions such as Authentication, Authorization, and Accounting. The SSO feature is configured through the SyncThru^{TM} Web Service.



Authentication Method:
○ No Authentication
● Local Authentication
○ Kerberos(Unix, Linux)
○ Kerberos(Windows ADS)
○ SMB(Windows NT 4)
○ SMB(Windows ADS)
○ LDAP

Options

Single Sign On (SSO): ☑ Enable

Password Expires In: Never Expire

7.8 Key Benefits of "Secure User"

This section describes the benefits provided by the Samsung Secure User category of the Samsung Security Framework.

7.8.1 Good Basic Security

"Secure User" protects the Samsung MFP from unauthenticated or unknown user access. This is a very basic step in protecting your valuable data and information on the MFP.

7.8.2 Increased Productivity

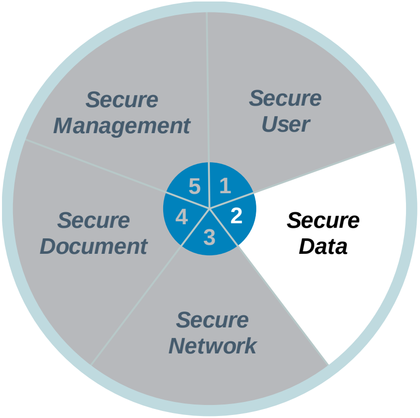
Simple user management tools allow administrators to easily perform their administrative tasks from one location to several devices. A Single Sign-On path for authorizing multiple MFP features allows easy access for end users to the information and resources they need. Both of these features provide the increased productivity required by today's lean business model.

7.8.3 Cost Control

Accounting allows you to track job costs and charge the correct departments for their portion of the MFP expenses.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

8. Secure Data



The "Secure Data" category of the Samsung Security Framework is designed to protect your valuable data from threats while it is residing or passing through the MFP. Confidential and private data such as patient information, student records, client information in banks, insurance companies, etc. must now be protected on an MFP in the same way a server must be protected from unauthorized access. It is no longer surprising to find MFPs and printers equipped with hard drives. These hard drives store various types of hardcopy information such as, user information, copy/scan/fax/print images from processed jobs, and device activity logs. Some or all of the information on the hard drives need to be protected securely. Hard drive overwriting technology and encryption are the industry standard methods for securely protecting the data.

Samsung's "Secure Data" protects your valuable data by using advanced security features like Encryption of the hard drives, scans, and Network printing, and hard drive image overwriting.

8.1 Encryption

Encryption is the process of changing data into useless characters that must be unscrambled by using a key. The Samsung Secure Data feature uses the following methods:

- Hard Disk Drive (HDD) Encryption
- Print Job Encryption
- PC Scan Security
- Secure PDF (PDF Encryption, Digital Signature in PDF)
- Secure Email (SMTP)
- Email Encryption.

8.1.1 Hard Disk Drive (HDD) Encryption

To protect the confidentiality of the data stored on a computer HDD, encryption is used. Data on the HDD is written in plain text which makes it available for everyone to read. To prevent this from occurring, HDD encryption is required.

Samsung MFPs protect data by using built-in AES-256 HDD encryption technology.

When a user stores data on the HDD, the original data is encrypted and stored on the HDD. When the user retrieves the data from the HDD, the encrypted data is decrypted using a key before it is sent to the user. HDD encryption is a built-in feature available on all HDD-equipped Samsung MFPs.

Samsung offers our optional Common Criteria certified Secure Data Kit. This Secure Data Kit includes security features such as image overwrites options, Hard Drive encryption, and SSL/TLS. This kit provides up-to-date security technology, allowing you to achieve the highest level of security.

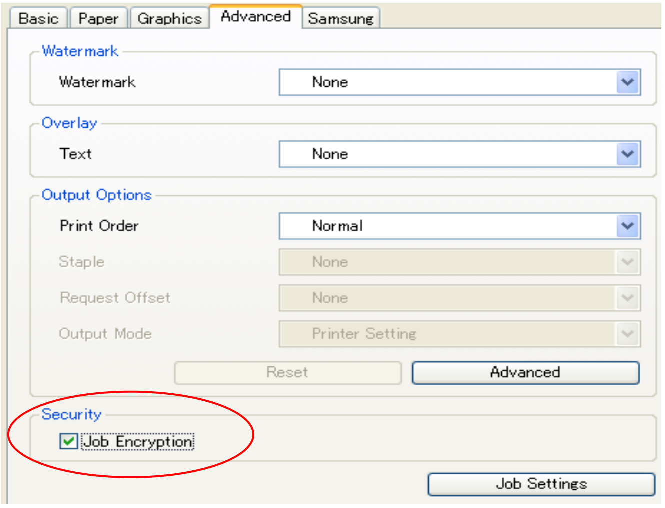
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

8.1.2 Print Job Encryption

Print Job Encryption encrypts the data used by the network while printing. The network encryption process follows this path: Make and share keys (ECDH) --> Encrypt data (AES) --> Transmit encrypted data --> Decrypt data --> Print decrypted data.

This feature can be enabled from the Printer Driver and it is transparent to the User.

There is no visible printing performance deterioration even when the encryption is enabled.



Watermark

Watermark: None

Overlay

Text: None

Output Options

Print Order: Normal

Staple: None

Request Offset: None

Output Mode: Printer Setting

Security

☑ Job Encryption

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

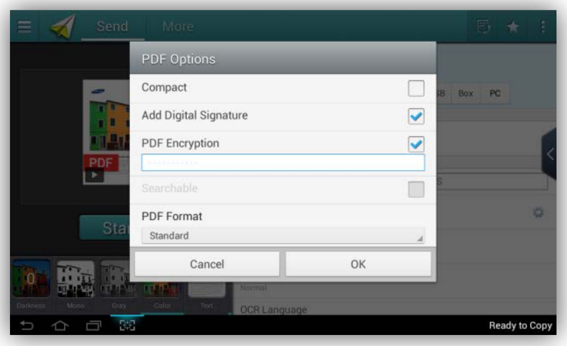
8.1.3 Secure PDF - PDF Encryption

Samsung Secure Data allows you to encrypt a PDF document to protect its contents from unauthorized access. Encryption applies to all strings and streams (Scanned Images) in the document's PDF file, but not to other object types such as integers and Boolean values, which are used primarily to convey information about the document's structure rather than its content. Leaving these values unencrypted allows random access to the objects within a document, whereas encrypting the strings and streams protects the document's substantive contents.

8.1.4 Secure PDF – Digital Signature in PDF

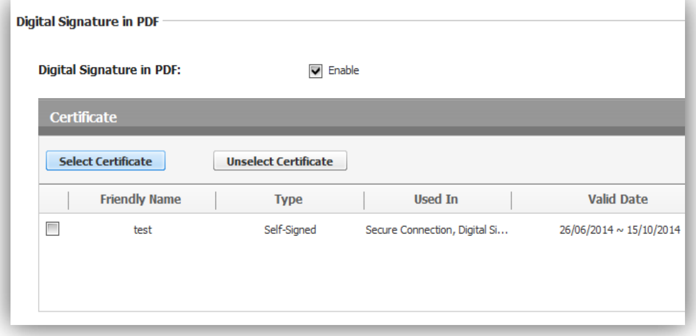
Users can add a Digital Signature to the PDF with certification. To add the Digital Signature, users must create the digital certificate (See 8.1.5) from the SyncThru^{TM} Web Service. The Digital Signature in the PDF function can be used in the Scan to Server feature.

Example of MFP menu for PDF Encryption / Digital Signature in PDF:



PDF Options

- Compact ☐
- Add Digital Signature ☑
- PDF Encryption ☑
- Searchable ☐
- PDF Format: Standard



Digital Signature in PDF

Digital Signature in PDF: ☑ Enable

Certificate

	Friendly Name	Type	Used In	Valid Date
☐	test	Self-Signed	Secure Connection, Digital Si...	26/06/2014 ~ 15/10/2014

8.1.5 Digital Certificate

Digital certificate is an electronic credential that can help verify the secure connection between communication nodes. The most common use of digital certificates is to prove the identity of a person or device and to provide the secure exchange of encrypted information.

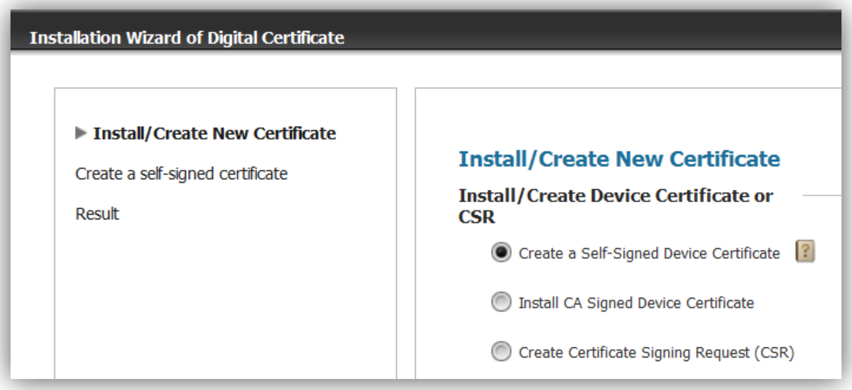
There are 2 kinds of Certificate.

- **Self Signed Device Certificate**

  The certificate created by device itself

- **CA (Certificate Authority) Signed Device Certificate**

  The certificate authorized by third-party CA (Certificate Authority). This certificate is more reliable than the Self Signed Device Certificate. To get CA Signed Device Certificate, a Certificate Signing Request should be sent to the CA.


Installation Wizard of Digital Certificate
▶ Install/Create New Certificate
Create a self-signed certificate
Result
?

Install/Create New Certificate

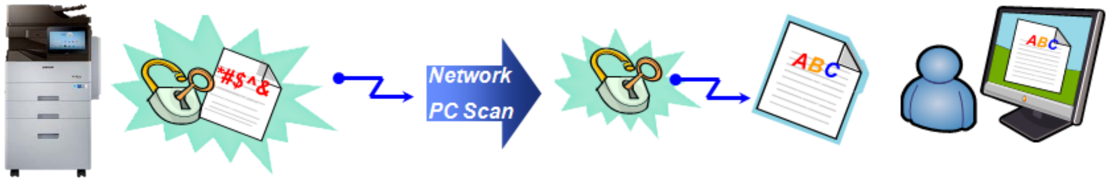
Install/Create Device Certificate or CSR

- ● Create a Self-Signed Device Certificate
- ○ Install CA Signed Device Certificate
- ○ Create Certificate Signing Request (CSR)

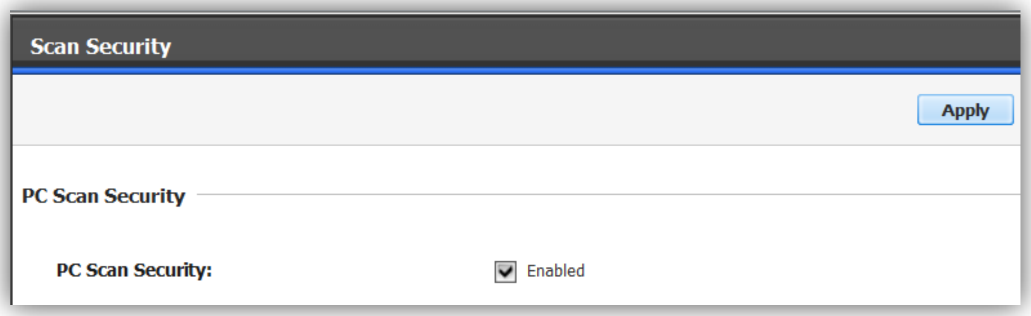
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

8.1.6 PC Scan Security

PC Scan Security Feature provides the Security Protection for scanned documents. Scanned data is delivered to a PC or to a user by using encryption. Scan jobs sent through the Twain Protocol are supported by ECDH key exchange and AES encryption algorithms. This feature is managed through the Web UI.



Example of WUI PC Scan setting



Scan Security

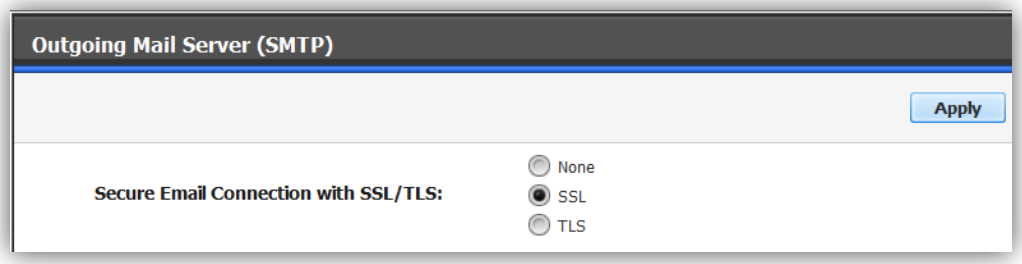
Apply

PC Scan Security

PC Scan Security: ☑ Enabled

8.1.7 Secure Email (SMTPs)

The Secure Email feature sends an email with attached image files generated from MFP scans, faxes, and notifications to SMTP server over secured network (SSL/TLS). By using this feature, users can always ensure that the email data is sent to SMTP server with encrypted. This feature is managed through the Web UI.



Outgoing Mail Server (SMTP)

Apply

Secure Email Connection with SSL/TLS: ○ None ● SSL ○ TLS

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

8.2 Image Overwrite

User information created during the copying, printing, network scanning, scanning to email, or scanning to server processes is immediately recorded on the hard disk drive of MFP. To secure this information, the MFP software implements an image overwrite function to erase image data created during the copying, printing, network scanning, scanning to email, or scanning to server processes. The MFP software provides various image overwrite standard methods such as DoD 5220.28-M, Australian ACSI 33, DoD5220.22-M (ECE), German standard (VSITR) standard, and Custom (Up to 9 times). The MFPs can perform the following image overwrites:

- Automatic Image Overwrite
- Manual Image Overwrite
- Scheduled Image Overwrite

8.2.1 Automatic Image Overwrite

The Automatic Image Overwrite feature overwrites temporary image files automatically after the completion of each MFP task.

8.2.2 Manual Image Overwrite

The Manual Image Overwrite feature allows the MFP System Administrator to manually perform a data overwrite of the HDD data.

8.2.3 Scheduled Image Overwrite

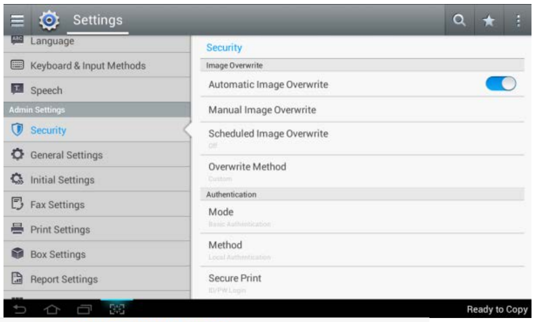
The Scheduled Image Overwrite feature allows the MFP System Administrator to reserve a data overwrite of the HDD data based on an assigned schedule (Frequency, Day, Week, and Time).

8.2.4 Image Overwrite from the Local UI.

The system automatically overwrites temporary files created during processing and manually overwrites temporary files created during processing on a specially-reserved section of the hard drive (Automatic Image Overwrite).

The image overwrite security function can also be invoked manually by the system administrator. Once invoked, it cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section on the hard drive, and then it reboots the main controller. When a power failure interrupts the manual overwrite, the process will restart automatically after the power returns allowing it to finish overwriting all of the remaining files (Manual Image Overwrite).

Examples of MFP menus for Image Overwrite:



Settings

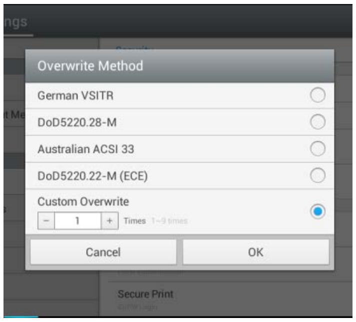
Language
Keyboard & Input Methods
Speech
Admin Settings
Security
General Settings
Initial Settings
Fax Settings
Print Settings
Box Settings
Report Settings

Security

Image Overwrite
Automatic Image Overwrite
Manual Image Overwrite
Scheduled Image Overwrite
Off
Overwrite Method
Custom

Authentication
Mode
Basic Authentication
Method
Local Authentication
Secure Print
ID/PW Login

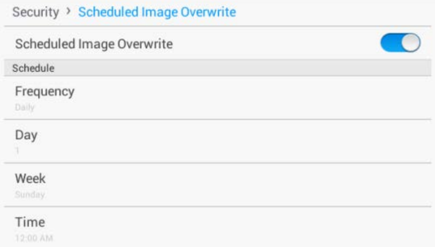
Ready to Copy



Overwrite Method

○ German VSITR
○ DoD5220.28-M
○ Australian ACSI 33
○ DoD5220.22-M (ECE)
● Custom Overwrite
− 1 + Times 1~9 times

Cancel OK



Security › Scheduled Image Overwrite

Scheduled Image Overwrite

Schedule
Frequency
Daily
Day
1
Week
Sunday
Time
12:00 AM

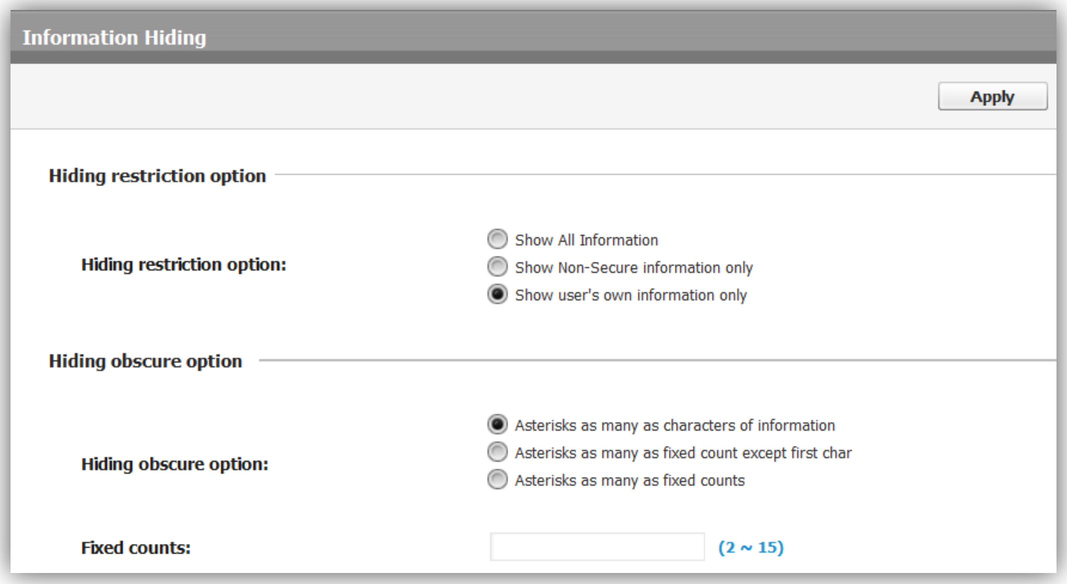
8.3 Information Hiding

User information created during the copying, printing, network scanning, scanning to email, or scanning to server processes is immediately recorded on the MFP's hard drive. Some data includes sensitive information from the job list. You want this information to be obscured in the Local UI, Web-UI, and the Job Monitor. Information Hiding displays information differently according to the login user and the Information Hiding settings. Information Hiding settings include the following:

- Hiding restriction option
  - All information
  - Non-Secure information only
  - User's Own information only
- Hiding obscure option
  - Asterisks as many as characters of information
  - Asterisks as many as fixed count except first character
  - Asterisks as many as fixed counts.

Note: Secure information includes Secure Print, and Secure Received Fax jobs.

Example of Information Hiding menu:



Information Hiding

Apply

Hiding restriction option

Hiding restriction option:
○ Show All Information
○ Show Non-Secure information only
● Show user's own information only

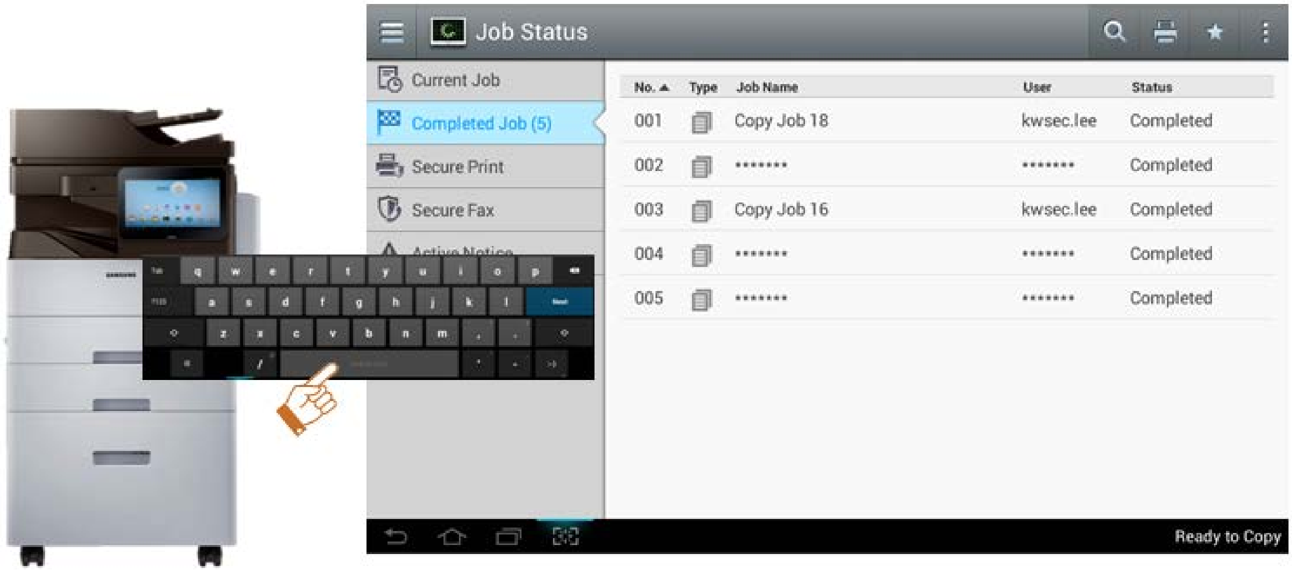
Hiding obscure option

Hiding obscure option:
● Asterisks as many as characters of information
○ Asterisks as many as fixed count except first char
○ Asterisks as many as fixed counts

Fixed counts: (2 ~ 15)

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Example of Hidden Information on the Local UI:



No. ▲	Type	Job Name	User	Status
001		Copy Job 18	kwsec.lee	Completed
002		*******	*******	Completed
003		Copy Job 16	kwsec.lee	Completed
004		*******	*******	Completed
005		*******	*******	Completed

8.4 Key Benefits of Using Secure Data

8.4.1 Data Protection

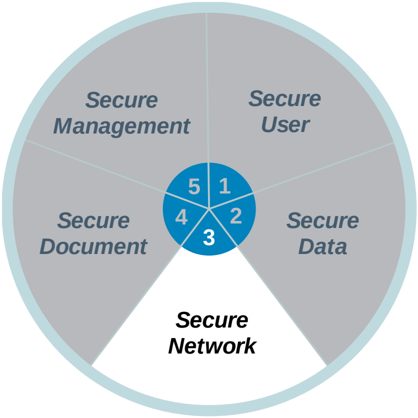
By using these various MFP data security methods, you can protect your secured information from unauthorized access. Information in the system device (MFP) and in the Server can be protected by using encryption, overwriting and some network security features.

8.4.2 Various Options Settings

Administrators will experience various option methods using the Web & Local UI. Also, user has a chance to choose the best way to protect their data with many option items.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

9. Secure Network



The Secure Network category of the Samsung Security framework is designed to protect your network from unauthorized access through the MFP. This protection is made possible by using industry standard methods including the following:

- Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
- Simple Network Management Protocol (SNMPv3)
- IP Security (IPSec)
- 802.1x Network Security
- Protocol/Port Management
- IP/MAC Filtering.

9.1 Transport Layer Security (TLS) / Secure Sockets Layer (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communications over TCP/IP networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Transport Layer from end-to-end.

- FTP over SSL/TLS
- SMTP over SSL/TLS
- HTTP over SSL/TLS
- LDAP over SSL/TLS
- IPP over SSL/TLS
- POP3 over SSL/TLS
- ThinPrint over SSL/TLS.

9.2 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 TCP/IP 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. The SNMPv3 used on Samsung MFPs can support authentication by using the SHA algorithm and can support one account to read and write.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

9.3 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 is used to protect IP-based network traffic.

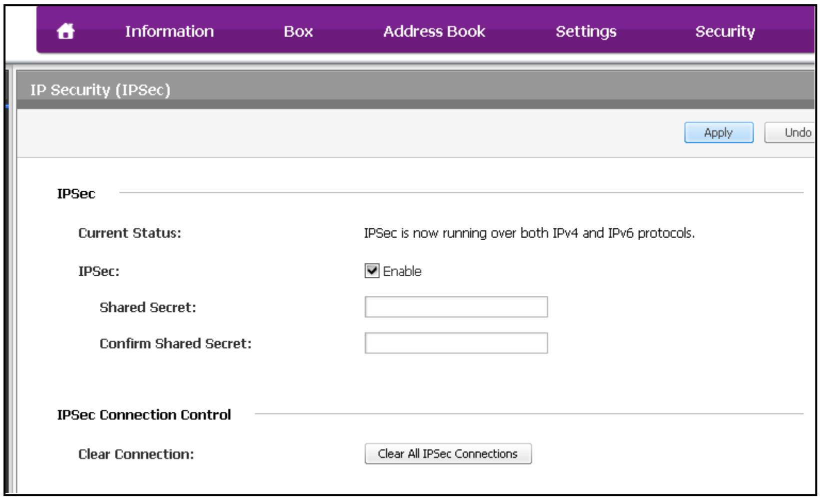
IPSec is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

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^{TM} RFCs:

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

IPSec only supports the pre-shared key method for IPSec authentication. Users can setup pre-shared key values through a Web UI. IKE protocol is used to establish and manage Security Association (SA) between a printer and a user node in the AH and ESP services.

Example if IPSec menu in the Web UI:



IP Security (IPSec)

IPSec

Current Status: IPSec is now running over both IPv4 and IPv6 protocols.

IPSec: ☑ Enable

Shared Secret:

Confirm Shared Secret:

IPSec Connection Control

Clear Connection:

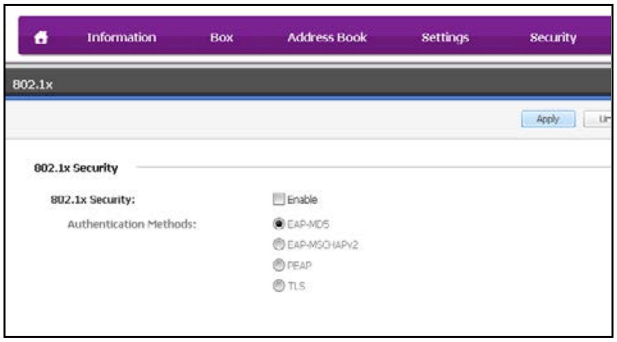
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

9.4 802.1x Support

802.1x Network Security is a protocol used for authenticating network access for 802.1x enabled ports. Generally it is used in 802.11 wireless security communications. Wired network communications also use 802.1x enabled ports. A switch network device called the 'Authenticator' requires the 802.1x authentication to be connected to the MFP and requires that the MFP responds with its credentials when polled. The authenticator transfers the MFP's credentials to an authentication server called 'RADIUS' and finally RADIUS decides whether to permit the connection or not.

802.1x Network Security protocol uses some Extensible Authentication Protocols (EAP).

Example of 802.1x Web UI menu:



802.1x Security

802.1x Security: □ Enable

Authentication Methods: ● EAP-MD5 ○ EAP-MSCHAPv2 ○ PEAP ○ TLS

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

9.5 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 Protocol Management 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
- SSL
- LDAP

9.6 IP/MAC Filtering

Samsung MFPs 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 (supports 10 IPv4 address ranges and 10 IPv6 address ranges).

MAC Address Filtering is also capable of rejecting or accepting requests from specific Ethernet MAC addresses.

9.7 Key Benefit of Using Secure Network

The Samsung MFP Secure Network feature protects your information from unauthorized network access.

Hackers are always finding new ways to access your valuable information. One of those new points of access is through what were once considered “dumb” devices. Now because of the high level of features and technology in these devices and their network management access, you must employ security measures that protect these devices. Methods of protection include IP/MAC address filtering. This only allows PCs that have a registered IP address (Internet Protocol) or MAC address (Media Access Control) to access and use the device over the network. Server-based port filtering is another method used when the network firewall software does not suffice to secure servers and LANs from TCP/IP-based security attacks. Network data encryption can also be deployed to protect print data streams and Web interfaces from eavesdropping and making malicious data interceptions. Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are used as cryptographic protocols to provide security and data integrity for communications over TCP/IP networks. By shuffling data and passwords as they travel over the LAN, these security protocols make it very difficult for hackers to intercept, decipher, and tamper with this information. Another method of protection is cryptographic algorithms used on internal hard drives and volatile memory that could be accessed maliciously. Samsung even includes overwriting of unwanted data from the hard drive so that it can never be recovered, ensuring the confidentiality of vital data and information (e-shredding).

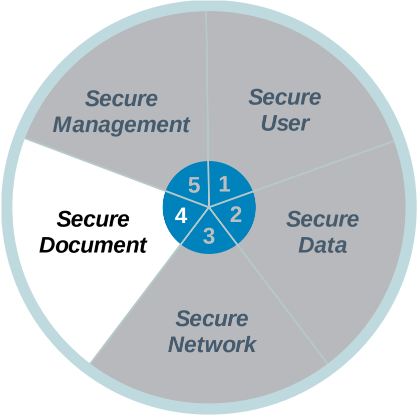
The Samsung MFP provides the feature management option to enable/disable the port/protocol and physical device such as Ethernet and USB host/device. Therefore, if administrators don't want to use physical interfaces such as USB ports, USB devices, and Ethernet (Network Connection), the administrators can easily disable each interface.

In general, a Samsung MFP does not provide network access abilities thru the USB port/device. Therefore, the malicious users cannot access the network thru any other interface. Even when the Samsung MFP is installed within a LAN and a PC is connected thru USB additionally with the device, the PC cannot access the network thru the MFP. Samsung Printing Division has designed our MFPs to prevent malicious access to the network thru any USB port/device.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

10. Secure Document

The Secure Document category of the Samsung Security Framework is designed to secure the document path from unauthorized access.



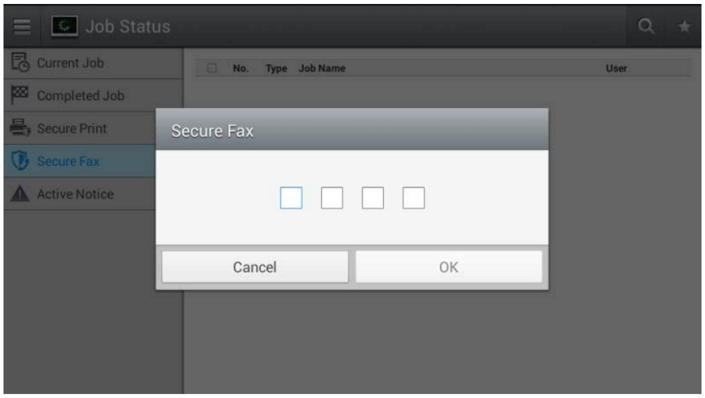
10.1 Confidential Print (Secure Print)

The Confidential Print feature restricts unauthorized people from accessing printed documents. When Confidential Print is enabled through Printer-Driver, the user must input the pin number or password. To collect the print job at the device, the user must enter the job password to print the job. Using this feature, users can always ensure that they are at the device when their job is delivered.

10.2 Secure Fax

The Samsung Secure Fax feature restricts unauthorized access to received fax documents. When the Secure Fax Option is enabled, all received fax documents are stored in memory. These stored fax documents are protected by a password. You can only print out or disable this feature when you have the password. Selecting the "Job Status – Secure Fax" button from the MFP UI and entering the password, allows you to access the Secured Received Fax Folder and retrieve your faxes.

Examples of the Secure Fax MFP UI:



10.3 Document Tagging

The Document Tagging feature allows you to add distinctive markings to your documents to enhance document control, a requirement of several regulatory standards.

10.3.1 Watermarks

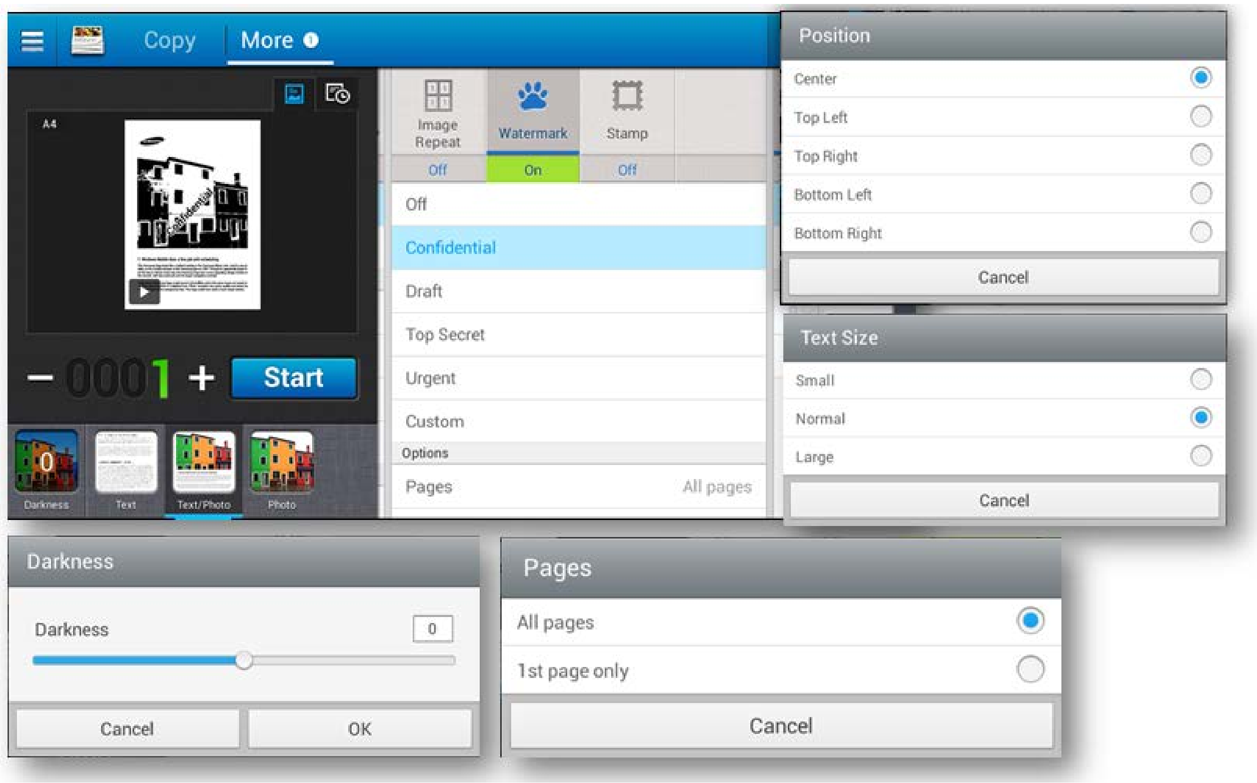
The Watermark feature is designed for Controlled documents such as "Classified" information or documents designated as officially secret, which require markings like "Confidential" or "Top Secret". This feature allows you to print text over copied documents by using the Advanced Copy menu on the Local UI. You can select several predefined watermarks including the following:

- Confidential
- Draft
- Top Secret
- Urgent
- Custom

You can also create your own watermark and modify the following parameters:

- Pages
- Text Color
- Text Size
- Position
- Darkness

Examples of Watermark menus from the Local UI:



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

10.3.2 Stamp

The Stamp feature allows you to add tracking information to your documents. This feature adds job information to the document such as, user ID, device serial number, printed date and time, etc.

Print jobs that can use the Stamp feature include the following:

- Copy
- Print (PC Printing, Reports, Stored Job Printing, Document Box Printing, USB Direct Printing)

The information that can be stamped on the document includes the following:

- IP Address
- User ID
- Device Information
- Comment (Custom)
- Page Number
- Date & Time.

You can also modify the following parameters:

- Text Color
- Text Size
- Position (Top, Bottom)
- Opacity (Opaque, Transparent).

Example of the Stamp feature menu in the Local UI:

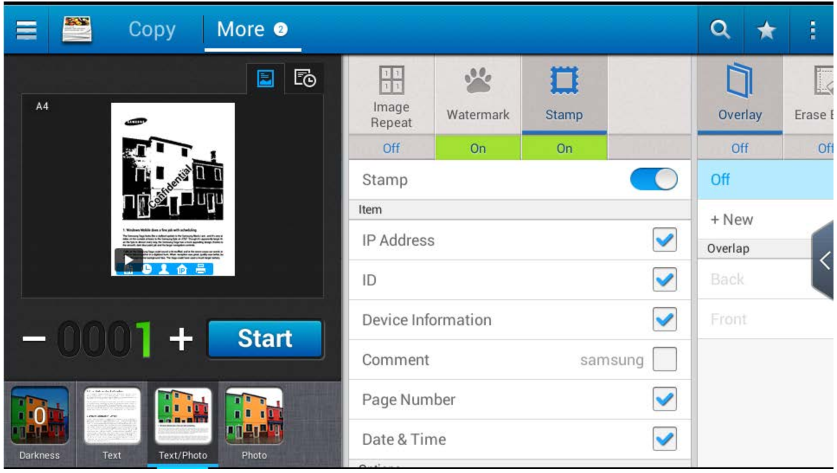


Image Repeat: Off
Watermark: On
Stamp: On
Overlay: Off

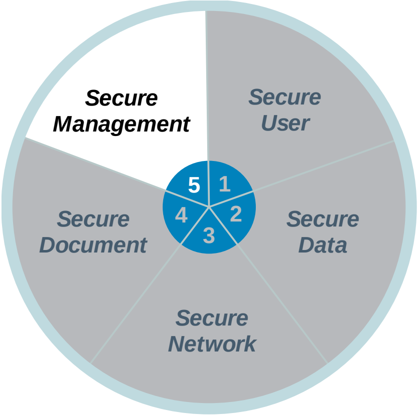
Stamp ●

Item

IP Address ☑
ID ☑
Device Information ☑
Comment samsung □
Page Number ☑
Date & Time ☑

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

11. Secure Management



The Secure Management category of the Samsung Security Framework is designed to protect the logging and notification features of the MFP. If MFP supports Smart UX using Android, this secure management provides the methods to protect system security.

The logs can contain sensitive information that is useful to administrators and managers. The sensitivity of this information requires that it be protected from unauthorized access. While the notification pathways must be secured from unauthorized redirection or snooping.

The logging and notification features protected by Secure Management include the following:

- Logging (Job Auditing)
- System Back-up
- Email Notification.

The Smart UX Android Security is explained in Section 13.Smart Print UX with Android Security.

- Installation of Android App
- Android App security management
- Android Firmware Security

11.1 Logging (Job Auditing)

Samsung MFPs track events and actions for logged-on users such as, print jobs, scan jobs, and fax jobs. Job Auditing tracks the following metrics:

- Who (ID)
- What (Print Job, Scan Job, Fax Job ...)
- When (Time and Date Stamp)

While the Stamp feature can add useful tags to the documents, this feature allows the Administrator to manage and monitor all of the jobs, MFP operations, and events on the MFP. All of this log information is stored on the MFP HDD. Log data stored on the MFP HDD can be exported and backed up to an external server. The following logs are kept on the MFP:

- Job Log
- Operation Log
- Security Event Log

These audit logs track data requests, changes made to the security audit functions, image overwriting results, and inquiries/changes to the security audit configuration. Because Log data is only available to authorized web administrators, unauthorized users cannot change or delete them. Log data can be downloaded by using the Web UI for viewing and analysis. When the MFP HDD storage is full of log data, the latest records overwrite the oldest audit records.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

11.1.1 Job Log

The Job log is used for storing all of the job activity data on the MFP.

11.1.2 Operation Log

The Operation log is used by the MFP to store all of the user's activities performed on the MFP.

11.1.3 Security Event Log

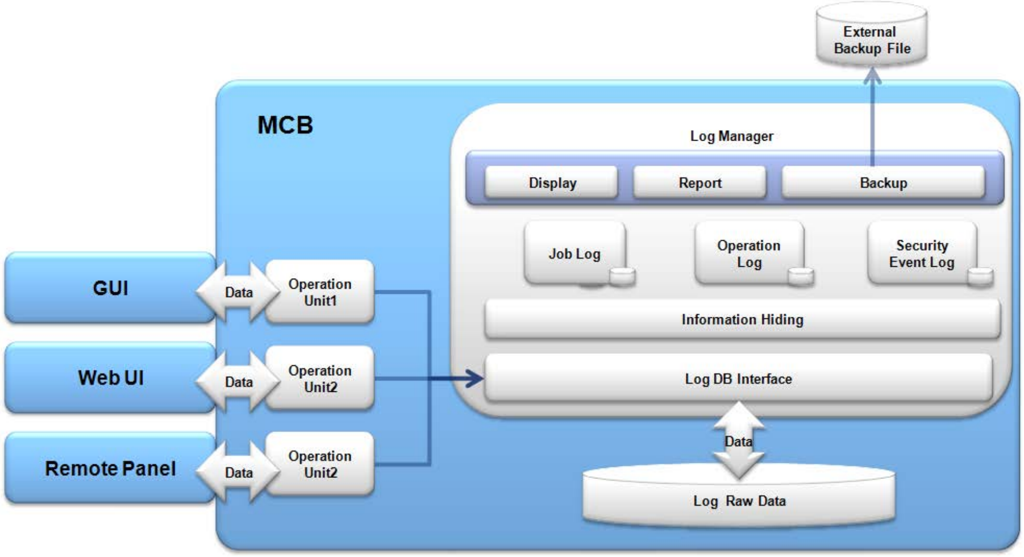
The Security Event log is used for storing all of the attempts to access the MFP.

11.2 Log Features

Log features include the following:

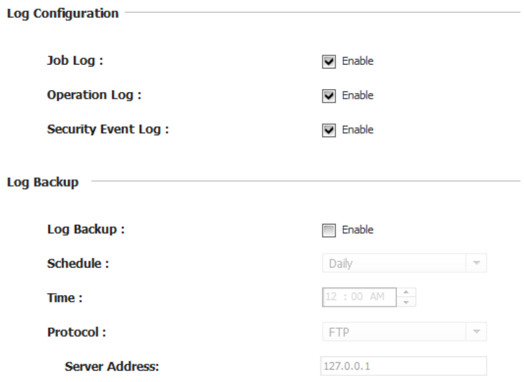
- Log Enablement
  This feature allows you to enable logs from the Local UI and SyncThru^{TM} Web Service UI.
- Log Report
  This feature allows you to generate a Job Log Report, an Operation Log report, and a Security Event Log Report from the Local UI.
- Log Query
  This feature allows you to query the log entries by using parameters such as, Log Type, User Name, and Date.
- Log Export
  This feature allows you to export the logs by using the SyncThru^{TM} Web Service UI. The logs are exported using the comma separated (.csv) file format.
- Log Backup
  This feature allows you to perform periodic backups (Daily/Weekly/Monthly) or Manual backups to the Backup Server (SMB/FTP) using the comma separated (.csv) file format.

Example of Log process:



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Example of Log enablement menus from the Web UIs:



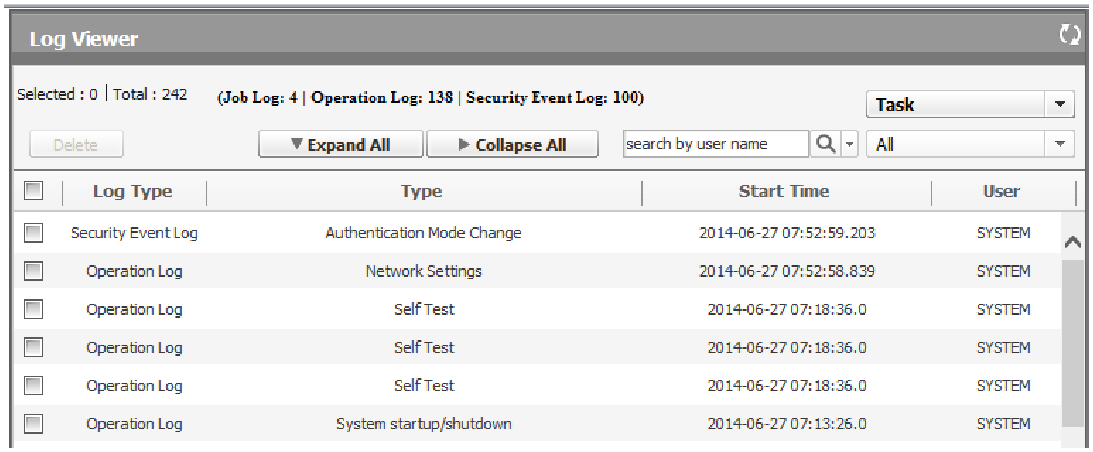
Log Configuration

Job Log :	☑ Enable
Operation Log :	☑ Enable
Security Event Log :	☑ Enable

Log Backup

Log Backup :	□ Enable
Schedule :	Daily
Time :	12 : 00 AM
Protocol :	FTP
Server Address:	127.0.0.1

Example of Log viewer:

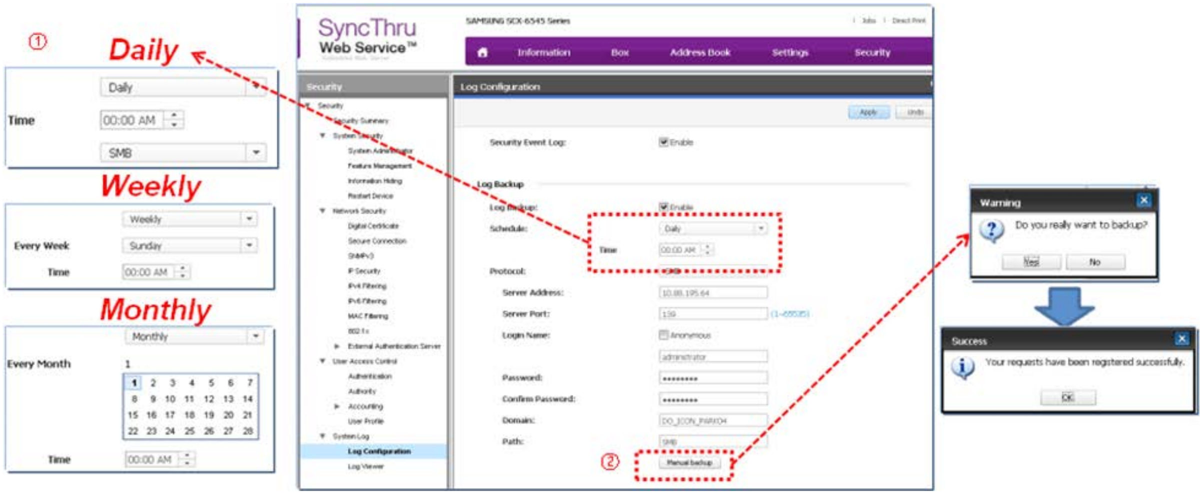


Log Viewer

Selected : 0 | Total : 242 (Job Log: 4 | Operation Log: 138 | Security Event Log: 100)

□	Log Type	Type	Start Time	User
□	Security Event Log	Authentication Mode Change	2014-06-27 07:52:59.203	SYSTEM
□	Operation Log	Network Settings	2014-06-27 07:52:58.839	SYSTEM
□	Operation Log	Self Test	2014-06-27 07:18:36.0	SYSTEM
□	Operation Log	Self Test	2014-06-27 07:18:36.0	SYSTEM
□	Operation Log	Self Test	2014-06-27 07:18:36.0	SYSTEM
□	Operation Log	System startup/shutdown	2014-06-27 07:13:26.0	SYSTEM

Example of the Log back-up process from the SyncThru^{TM} Web Service UI:



Daily: Daily, Time: 00:00 AM, SMB

Weekly: Weekly, Every Week: Sunday, Time: 00:00 AM

Monthly: Monthly, Every Month: 1, Time: 00:00 AM

Log Configuration

Security Event Log: ☑ Enable

Log Backup

Log Backup: ☑ Enable

Schedule: Daily

Time: 00:00 AM

Protocol: SMB

Server Address: 10.88.195.64

Server Port: 139 (1~65535)

Login Name: □ Anonymous administrator

Password: ••••••••

Confirm Password: ••••••••

Domain: DO_ICON_PARK04

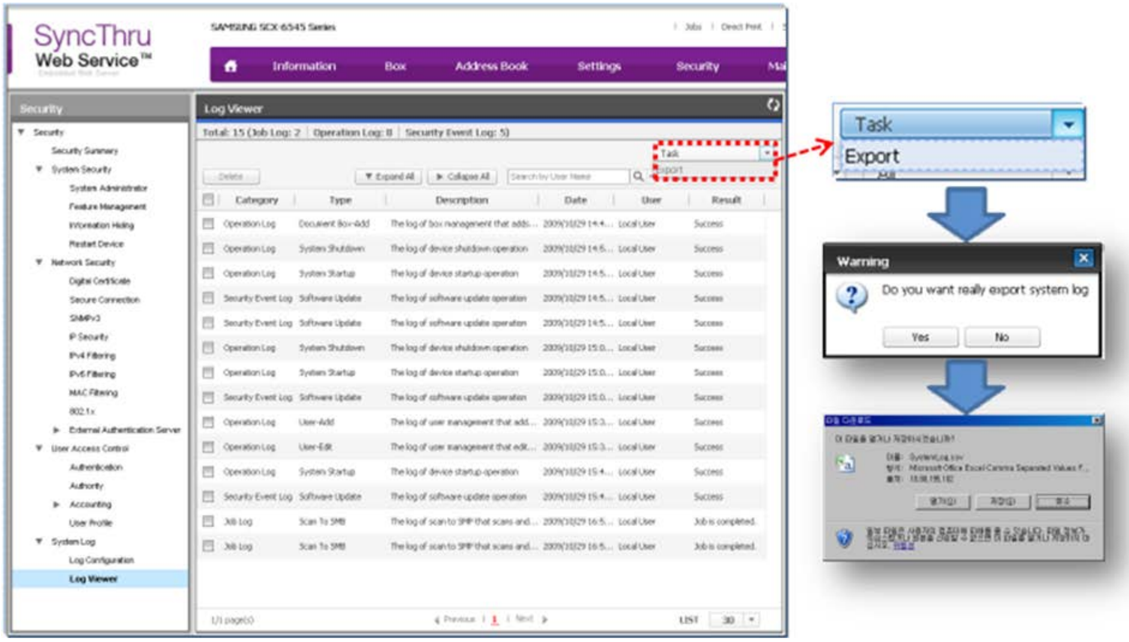
Path: SMB

Warning: Do you really want to backup? Yes No

Success: Your requests have been registered successfully. OK

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Example of the Log Export process from the SyncThru^{TM} Web Service UI:



Log Viewer

Total: 15 (Job Log: 2 | Operation Log: 8 | Security Event Log: 5)

	Category	Type	Description	Date	User	Result
□	Operation Log	Document Box-Add	The log of box management that adds...	2009/10/29 14:4...	Local User	Success
□	Operation Log	System Shutdown	The log of device shutdown operation	2009/10/29 14:5...	Local User	Success
□	Operation Log	System Startup	The log of device startup operation	2009/10/29 14:5...	Local User	Success
□	Security Event Log	Software Update	The log of software update operation	2009/10/29 14:5...	Local User	Success
□	Security Event Log	Software Update	The log of software update operation	2009/10/29 14:5...	Local User	Success
□	Operation Log	System Shutdown	The log of device shutdown operation	2009/10/29 15:0...	Local User	Success
□	Operation Log	System Startup	The log of device startup operation	2009/10/29 15:0...	Local User	Success
□	Security Event Log	Software Update	The log of software update operation	2009/10/29 15:0...	Local User	Success
□	Operation Log	User-Add	The log of user management that add...	2009/10/29 15:3...	Local User	Success
□	Operation Log	User-Edit	The log of user management that edit...	2009/10/29 15:3...	Local User	Success
□	Operation Log	System Startup	The log of device startup operation	2009/10/29 15:4...	Local User	Success
□	Security Event Log	Software Update	The log of software update operation	2009/10/29 15:4...	Local User	Success
□	Job Log	Scan To SMB	The log of scan to SMP that scans and...	2009/10/29 16:5...	Local User	Job is completed.
□	Job Log	Scan To SMB	The log of scan to SMP that scans and...	2009/10/29 16:5...	Local User	Job is completed.

Do you want really export system log

11.3 System Back-Up

The MFP System Back-Up feature allows you to back-up important data on the MFP to ensure quick disaster recovery. The information you can back-up on the MFP includes the following:

- Logs
- Mailbox
- Address Book

11.4 Email Notification

The Samsung MFPs are capable of using your email system to notify you when the MFP needs your attention. This process allows you to respond to MFP issues faster and increase productivity.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

11.4.1 Device Alert Notification

When a Samsung MFP experiences an event that needs your attention such as, out of paper or low toner, the MFP can send you an email.

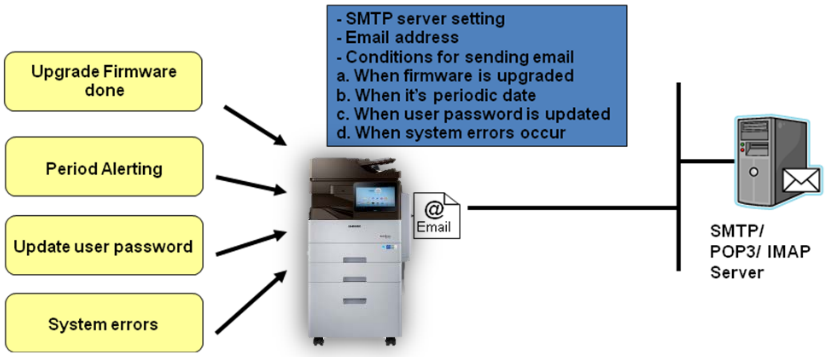
This feature requires the following settings in the MFP to be configured:

- SMTP server
- Email addresses
- Event thresholds.

Events can include the following:

- Firmware upgrades
- User password expiration
- System errors.

Example of Email notification workflow:


Upgrade Firmware done
Period Alerting
Update user password
System errors
- SMTP server setting
- Email address
- Conditions for sending email
a. When firmware is upgraded
b. When it's periodic date
c. When user password is updated
d. When system errors occur
@
Email
SMTP/
POP3/ IMAP
Server

11.4.2 Device Status Notification

Device status can be notified to Administrator by Email periodically. Device status includes the following:

- Configuration Report
- Counter Information Report
- Email Sent Report
- Fax Sent Report
- Network Accounting Report
- Standard Accounting Usage Report
- Standard Accounting Remain Report

And you can specify notification period as:

- Every page
- Daily
- Weekly
- Monthly
- Or every 100 to 10000 pages.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

12. Samsung Business Core™ MFP Security Solutions

The Samsung core business MFP security solutions include the following:

- Cloud Connector

- Secure Login Manager

- SecuThru™ Lite 2

- Usage Tracker

Each of these core business MFP security solutions are discussed in detail in the following section.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

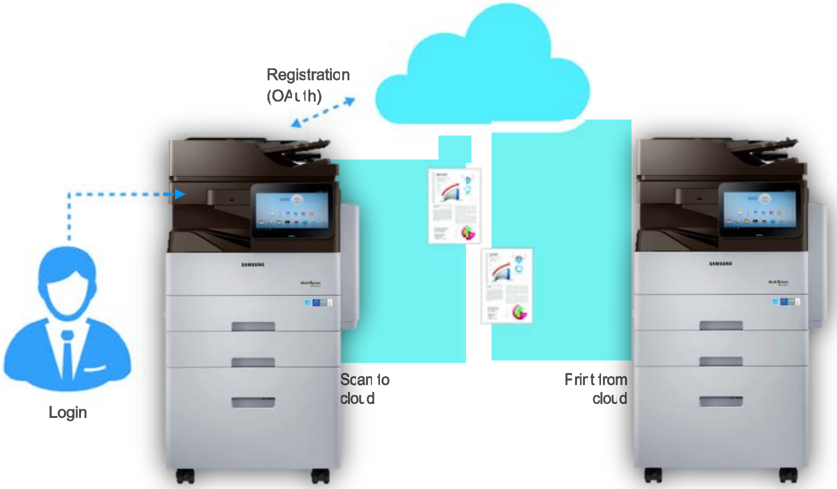
12.1 Cloud Connector

With the Samsung Cloud Connector solution, users can directly scan to, and print from, the Cloud. Users can also preview the content before uploading to the Cloud.

Easy, Secure Access to the Cloud

Cloud Connector supports a variety of Cloud services and provides an easy way to upload, scan, and access content for printing directly without an additional server. Supported Cloud services include Google® Drive and Microsoft® Sharepoint® Online. Additional Cloud services will be supported as they become available.

Secure authentication and authorization for Google®Drive online storage service is provided by the use of OAuth 2.0 for secure file access.



Support for Various File Formats and Cloud Services

Cloud Connector can accept PDF, TIFF, and XPS scans and can print PDF and Google® Drive formats.

With the ability to support various file formats and services including Microsoft® SharePoint® Online, Google® Drive, One Drive, Evernote and Hightail, Cloud Connector allows users achieve the most efficient and convenient experience possible.

SharePoint® Online Evernote OneDrive Dropbox Hightail	Scan (Upload)	PDF (Secure & Searchable), XPS, TIFF, JPG
	Print (Download)	PDF (Secure & Searchable), TIFF, JPG
	Scan (Upload)	PDF (Secure & Searchable), XPS, TIFF, JPG

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

	Print (Download)	PDF (Secure & Searchable), TIFF, JPG, Google Document*

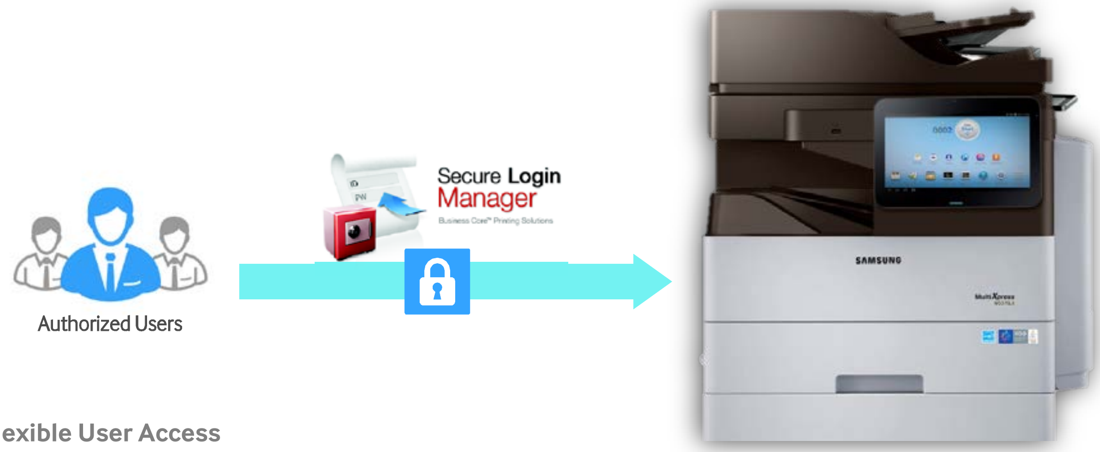
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

12.2 Secure Login Manager

In today's fast-paced business environment, it is essential that companies protect valuable devices from unauthorized access and use. To ensure that only authorized users log in to the systems, Samsung has developed Secure Login Manager. This authentication security solution supports a variety of authentication methods and types for SMBs.

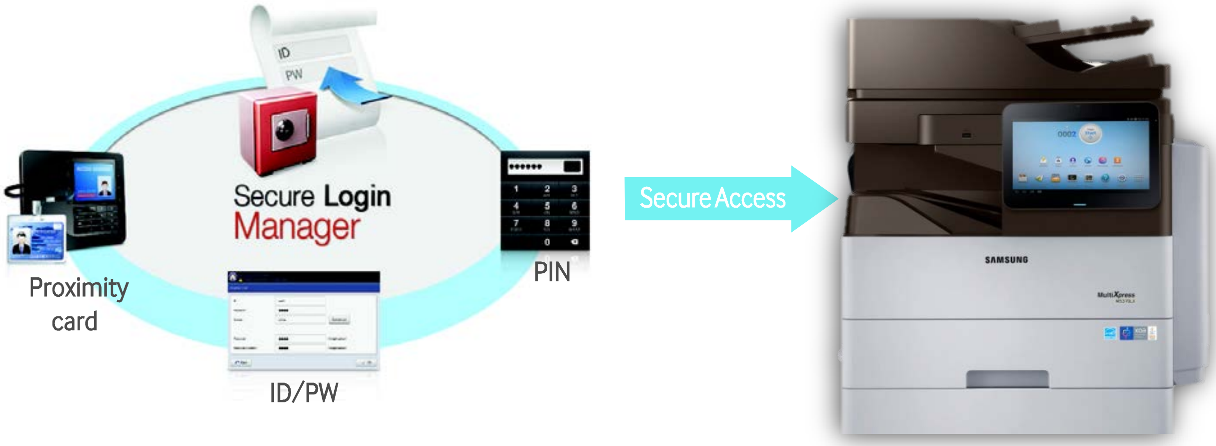
Secure Authentication

Protect access and usage of your valuable MFP devices from unauthorized personnel by using secure login authentication. Only authorized users will be able to access permitted functions.



Flexible User Access

Secure Login Manager supports a variety of authentication types, including ID/Password, proximity card and Personal Identification Number (PIN). The optimal access method can then be chosen based on the situation and preference of each SMB.



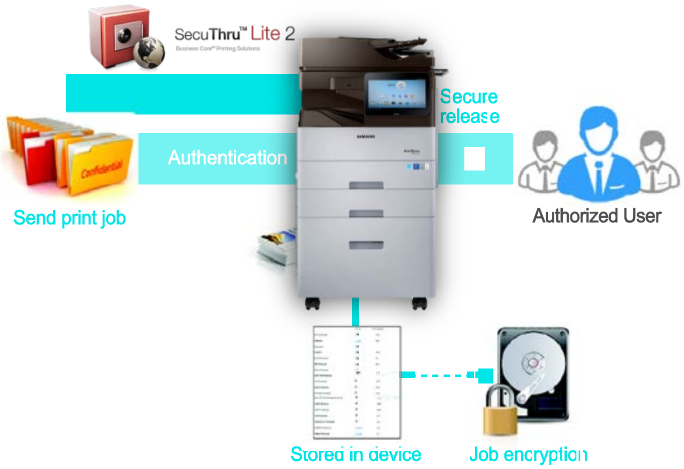
Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

12.3 SecuThru™ Lite 2

The modern SMB requires much more than high-quality network printing and multifunction devices. Business and IT managers demand productive solutions that handle document output effectively and securely while keeping costs under control. Samsung SecuThru^{TM} Lite 2 raises business print environment security to the same high level as that of the overall IT infrastructure, quickly and cost-effectively.

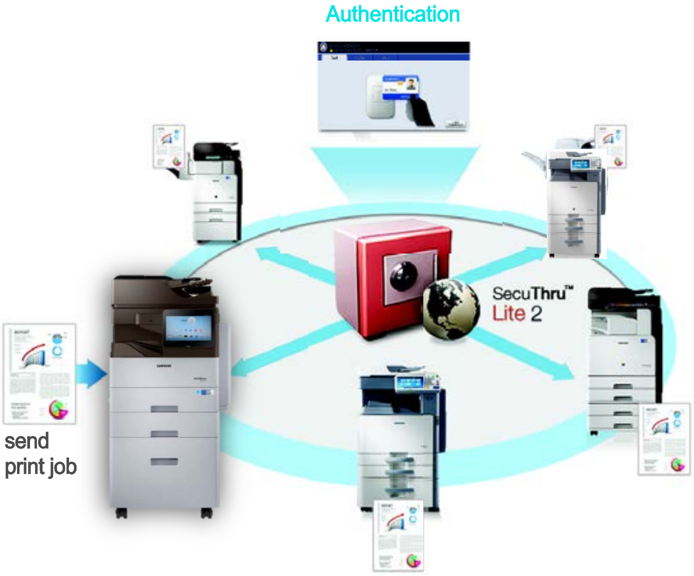
Secure Authentication and Release

SecuThru^{TM} Lite 2 provides secure authentication and release of documents. When the user sends a document to a printer, all jobs are temporarily stored in the device securely through encryption. Once the authorized user provides authentication the document is then released. By utilizing this safe and efficient user authentication flow, enterprise-level security can be professionally supported.



Serverless, Secure Pull Printing

Equipped with secure pull printing, SecuThru^{TM} Lite 2 ensures only authorized users can pull documents from up to 10 compatible devices connected to the network. This allows you to safely and conveniently share print jobs while protecting confidential documents. Delivers print jobs securely, only to authorized users, through a flexible authentication process supporting up to 500 users.



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Reduced Printing Costs

This output management solution helps SMBs reduce printing cost by providing pull printing capabilities that reduce paper usage from unclaimed printouts.

Additionally, solution allows SMBs to save expenses by eliminating the costly need for an additional server.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

12.4 Usage Tracker

The Samsung Usage Tracker solution provides businesses with the ability to remotely manage and monitor functionality of multiple devices, which offers a big advantage to any business. This advantage is especially important for SMBs that need to keep operating costs at a minimum.

Printing-Cost Tracking

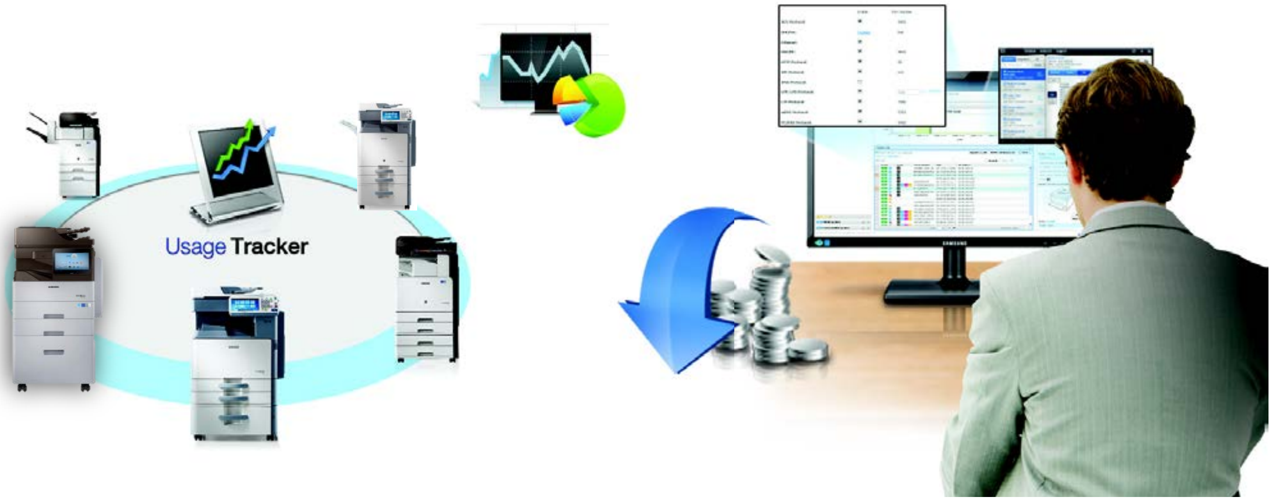
With the Usage Tracker tool, easily track printing and copying counts and cost as well as scanning and faxing counts without a server. Conveniently utilize the touch screen user-interface of a compatible device for intuitive right-away tracking of one or multiple devices integrated in the network environment.

This solution also creates historical or current time-based reports.

01 20 12 80
PRINT SCAN FAX COPY
50 19 04 37
PRINT SCAN FAX COPY
Usage Tracker
62 35 05 21
PRINT SCAN FAX COPY
85 07 39 62
PRINT SCAN FAX COPY

Proactive Monitoring

Monitor device usage from a central location with email notifications. By proactively monitoring print device and function usage, IT staff can more efficiently manage their print environments. IT managers can aggregate reports on up to 10 compatible devices.



Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

13. Smart Print UX with Android Security

Smart Printing UX

Samsung introduced new MFP products that provide a versatile smart printing UX by using an Android User Interface along with a 10.1" Color touch Panel LCD. It provides easy, intuitive, expansible user experience. To ensure that your MFP maintains a high level of quality and offers a consistent experience for your users, Samsung certified these MFPs with Google's CTS (Compatibility Test Suite) certification.

MX4 Series

X4300LX/4250LX/4220LX
K4350LX/4300LX/4220LX

M53 Series

M5370LX/4370LX

M4580 Series

M4580FX/M4583FX

Securing an open platform requires robust security architecture and rigorous security programs. Android was designed with multi-layered security that provides the flexibility required for an open platform, while providing protection for all of the users of the platform. Android was designed with device users in mind. Users are provided visibility into how applications work, and provided with control over those applications. This design includes the expectation that attackers will attempt to perform common attacks, such as social engineering attacks to convince device users to install malware, and attack third-party applications on Android. Android was designed to both reduce the probability of these attacks and the impact of the attack in the event it was successful.

Samsung has developed security mechanism and user access control to improve Android security. Samsung provides the Samsung Application Store which allows users to access powerful Android application. These applications are verified by Samsung Printing Division's auditor to guarantee the security level of each application. Note that only an administrator can install additional applications. This will prevent any application (malware) using third-party applications to reveal a customer's valuable information. If customers do not want to install any additional applications on the MFP, Samsung provides an Application Locking Solution that prohibits the installation of any additional applications.

Samsung continuously improves its security abilities and offerings to improve Android level security.

For more detail information about Android Security, please refer to the following link:

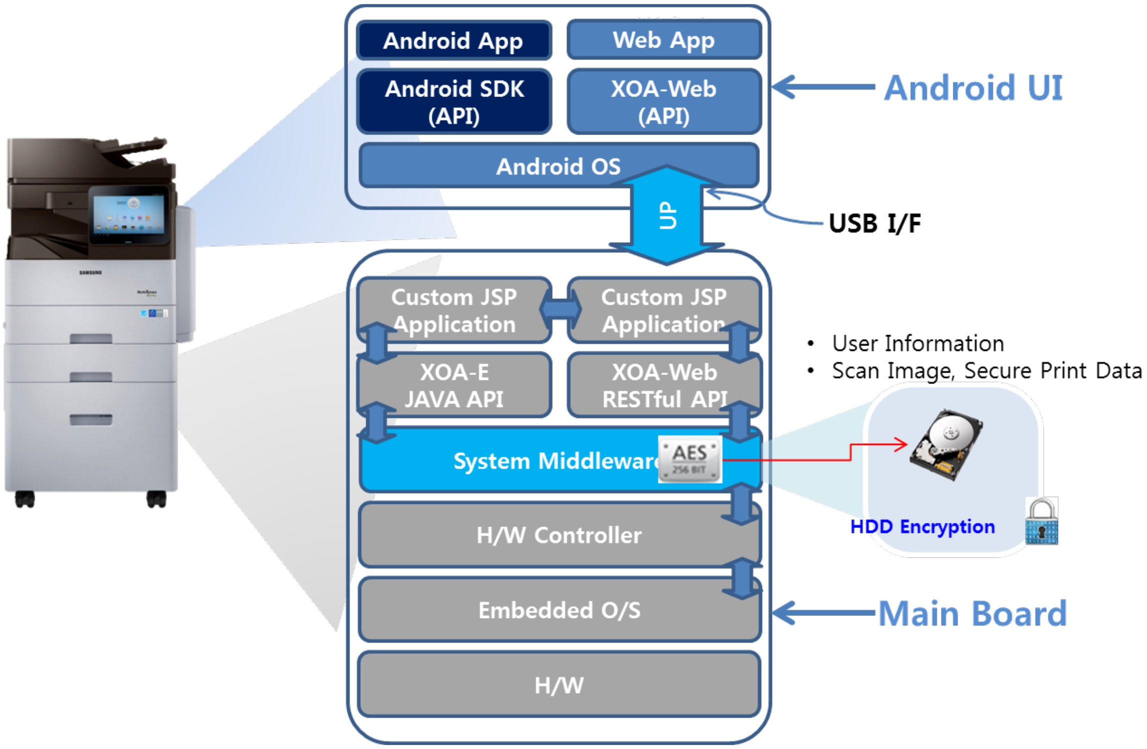
http://source.android.com/devices/tech/security/index.html

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

Portions of this page are modifications based on work created and shared by the Android Open Source Project and used according to terms described in the Creative Commons 2.5 Attribution License.

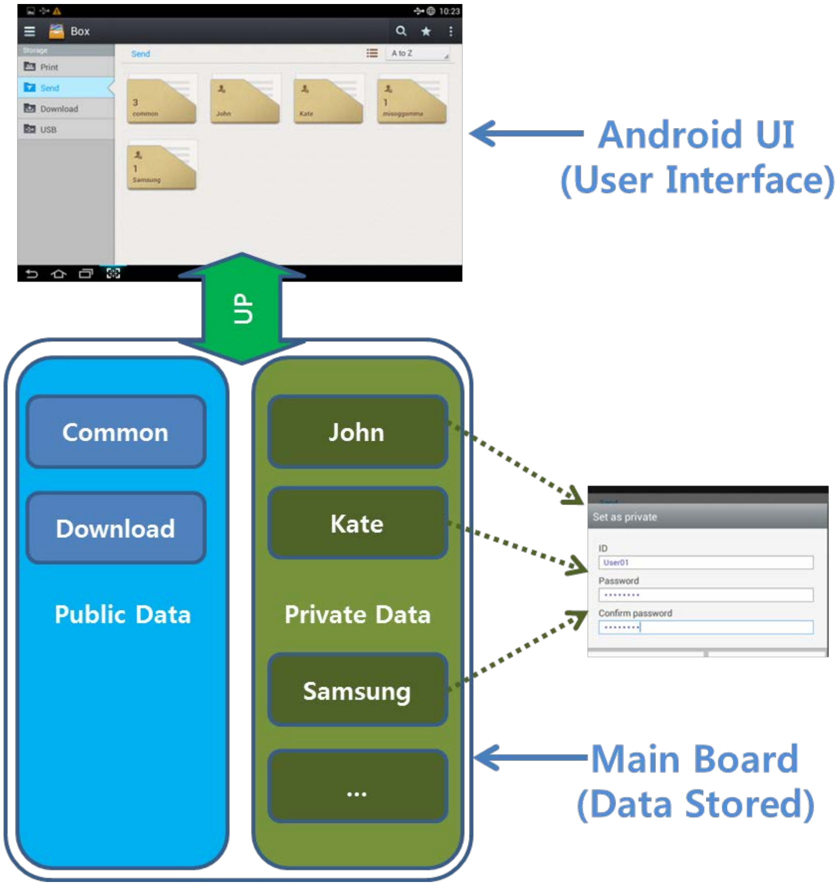
13.1 System Security (MFP with Android UI)

Samsung MFP consists of two systems (Main board and Android UI) and they communicate with each other using USB Interface in private way. Main board performs most features of MFP and stores user data. On the other side, UI Android system provides user interface function and UI system stores only Android App information. It does not handle and store user data and images. Thanks to this structure, main board and UI is separated each other logically and physically. Android UI system has very limited access to main board storage.

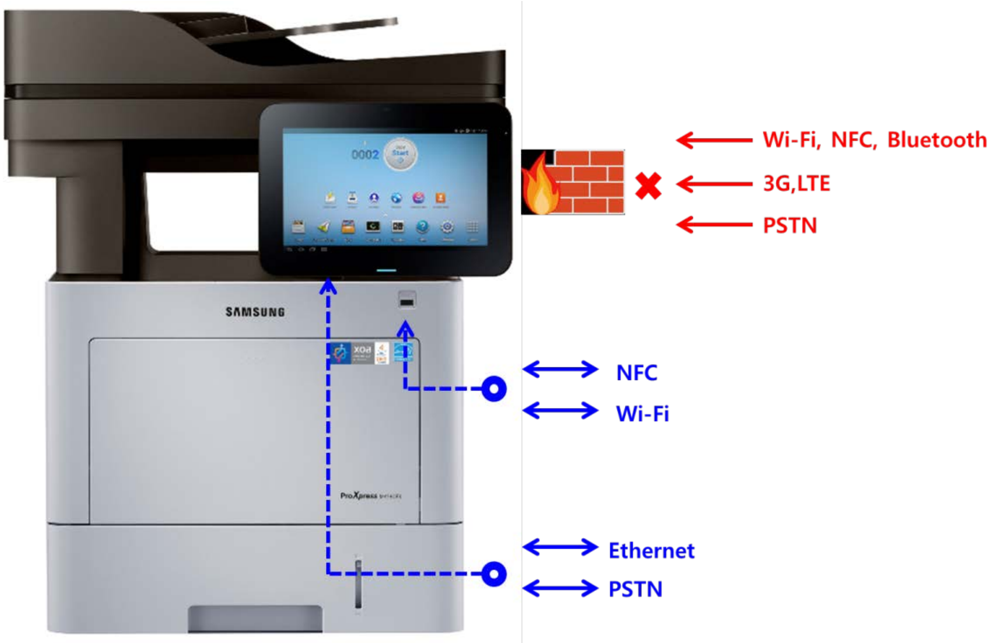


User data (Scan Image, Address book and so on) are stored in main board. For example, user can operate MFP machine using Android UI and start to scan documents. Then images scanned are stored in main board system so images are in safe area. Furthermore, the main board system separates the data storage into personal and public area. If user wants to store data in secure way, the user can create the private folder using ID and password.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.



The Android UI system is blocked to communicate with other network devices directly. All communication is available only through main board network. So, Android UI system can be managed by main board and it is safe from external network access. In case of an application has been installed on the Android UI allowing connections, it will then allow external connections to be established.

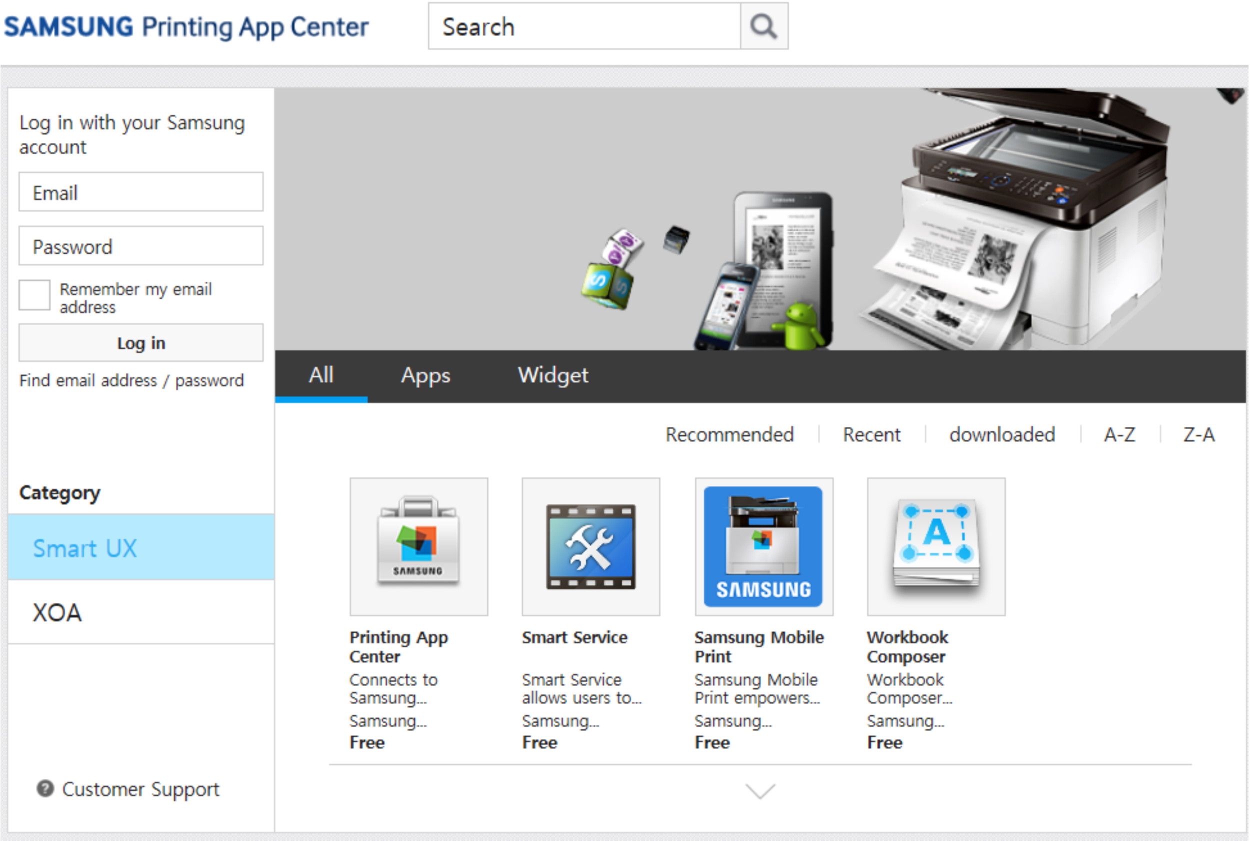


Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

13.2 Android UI Security

13.2.1 Installation of Android App

Samsung provides “Samsung Printing App Center” to share useful and safe applications. All applications are verified in view of security. (http://printingapps.samsung.com)


SAMSUNG Printing App Center
Search
Log in with your Samsung account
Email
Password
Remember my email address
Log in
Find email address / password
Category
Smart UX
XOA
Customer Support
All
Apps
Widget
Recommended
Recent
downloaded
A-Z
Z-A
SAMSUNG

Printing App Center
Connects to Samsung...
Samsung...
Free

Smart Service
Smart Service allows users to...
Samsung...
Free

Samsung Mobile Print
Samsung Mobile Print empowers...
Samsung...
Free

Workbook Composer
Workbook Composer...
Samsung...
Free

Only administrator can install Android application but, general user cannot install anything.

13.2.2 Android App security management

Samsung MFP supports a few methods to keep system security.

- Home Screen Lock

Administrator can prevent to change “Home Screen” by general user.

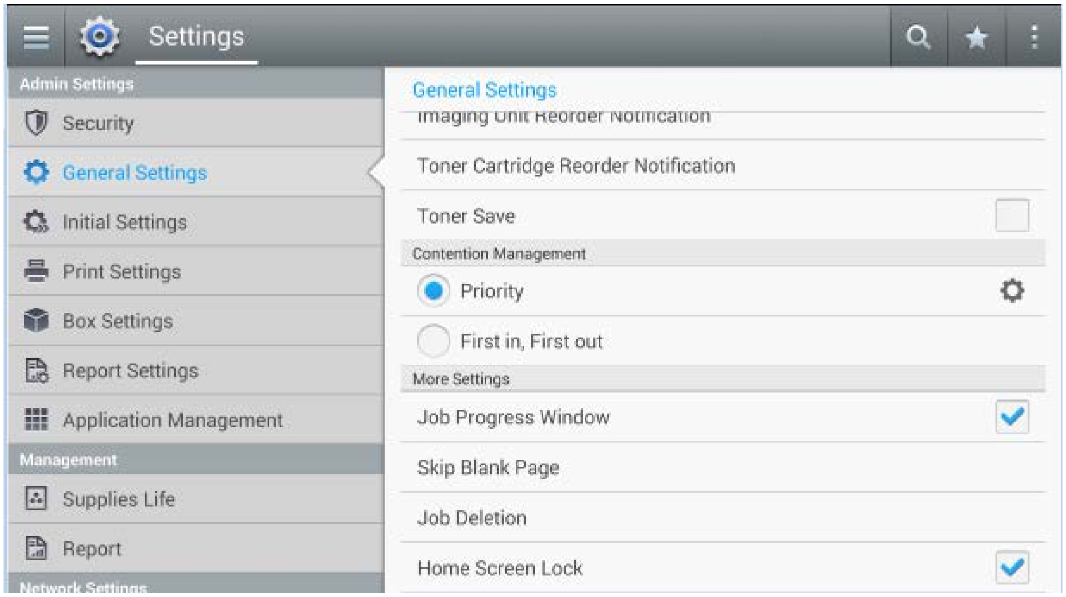
If Home Screen Lock is enabled,

- The user can't move icons and widgets.
- The user can't remove icons and widgets.
- The user can't add icons and widgets.
- The user can't change background.

This function can be enabled from the Local UI and SyncThru™ Web Service UI

After admin login, Click device -> Settings -> Admin Settings -> General Settings -> home Screen Lock -> checked

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.



General Settings

Imaging Unit Reorder Notification

Toner Cartridge Reorder Notification

Toner Save □

Contention Management

● Priority

○ First in, First out

More Settings

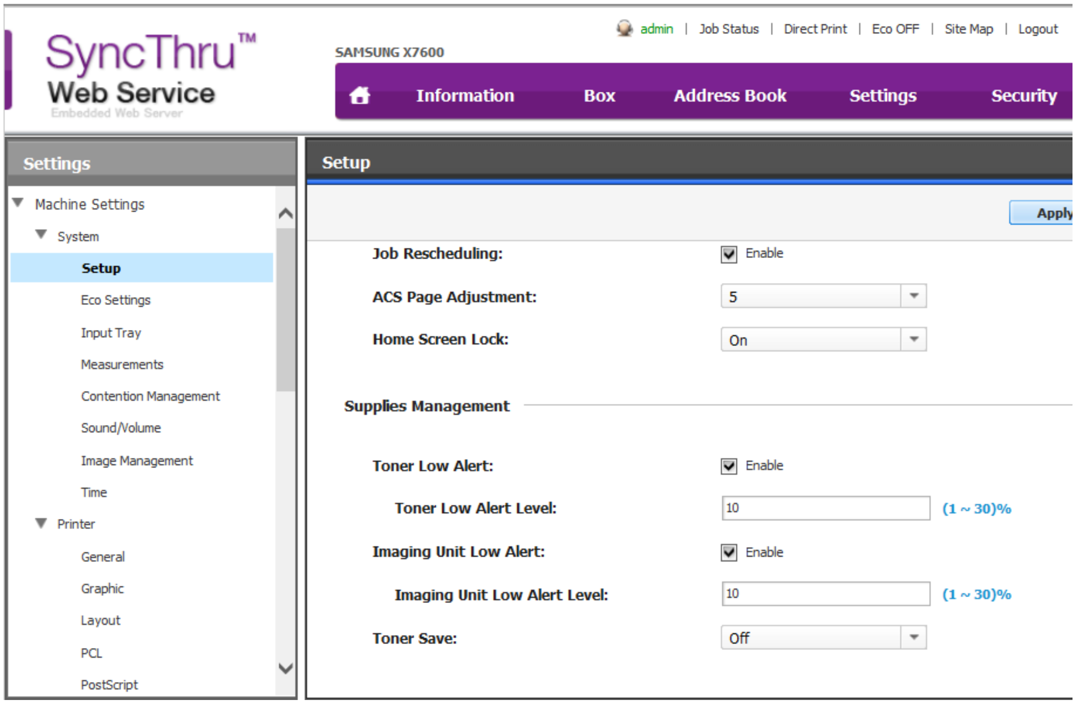
Job Progress Window ☑

Skip Blank Page

Job Deletion

Home Screen Lock ☑

After admin login, Click SWS -> Settings -> Machine Settings -> System -> Setup -> General -> home Screen Lock -> On then apply



Setup

Job Rescheduling: ☑ Enable

ACS Page Adjustment: 5

Home Screen Lock: On

Supplies Management

Toner Low Alert: ☑ Enable

Toner Low Alert Level: 10 (1 ~ 30)%

Imaging Unit Low Alert: ☑ Enable

Imaging Unit Low Alert Level: 10 (1 ~ 30)%

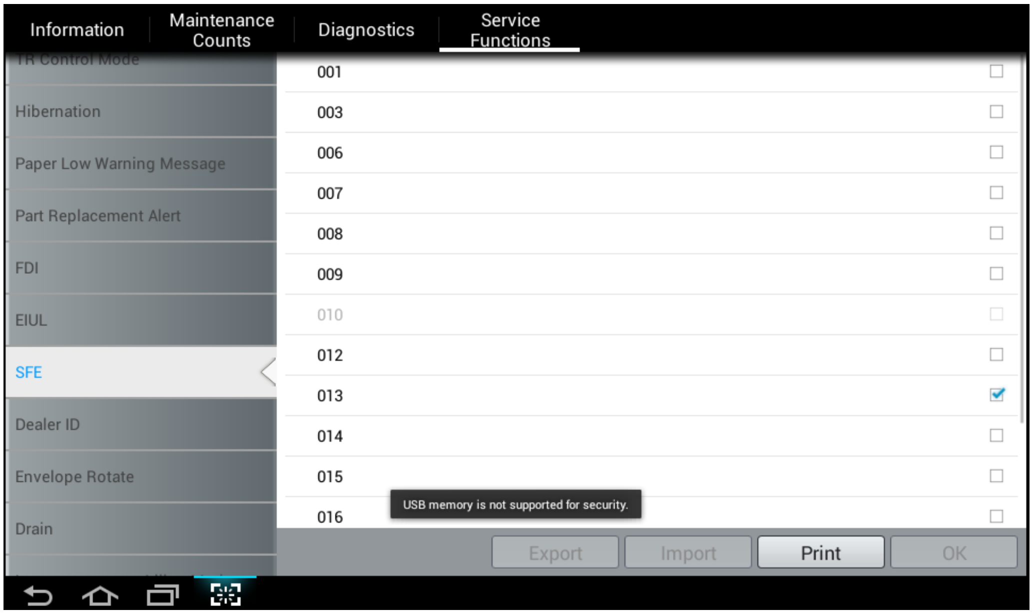
Toner Save: Off

- SFE (Special Feature Enable)

In Service Mode, admin can enable SFE feature for Android UI security.

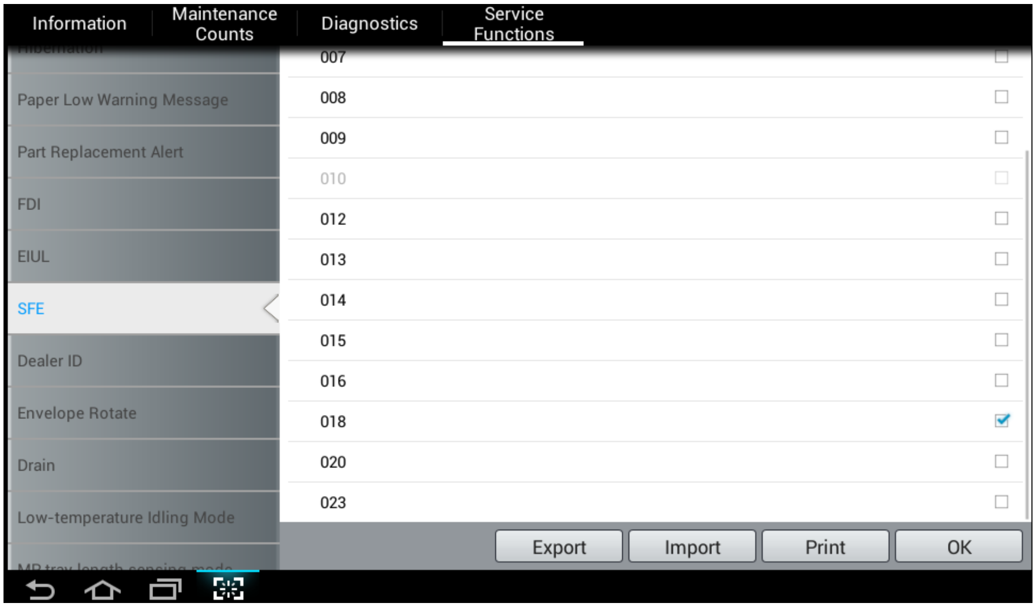
- SFE 013 (Ignore USB memory stick): When SFE 013 is enabled; MFP blocks all USB memory access including Android App installation by USB.
- SFE 018 (Disable 'apk' installation): When SFE 018 is enabled; MFP blocks 'apk' installation.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.



001 □
003 □
006 □
007 □
008 □
009 □
010 □
012 □
013 ☑
014 □
015 □
016 □

USB memory is not supported for security.

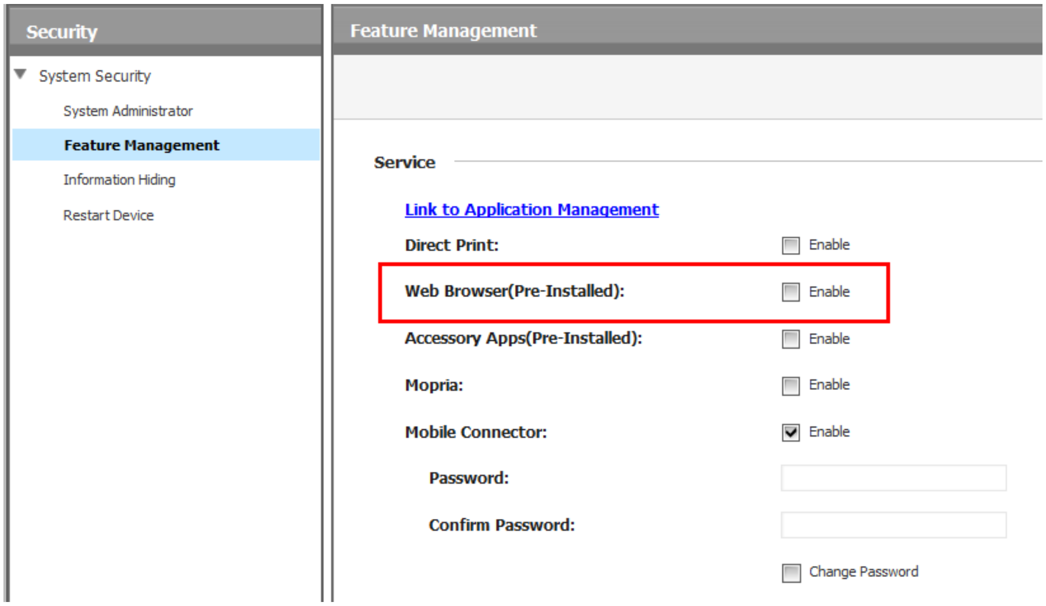


007 □
008 □
009 □
010 □
012 □
013 □
014 □
015 □
016 □
018 ☑
020 □
023 □

- Android UI Web Browser application Security

Android UI Web Browser application can be managed in secure way. Administrator can prevent all users using 'Web Browser'. After admin login, Click SWS -> Security -> Feature Management -> Service -> Web Browser -> select 'Enabled' or 'Disabled'.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.



Service

Link to Application Management

Direct Print: □ Enable

Web Browser(Pre-Installed): □ Enable

Accessory Apps(Pre-Installed): □ Enable

Mopria: □ Enable

Mobile Connector: ☑ Enable

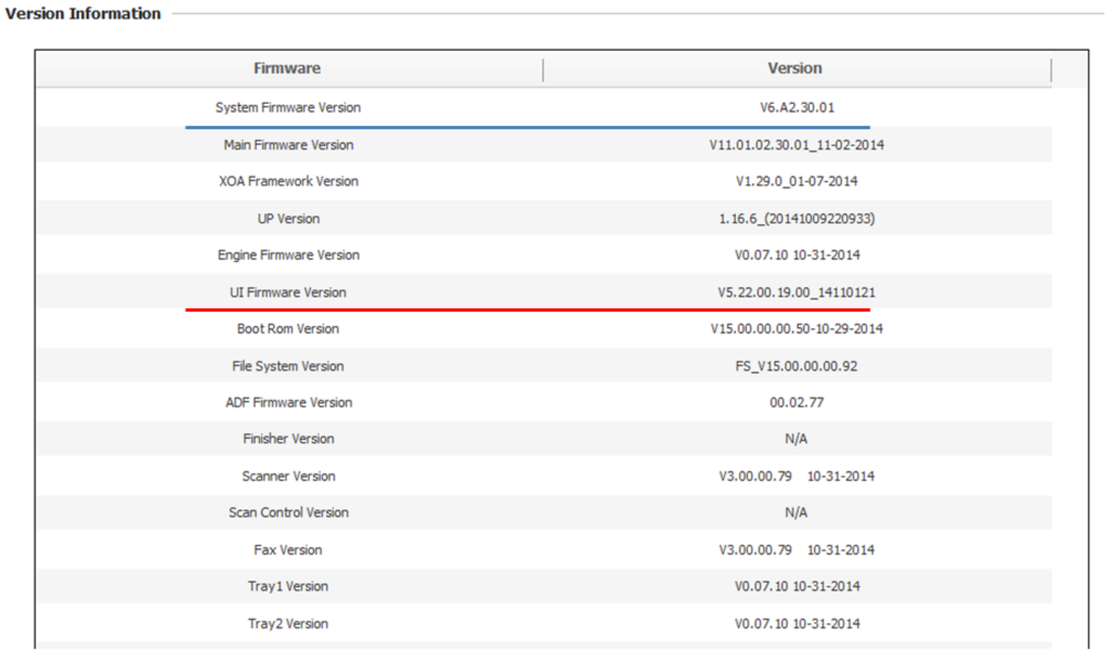
Password:

Confirm Password:

□ Change Password

13.2.3 Android Firmware Security

Samsung provides only one MFP firmware to upgrade and it contains Android firmware built with signature and encrypted. So, administrator can upgrade the one MFP firmware by official firmware upgrade method such as SyncThru^{TM} Web Service and Fleet Admin Pro^{TM}. For system component maintenance, Android UI firmware is managed in System firmware as like below.



Version Information

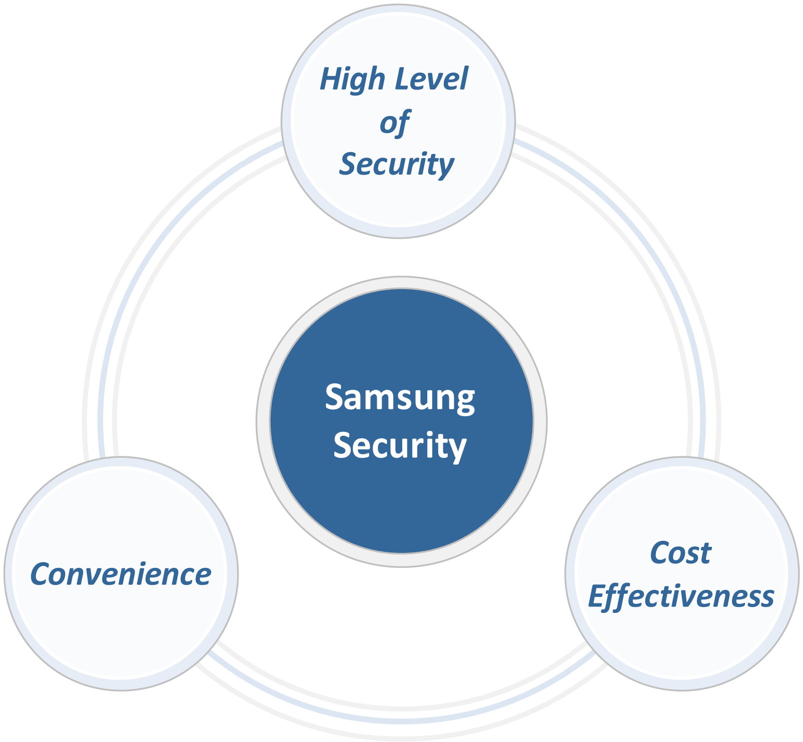
Firmware	Version
System Firmware Version	V6.A2.30.01
Main Firmware Version	V11.01.02.30.01_11-02-2014
XOA Framework Version	V1.29.0_01-07-2014
UP Version	1.16.6_(20141009220933)
Engine Firmware Version	V0.07.10 10-31-2014
UI Firmware Version	V5.22.00.19.00_14110121
Boot Rom Version	V15.00.00.00.50-10-29-2014
File System Version	FS_V15.00.00.00.92
ADF Firmware Version	00.02.77
Finisher Version	N/A
Scanner Version	V3.00.00.79 10-31-2014
Scan Control Version	N/A
Fax Version	V3.00.00.79 10-31-2014
Tray1 Version	V0.07.10 10-31-2014
Tray2 Version	V0.07.10 10-31-2014

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

14. Key Benefits of Samsung MFP Security

With the cost of security breaches and information loss being so high, all IT professionals are looking for products that offer security. The Samsung MFPs offer you the Samsung Security Framework – a five point fortress against unauthorized access to your data. Now your MFP security is one less thing you need to worry about. Samsung offers certified high-level security that is also convenient and affordable. Samsung's "Out of the Box" built-in MFP Security includes the following:

1. **Samsung Security Framework:**
   - Secure User:
     - Authentication
     - Authorization
     - Accounting
     - SSO
     - Access Control
   - Secure Data
     - Encryption
     - HDD Image Overwrite
     - Information Hiding
   - Secure Network & Fax
     - SSL/TLS
     - SNMPv3
     - IPSec (IPv4, IPv6)
     - 802.1x (with EAP)
     - Protocol/Port Management
     - IP/MAC Filtering
     - Watermarks
     - Stamps
   - Secure Document
     - Secure Print
     - Secure Fax
     - Document Tagging
   - Secure Management
     - System Logs
     - System Back-Up
     - Email Notification



2. **Common Criteria Certification:**

   Samsung MFP Security has received EAL 3 certification.

3. **Out of the Box Security:**

   Enjoy Samsung's valuable MFP security features without the need to purchase a "Security Kit" to ensure device security.

4. **End Of Lease:**

   At the end of the lease the user/service can easily erase all data from the MFP/Printer before returning the device.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.

15. Conclusion

Samsung has created an MFP security system that is affordable, convenient, and effective. This security system has been verified and certified by Common Criteria and it complies with IEEE 2600 security standards. Now enterprises and IT managers have a choice for low TCO MFPs with built-in security. The “Out of the Box” built-in MFP security features are perfect for most enterprises and they do not require you to buy a “Security Kit” to ensure your system security.

Samsung is continually working with our customers and designing MFPs that keep your documents safe and secure from internal and external threats. We understand your security requirements and strive to provide value-based security technology that satisfies your needs. Our out-of-the-box comprehensive and reliable security offerings are the foundation to a productive and secure work environment.

Copyright© 2015 Samsung Electronics Co., Ltd., All rights reserved.