

Common Criteria Certification for Samsung Multifunction Printers



Introduction

This white paper describes the Common Criteria certification process used for the Samsung multifunction printers (MFPs) and the MFP security features. The MFPs this paper applies to include the MultiXpress 6345N, 6555N, and C8380ND models.

Overview

The Common Criteria (CC) certification process provides the same level of scrutiny and evaluation to IT security products as the Underwriters Laboratories (UL) provides for electrical products, and ISO 9000 certification provides for manufacturing quality processes. By establishing common evaluation requirements and by standardizing the evaluation methods, the Common Criteria system allows testing facilities to evaluate and certify IT products for use in secure environments. In creating a standardized system for evaluating IT security products, the Common Criteria certification process makes it easier for IT departments to identify which products meet their security requirements.



Many government and military IT departments have adopted CC certification as a requirement for the IT products they purchase. These customers have large IT departments that can account for a significant market share. Samsung's desire to participate in this market sector has led to the pursuit and the acquisition of CC certification for our MFP security features.

Target of Evaluation

Target of Evaluation or TOE is the designation given to the IT security product submitted to the CC laboratory for evaluation. Samsung submitted the MFP TOE with the designation of "Samsung MFP Security Kit Type_A V1.0" to the CC laboratory for evaluation and received an EAL 3 certification.

CC Certified Samsung MFP Security Features

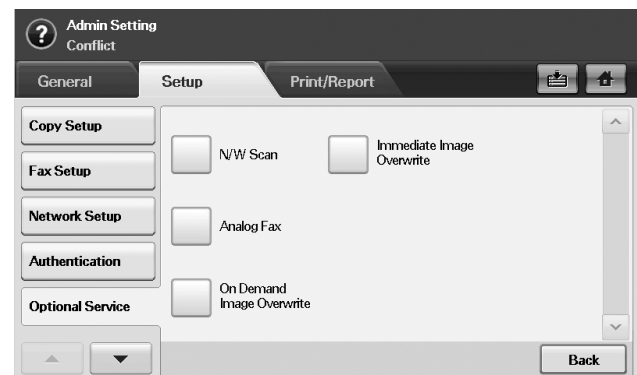
Malicious attacks on IT infrastructure have increased over the years in exponential numbers. The products that make up our IT systems, which we once thought of as passive and unrelated to security, have been exploited. To counteract these attacks, we have employed new security strategies.

Samsung has employed security features on its MFPs to eliminate vulnerabilities to malicious attacks and to protect sensitive information.

The Samsung MFP security features include the following:

- Image Overwrite
- User Authentication
- Security Management
- Security Audit Log
- Data Flow Management
- SyncThru™ Web Service User Interface
- MFP User Interface

Image Overwrite



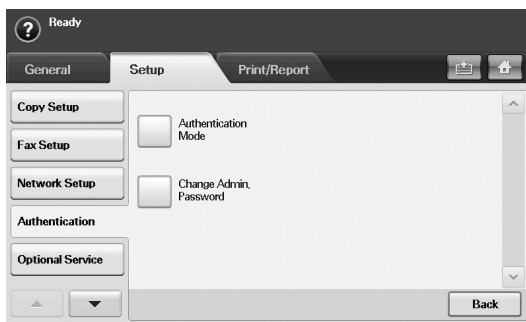
User information created during the copying, printing, network scanning, scanning to e-mail, or scanning to server processes is immediately recorded on the MFP's hard drive. To secure this information, the MFP software implements an image overwrite function to erase image data created during the copying, printing, network scanning, scanning to e-mail, or scanning to server processes. The MFP software performs three overwrite passes of the data using the methods defined in Department of Defense (DoD) 5200.28-M. The MFPs can perform two kinds of image overwrites:

- **Immediate Image Overwrite (IIO)**
The IIO overwrites temporary image files automatically at the completion of each job.
- **On Demand Image Overwrite (ODIO)**
The ODIO function can be performed manually by the system administrator only.

The MFP software implements a hard drive image overwrite security function (IIO) to overwrite temporary files created during the copying, printing, network scan, scan to e-mail, or scan to server process. Immediately after the job has completed, the files on the hard drive are overwritten using a three pass overwrite procedure as described in DoD 5200.28-M. The MFP does not write Fax jobs to the hard drive.

I/O automatically overwrites temporary files created during processing and manually overwrites temporary files created during processing on a specially reserved section of the hard drive. The image overwrite security function can also be invoked manually by the system administrator (ODIO). Once invoked, the ODIO cancels all print and scan jobs, halts the printer interface (network), overwrites the contents of the reserved section on the hard drive, and then the main controller reboots.

User 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 SyncThru™ Web Service interface requires you to enter an account and a password to gain administrative access, while the local MFP user interface requires you to enter a PIN to gain administrative access.

The MFP can restrict the unauthorized network transmission of scanned data in NetScan, Scan to Server, or Scan to Email jobs. The SyncThru™ Web Service administrator creates, modifies, and deletes the accounts and passwords for the network scan service users.

Documents stored on the MFP can be stored using the following methods:

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

- **Secured**
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.

System Authentication

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.

Security Management

Samsung provides tools for managing security features and security data.

Managing Security Features

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 I/O
- Enable or disable ODIO
- Start or stop ODIO
- 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)
- 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 I/O enabling or disabling

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 scan service authentication.
- System audit logs.
- User information for network scan service

System administrators must configure I/O and ODIO to always be enabled. SyncThru™ Web Service administrators must select between **Require Network Authentication** and **Require Local Authentication** for network scan service.

When selected, the **Require Local Authentication** option stores user account information on the MFP hard drive, then network administrator must manage them safely. When selected, the **Require Network Authentication** option stores user information on an authorized server. Users must authenticate by entering their account and password information prior to being granted access to the network resources. That is assuming that the authorized server and remote authentication service are managed safely.

Data Flow Management

Data flow management security prevents unauthorized access to the internal network from a telephone line or a modem used for fax communication. This feature is standard on MFPs that have built-in fax functionality. If the fax functionality is optional, this feature is enabled when the fax option is installed.

The main controller software controls all of the functions of the main controller board as well as the Fax modem board. There is a physical interface between the two. Separation between the PSTN port on the Fax modem board and the network port on the main controller board is established through the architectural design of the main controller software.

For incoming faxes, the Fax modem board will signal a request for service from the main controller, which will initiate the fax receive function of the Fax modem board. The main controller software buffers the entire incoming fax data into the main controller board memory. Once the MFP receives the entire job, the main controller software will disconnect the call at the PSTN port. When fax data is determined to be free of malicious codes and verified to be proper information, the main controller software will initiate the marking function of the IOT software to produce hardcopy output.

Security Audit Logs

The MFP software generates audit logs that track events/actions (e.g., print/scan/fax job submission) to users based on their network login. Each audit log provides the user's identification, event number, date, time, ID, description, and data.

The audit logs are available to SyncThru™ Web Service administrators who can export them for viewing and analysis by using the SyncThru™ Web Service UI.

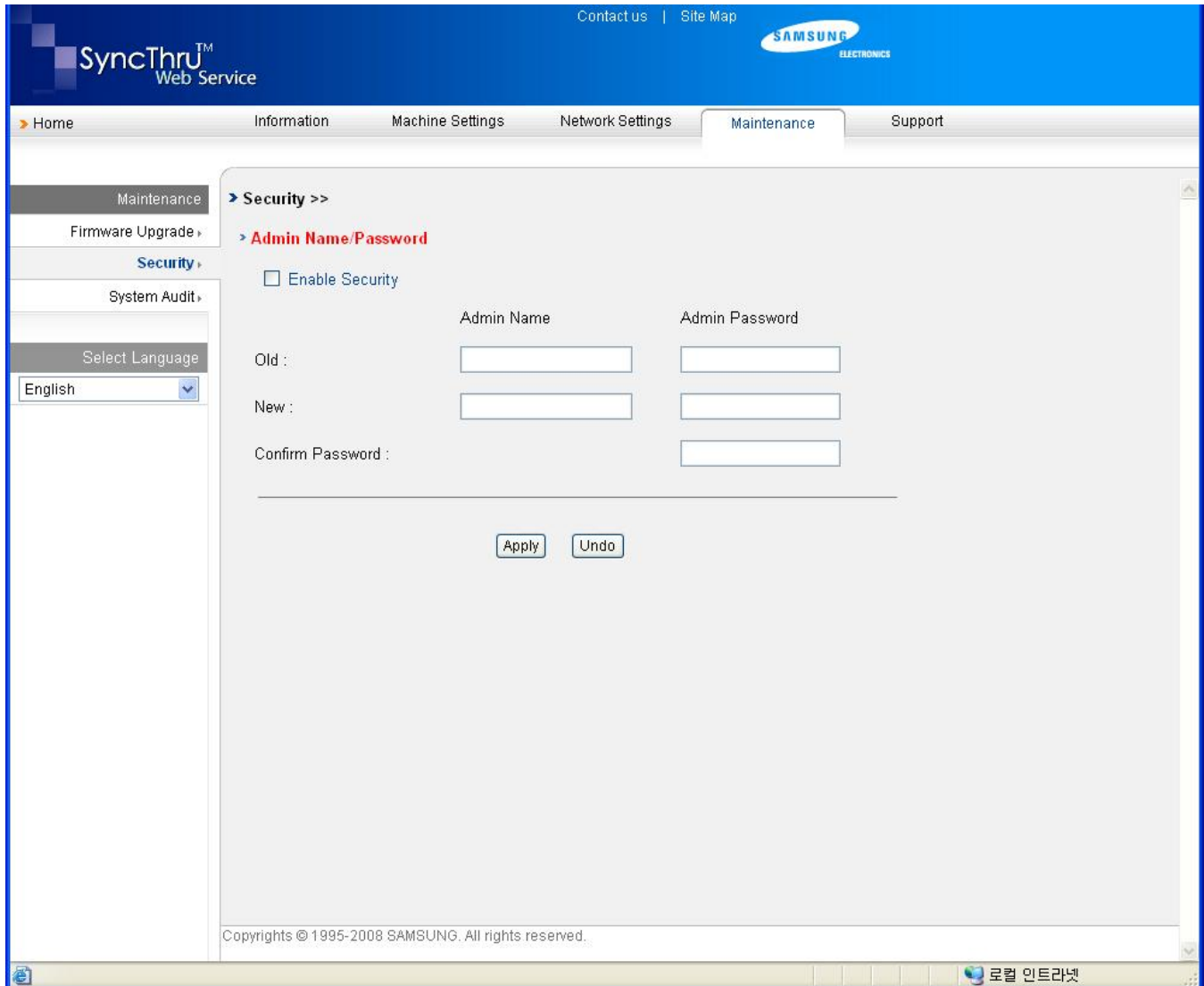
The audit log consists of the following fixed-size input data:
 Input Number (An integer number from 1 to the number of log data)
 Event Date (mm/dd/yyyy)
 Event Time (hh:mm:ss)
 Event ID (Specific number – Refer to the following table)

Event ID	Event Explanation	Input Data
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 faxes received, fax number to receive, destination address.
8	IFAX	The security audit does not support this feature.
9	Scan To Email job	Job name, user name, completion status, I/O job status, SyncThru™ user's account, total number of SMTP receivers, SMTP receivers.
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 faxes, faxes received, destination address.
14	PC-Fax job	Job name, user name, completion status, I/O job status, SyncThru™ user's account, total number of the faxes, faxes received, destination address.

SyncThru™ Web Service MFP User Interface

The browser-based SyncThru™ Web Service UI allows administrators to perform security tasks remotely over the network.

The following is an example of the CC certified SyncThru™ Web Service UI:



MFP User Interface

The user interface built in to the Samsung MFP allows administrators to perform security tasks locally on the MFP. The following is an example of the CC certified local MFP UI:

Users can also securely store and retrieve pages from the MFP by using the Secured option on the local MFP UI:

User Name	File Name	Date	Page
Value 1111	FirstRoww	2001/2/3	1
Value 1111	FirstRoww	2001/2/3	3
Value 1111	FirstRoww	2001/2/3	5
Value 1111	FirstRoww	2001/2/3	7
Value 1111	FirstRoww	2001/2/3	9
Value 2222	Second Roww	2011/2/3	2

Samsung's Roadmap for Common Criteria and Security

Samsung develops more “smart” devices every day, and the opportunity for malicious attacks on these devices is increasing daily. Samsung is dedicated to providing secure devices throughout its vast product line. As we bring more devices to the market and our customers identify areas of security requirements, we will work hard to create solutions that protect our devices from the latest threats. By obtaining Common Criteria certification, we are confirming our dedication to our customers and letting them know that we have met the challenge and successfully secured our devices for their protection.

Samsung is not only reacting to the needs of our customers, we are also helping to define the requirements of all future devices. An example of this effort is the development of a “protection profile” used for Common Criteria Certification. This will be an industry standard developed by many manufacturers. This program will allow printer and MFP manufacturers to have a set of guidelines to use for building secure devices and it will provide Common Criteria laboratories with a checklist for evaluating printer/MFP security. “P2600” is the name of this IEEE Computer Society sponsored program. For more information about P2600, please refer to the following web site: <http://grouper.ieee.org/groups/2600/>

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_CCC_Rev0A, 14 April 2009