

Common Criteria Certification for the MFX-4555 / 5555 Professional Edition

Introduction

This reference sheet describes the Common Criteria certification process used for the MFX-4555 and MFX-5555 Professional Edition sold by Muratec.

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. This results in faster printing and lower power consumption.

Target of Evaluation

Target of Evaluation or TOE is the designation given to the IT security product submitted to the CC laboratory for evaluation. 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.



Common Criteria Certified MFP Security Features

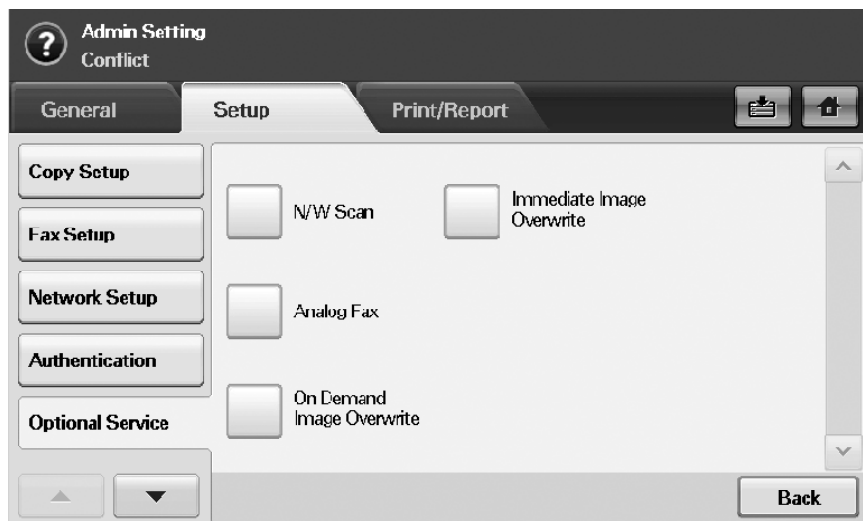
Malicious attacks on IT infrastructure have increased over the years in exponential numbers. The products that make up our IT systems, which we once thought of as passive and unrelated to security, have been exploited. To counteract these attacks, new security strategies have been employed.

Security features have been designed for these MFP's to eliminate vulnerabilities to malicious attacks and to protect sensitive information.

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:

Automatic Image Overwrite

The Automatic Image Overwrite feature overwrites temporary image files automatically at the completion of each job.

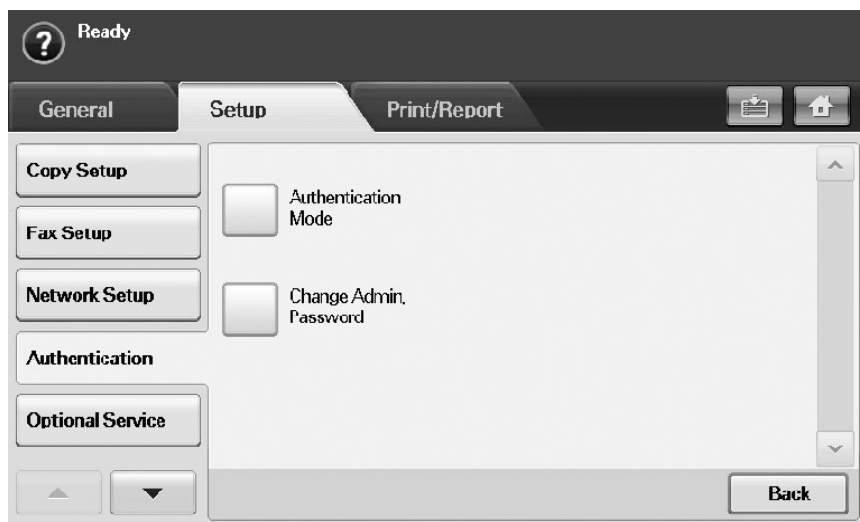
Manual Image Overwrite

The Manual Image Overwrite feature allows the system administrator to manually perform a disk overwrite.

The MFP software implements an automatic hard drive image overwrite security function to overwrite temporary files created during the copying, printing, network scanning, scanning to e-mail, or scanning to server processes. 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.

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. 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.

User Authentication



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 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 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

The MFX-4555 and MFX-5555 provide feature 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 Automatic Image Overwrite
- Enable or disable Manual Image Overwrite
- Start or stop a Manual Image Overwrite
- 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 image overwrite 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 image overwrites 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. The fax functionality on the MFX-4555 and MFX-5555 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 contain the print job activity information for each user 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	Manual Image Overwrite started	Device name, serial number of the device.
4	Manual Image Overwrite complete	Device name, serial number of the device, completion status.
5	Print Job	Job name, user name, completion status, Automatic Image Overwrite status, SyncThru™ user's account.
6	Network scan job	Job name, user name, completion status, Automatic Image Overwrite status, SyncThru™ user's account, total number of the destination address, destination address.
7	Server fax job	Job name, user name, completion status, Automatic Image Overwrite 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, Automatic Image Overwrite 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, Automatic Image Overwrite status, SyncThru™ user's account.
13	Embedded fax job	Job type (sending fax, receiving fax), job name, user name, completion status, Automatic Image Overwrite status, SyncThru™ user's account, total number of faxes, faxes received, destination address.
14	PC-Fax job	Job name, user name, completion status, Automatic Image Overwrite 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:

The screenshot shows a web browser interface for the MFP. At the top, there is a navigation bar with tabs: Home, Information, Machine Settings, Network Settings, Maintenance (selected), and Support. On the left side, there is a sidebar menu with options: Maintenance (selected), Firmware Upgrade, Security (selected), System Audit, and Select Language (English). The main content area is titled '> Security >>' and contains a sub-section '> Admin Name/Password'. It features a checkbox for 'Enable Security' which is unchecked. Below this, there are three input fields: 'Admin Name' (with 'Old :' label), 'Admin Password' (with 'New :' label), and 'Confirm Password :'. At the bottom of the form are 'Apply' and 'Undo' buttons.

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:

The screenshot shows a local MFP user interface. At the top, there is a dark header bar with a question mark icon and the text '01-01-2008 12:00 AM'. Below this is a dark bar with the text 'Network Authentication Login'. The main area is light blue and contains three input fields: 'Auth. ID', 'Password', and 'Realm Name :'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

The screenshot shows a software interface with a dark header bar containing a question mark icon and the text 'Ready'. Below the header are two tabs: 'Public' and 'Secured', with 'Secured' being the active tab. To the right of the tabs are two icons: a printer and a home button. The main area contains a table with four columns: 'User Name', 'File Name', 'Date', and 'Page'. The table has six rows of data. Below the table, there is a page indicator '1/2 Page' and four buttons: 'Detail', 'Edit', 'Delete', and 'Print'.

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