FUJIFILM Business Innovation Multifunction Devices Security White Paper

Jun 1st, 2021

Version 2.1

Introduction

Security Measures for Digital Multifunction Device (MFD)

FUJIFILM Business Innovation has been working on enhancement of information security and ensuring quality by expanding various security functions, compromising response for encryption algorithm, and so on at the development of products to solve customers' information security challenges.

In addition, if challenges on information security risks have been identified after product release, we immediately call a countermeasure meeting and consider an appropriate response in an effort to prevent customers from experiencing contingencies.

For customers who need tighter security, we offer various security services tailored to their business needs.

FUJIFILM Business Innovation makes further efforts to help customers ensure information security through application of cutting-edge technologies to products, appropriate quality management, swift response, and provision of sophisticated information security services.

Also, FUJIFILM Business Innovation has recognized the importance of balance between pursuing added value features and improving their security for a long time. To guarantee MFD security reliability, FUJIFILM Business Innovation has acquired "ISO/IEC15408" certification, which is an international standard for design and operations of information technology security with MFDs and acquired security certification (BLI Security Seal - Device Penetration) by passing the Security Validation Program of Keypoint Intelligence, a U.S. independent assessment agency.

Furthermore, FUJIFILM Business Innovation's MFDs conform to security standards guideline NIST SP800-171 stipulated by the U.S. government.

For details on certified products, please contact your regional sales.

https://www.fujifilm.com/fbglobal/eng

All contents described in this white paper are information as of the date when created. Therefore, its contents are subject to change in the future, as we are planning future enhancements of the service.

Furthermore, please contact us for the applicable machines and details of the functions described in this document.

Organizational Security

Complying with the laws and carrying out our business activities in a fair and honest manner is one of the basic values that we hold dear at FUJIFILM Business Innovation, the manufacturer of office multifunction devices. FUJIFILM Business Innovation and affiliated companies have been working on enhancing this framework and related measures to ensure these guidelines are firmly reflected in the actions of each one of our officers and employees.

For details on FUJIFILM Business Innovation’s corporate ethics and compliance actions, please refer to the following URL:

https://holdings.fujifilm.com/en/sustainability/vision/compliance

While establishing a trustful relationship with customers, FUJIFILM Business Innovation has been committed to improving the level of information security as a professional team who devotes ourselves to think, understand, and solve issues from our customer’s standpoint so that customers can feel secure using solution services and entrust their information asset to us. FUJIFILM Business Innovation and affiliated companies obtain information security related certificates issued by third parties.

For details on publication information on security, please refer to the following URL

https://www.fujifilm.com/fbglobal/eng/company/public/i_security

FUJIFILM Business Innovation continues to strengthen information security governance.

MFD Security Threats and Measures

The following are recognized as security threats for Office MFDs from the viewpoint of data breach, data tampering, and unauthorized data access.

1. Unauthorized operations by other users
2. Eavesdropping and tampering of communication data
3. Unauthorized access to administration functions
4. Software tampering and unauthorized rewriting of software
5. Audit log tampering
6. Breach of document data stored on the device (at return after lease end or device disposal)
7. Data breach caused by careless mistakes of system administrators or users

FUJIFILM Business Innovation Office MFDs provide optimal countermeasures for each expected risk as listed in Tables 1.-7.

Table 1. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
1. Unauthorized operations by other users When individual users perform operation on a device, documents stored on the device and related data will be compromised or tampered if appropriate protection (data access permissions, operation controls, etc.) is not implemented for document data to be handled.	**A) User authentication and permissions** ● **User authentication** You can identify and manage individual users. ● **Restriction in use of functions** Manage each user's usage. ● **Automatic logout** Prevent unauthorized use of MFDs by users other than the logged-in person. ● **Secure Print / Private Charge Print** You can print confidential documents without exposing them to third person. ● **Unified user authentication and permission control** Realize unified user authentication and permission control with ApeosWare Management Suite 2. ● **Centralized control for secure print** ApeosWare Management Suite 2 provides you with a secure printing environment of print jobs after user authentication. Realize secure print by centralized control.

A)User Authentication and Permissions

Authentication Feature

Registering the IC card information as attribute information in Active Directory, LDAP[*1] server, or Azure Active Directory allows the user information managed by the server to be used for user authentication when using MFDs or printers. Even when you forget your IC card, you can use MFDs or printers by entering your user ID and password. It reduces labor for the management for customers who manage various resources on the network using Active Directory, as output devices can also be managed collectively.

*1: Lightweight Directory Access Protocol

IC Card Reader

The authentication feature with a smart card can be realized by just adding an IC card reader to your device. It can link to a wide range of functions including service access control of output devices. This feature enhances both security management and user-friendliness.

IC card reader D is available in three formats: Embedded IC Card Reader, Embedded IC Card Reader for wing table, and external IC Card Reader.

Remote Server Authentication

By registering smart card information with Active Directory or the LDAP* server, you can use user information managed by the server for user authentication when operating the device or printer.

In case you forgot your smart card, you can use the device by entering your user ID and password. For customers who manage a wide range of resources on the network with Active Directory, it reduces time and effort as output devices can be under centralized management as well.

* Light Weight Directory Access Protocol

Feature Access Permissions

Function Access Control is a function of user authentication that restricts MFD functions. All function buttons such as copy or fax can be controlled. Only system administrator can set via the control panel or MFD setting software.

There are 3 types of function control.

1. Device Access control

   Control panel operation can be controlled. When the MFD is started up, Log-in UI appears firstly.

2. Service Access control

   The following services can be controlled. Hiding the service icons can also be set

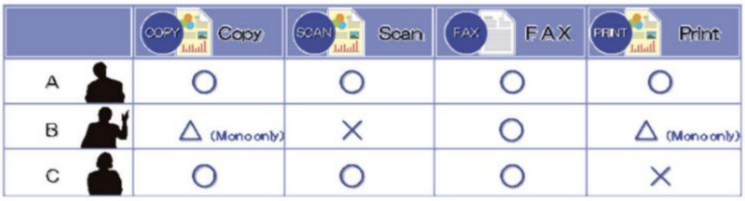
   - Copy
   - FAX/ internet FAX
   - Scan to Folder
   - Scan to PC
   - Scan to Email
   - Folder Operation
   - Job Flow
   - Print by media
   - External Access
   - Print

3. Access control per user

Function access and print & copy quota control can be set per user.

The system administrator sets copy & quota limitation per user via the control panel and MFD setting software.

When print or copy volume exceed the registered number, the user can no longer use the function. System administrator should clear the counted number.



	COPY Copy	SCAN Scan	FAX FAX	PRINT Print
A	○	○	○	○
B	△ (Mono only)	×	○	△ (Mono only)
C	○	○	○	×

Fig. Access Control per user

Access Control to Documents in MFD Folder

You can set a password to an MFD Folder where scanned / faxed documents are stored to protect them. Access to document data by a person who does not have any right can also be controlled by using the authentication mode, which enables user identification.

Automatic Logout

Automatic Logout is a function to prevent another user from accessing the MFD functions as a user previously logged in. □If the device is not in use for a certain period, automatic logout is performed and the device goes back to the initial state.

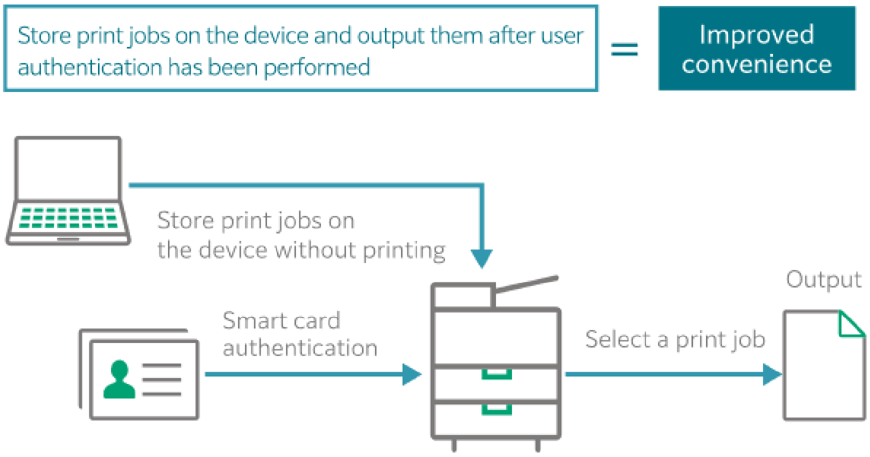
Secure Print

Secure Print helps prevent unauthorized viewers from gaining access to documents by holding jobs in the device until you enter a password.

You can fix the settings for the print driver to Secure Print with a free tool Print Driver Customization Tool.

Private Charge Print

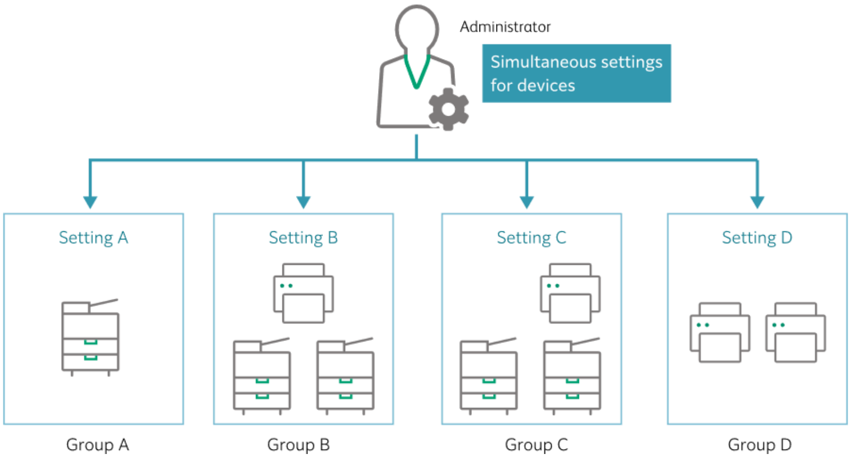
Print jobs are forcibly stored to the storage of the device and output after authentication has been performed. This feature prevents print jobs from being uncollected on the device or incorrect output. In addition, you can change print settings such as the number of copies, 2 sided/1 sided, color/BW and it reduces erroneous printouts and paper wastes and contributes to TCO reduction.


Store print jobs on the device and output them after user authentication has been performed
=
Improved convenience
Store print jobs on the device without printing
Smart card authentication
Select a print job
Output

* Operation in Authentication mode is required.

Unified User Authentication and Permission Control

A server base device management software, ApeosWare Management Suite 2 , can centralize user information for authentication against many devices and provide unified user authentication and permission control without hustle operation by system administrator.



Centralized control for secure print release

ApeosWare Management Suite 2 can also provide a capability to securely release a print job after authentication has been performed. This feature prevents print jobs from being uncollected on the device or incorrect output. The control is centralized at the server and system administrator can manage the settings for many devices at once.

Table 2. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
2. Eavesdropping of communication and tampering of data Eavesdropping of communication or tampering of data may occur when it is exchanged between a PC or file server used for device operations (print, scan, etc.) and the device on the network.	**B) Protection of communication and data** ● **SSL/TLS and IPSec** Encrypt communication between PC / File Server and MFD for information protection. ● **SMBv3, SFTP** Encrypt communication between PC / File Server and MFD for information protection. ● FIPS 140 Enabling FIPS 140-2 certification mode allows for operating with the module that conforms to the U.S. Federal Standard. ● **Digital certificate verification** Verify certificate chain, certificate revocation, and validity period. Certificate update (including the newly issued one), which has been manually performed by an administrator, and associated setting update processing can be automated. ● **Disabling setting by network protocol or port** Prevent unauthorized access and□data breach. ● **Encrypting scanned documents** Prevent data breach with password / public key. ● **Direct print of encrypted documents** You can print directly by decrypting encrypted DocuWorks files and PDF files. ● **E-mail encryption and e-mail signature** Reduce the risk of eavesdropping and tampering during e-mail delivery. ● **Data breach prevention between different interfaces** Prevent attacks on MFDs or internal network via fax line, Secondary Ethernet, wireless LAN, USB port, and malicious programs inside USB memory)

B)Protection of Communication and Data

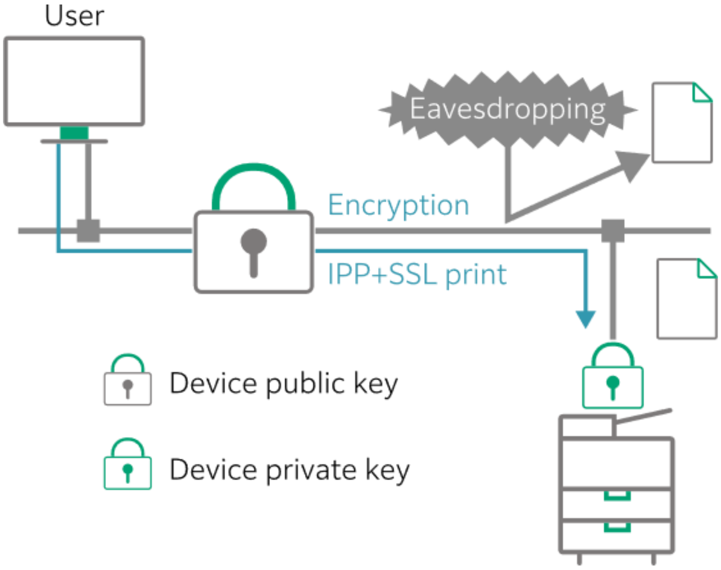
Encrypted Communication between Server or Client PC and MFD (SSL/TLS/IPSec)

You can prevent data breach and tampering in the communication between the device and server or client PC on the network by encrypting communications, assuming if someone attempts unauthorized access on the network. The following are examples of communications that can be encrypted. By default, only TLS1.2 is enabled*, however, TLS1.3 can be supported by changing the settings.

*: TLS1.0/TLS1.1/TLS1.3 are disabled by default.

- Print job using IPP port (print)

Encrypt the communication path of IPP (Internet Printing Protocol) that is used for exchanging print data to prevent eavesdropping on authentication information and print data.

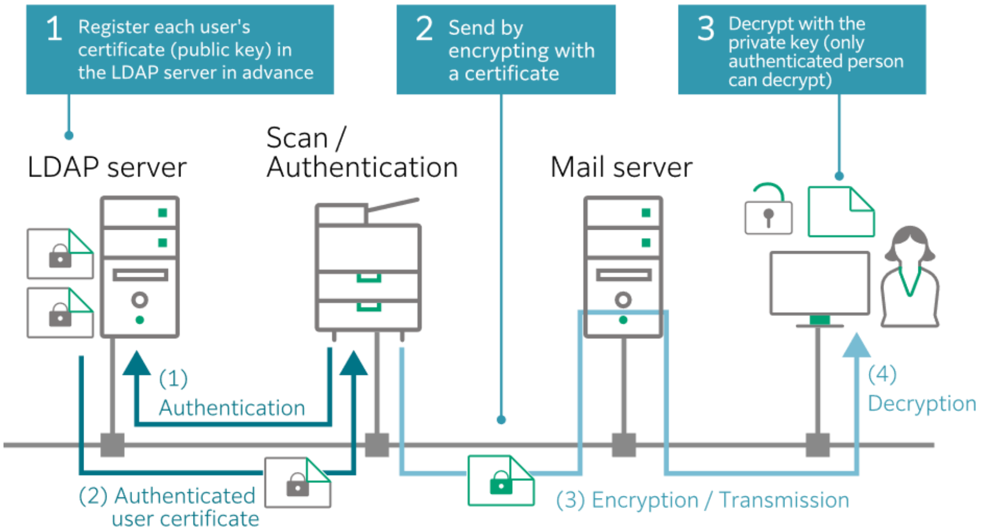


- Secure communication using HTTP

Perform secure HTTP communication when accessing the Internet Services on an MFD from your PC or when accessing an external server from an MFD.

- Communication with LDAP server (Address Book search / authentication)

Encrypt the communication path with the LDAP server to prevent eavesdropping on authentication information and Address Book data.


1 Register each user's certificate (public key) in the LDAP server in advance
2 Send by encrypting with a certificate
3 Decrypt with the private key (only authenticated person can decrypt)
LDAP server
Scan / Authentication
Mail server
(1) Authentication
(2) Authenticated user certificate
(3) Encryption / Transmission
(4) Decryption

- Communication with SMTP server (e-mail)

Encrypts the communication path with the SMTP (e-mail transmission) server to prevent eavesdropping on authentication information and e-mail data.

- Communication with POP server (e-mail)

Encrypts the communication path with the POP (e-mail reception) server to prevent eavesdropping on authentication information and e-mail data.

- Communication with SFTP (scan / file transfer)

hen transferring data to the server by FTP transfer in the job flow, communication path encryption / authentication is performed using the secure shell method to prevent eavesdropping on authentication information and data.

- Communication with SMB (scan / file transfer)

In SMBv3, a communication encryption function has been newly added, and it allows you to send files securely to the destination.

- Encryption of IP communication by IPsec

You can prevent tampering and eavesdropping in units of IP packets between devices in which connection by IPsec has been configured.

In client communication using certificates, SSL server authentication and IPSec PKI authentication prevent spoofing.

- Network device authentication using IEEE802.1X authentication

An authentication standard that regulates the connection of devices to the network when devices connect to each other on the network. As it supports IEEE802.1X authentication, you can securely connect an MFD to the network that is restricted by connected devices.

FIPS 140 compliant

FIPS 140 (Federal Information Processing Standard 140) refers to the U.S. Federal Standard that specifies security requirements concerning cryptographic modules. Setting the FIPS140-2 certification mode to [Enabled] allows for operating with the module that conforms to the FIPS 140.

Digital Certificate Validation

Certificate validation is a function to check a certificate used in a communication such as certification chain, revocation checking and validity period. Reliable verification and management of certificates can be carried out with trust anchor certificate management.

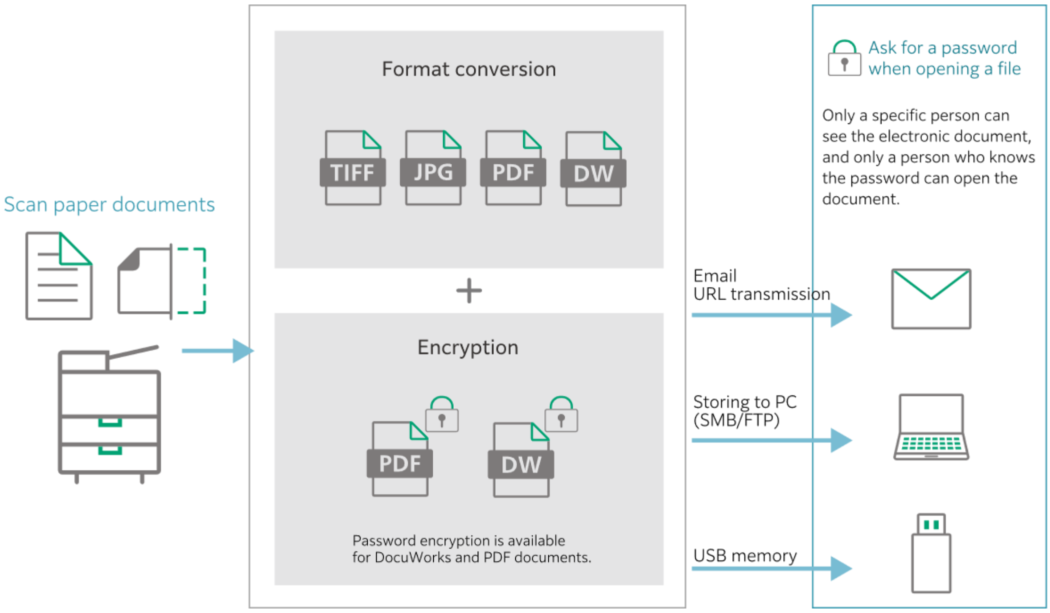
It supports automatic certificate delivery feature offered by Network Device Enrollment Service (NDES) of Windows Server. Certificate update (including the newly issued one), which has been manually performed by an administrator, and associated setting update processing can be automated by using SCEP (Simple Certificate Enrollment Protocol).

For details on certified products, please contact your regional sales.

https://www.fujifilm.com/fbglobal/eng

Encrypting Scanned Document with a Password

With this feature, when storing a scanned document to PC or sending it by email, you cannot only convert the document to a DocuWorks document or PDF file but also specify "file encryption" with a password. The security functions of applications such as printing and editing restrictions are also supported, let alone password setting for opening files. It reduces the risk of data breach and tampering of scanned documents.


Scan paper documents
Format conversion
TIFF
JPG
PDF
DW
+
Encryption
PDF
DW
Password encryption is available for DocuWorks and PDF documents.
Email
URL transmission
Storing to PC (SMB/FTP)
USB memory
Ask for a password when opening a file
Only a specific person can see the electronic document, and only a person who knows the password can open the document.

Note: DocuWorks Viewer Light or Acrobat Reader / Adobe Reader is required to open encrypted DocuWorks or PDF files.

However, as the document may not open in older versions, please use the latest DocuWorks Viewer Light and Acrobat Reader.

Digital Signing and Public Key-based Encryption for Scanned Documents

Digital signature is available when sending a scanned document in DocuWorks, PDF or XML Paper Specification (XPS) files by importing a certificate and private key into an MFD, allowing the detection of data tampering by third parties. Besides, as PKI encryption is available with DocuWorks documents, higher security than password encryption can be provided, and it is possible to create documents that only certain users can access.

* This feature is supported only on ApeosPort and Apeos models.

Direct print of encrypted documents

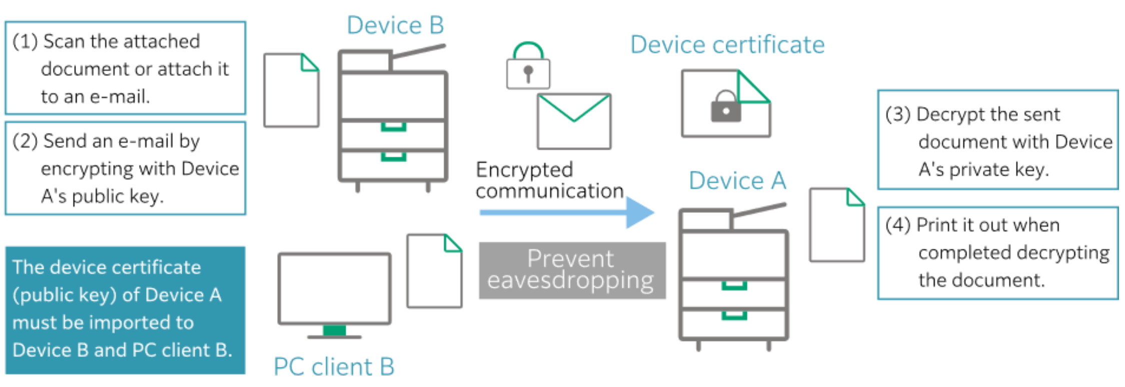
Using a password previously registered in the MFD, the encrypted DocuWorks files and PDF files stored in USB memory, Working Folder, etc. can be decrypted and directly printed. Furthermore, it also supports sending DocuWorks files or PDF files simultaneously with the password by using the Contents Bridge utility.

E-mail encryption and e-mail signature

E-mail encryption (S/MIME): Encrypt e-mail (including attached documents) by the user's digital certificate so that only the user can open it. It reduces the risk of data breach by eavesdropping during e-mail delivery.

E-mail signature (S/MIME): Sends an e-mail (including attached documents) by attaching the user's signature with a digital certificate of an MFD. It reduces the risk of tampering during e-mail delivery, and objectively prove the sender, allowing recipients to use it with peace of mind.

Automatically print the encrypted e-mail received



(1) Scan the attached document or attach it to an e-mail.

(2) Send an e-mail by encrypting with Device A's public key.

The device certificate (public key) of Device A must be imported to Device B and PC client B.

(3) Decrypt the sent document with Device A's private key.

(4) Print it out when completed decrypting the document.

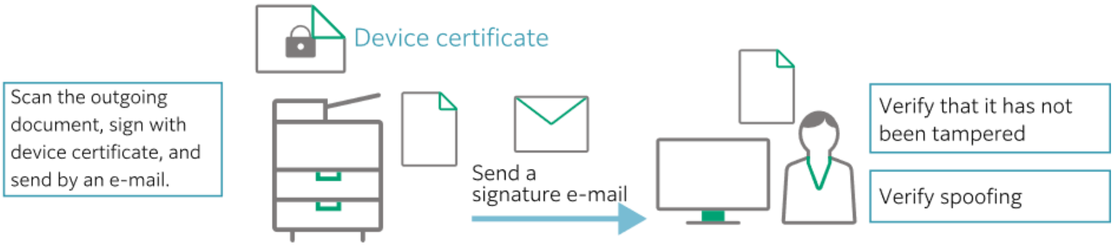
Preventing Attacks, Eavesdropping, and Data Breaches via Fax Line

Regarding access via fax line (telephone network), only fax protocol communication can be accepted. Therefore, malware in fax data will not affect MFD behavior and unauthorized command will not be executed.

All data received is handled as fax image format data. In case there is malformed data that does not follow the fax protocol standard, it will be processed as image data error such as decoding error.

Images and original documents stored in MFD Folder can be retrieved by polling communication from remote sites. However, no unauthorized data acquisition (breach) will occur by implementing strict password management to MFD Folder.

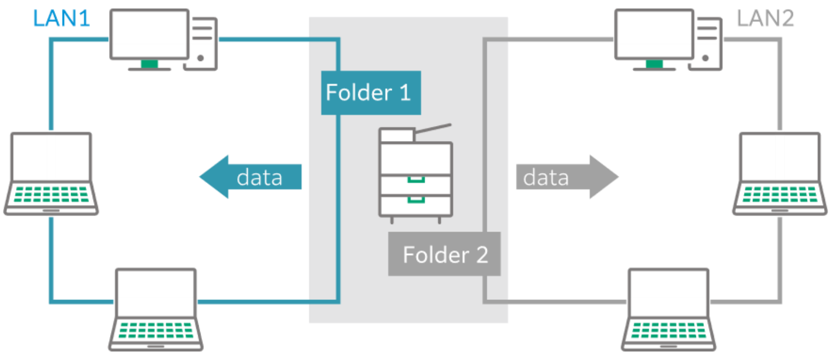
Scan a paper document, sign an e-mail, and send.


Device certificate
Scan the outgoing document, sign with device certificate, and send by an e-mail.
Send a signature e-mail
Verify that it has not been tampered
Verify spoofing

Preventing Attacks, Eavesdropping, and Data Breaches via Secondary Ethernet

Secondary Ethernet (optional) and Primary Ethernet (standard) establish communications independently (TCP/IP). The MFD will not router communications (TCP/IP) between network interfaces and the specification to access one network from another via the MFD as this function has been disabled.

Network access restriction can be imposed on an MFD folder. Display / document storage / document transfer to the MFD Folder from the network can be limited to either Primary Ethernet or Secondary Ethernet for each MFD Folder. Consequently, information leakage of documents within the MFD Folder due to unauthorized access from other networks is averted. Furthermore, managing the password of MFD Folder is required.



Secondary Ethernet allows use of below Scanner functions:

- Document retrieval by Internet Services using Scan to Folder
- Job flow (SMB transfer) starts from the MFD Folder
- AirPrint scan

Functions that involve the MFD Folder are protected by network access restrictions. For AirPrint scan, transmissions to the Secondary Ethernet side only occur when a scan instruction is received from the Secondary Ethernet. Therefore, unauthorized use of the Secondary Ethernet causing information leakage is averted.

Preventing Attacks, Eavesdropping, and Data Breaches via Wireless LAN (Wi-Fi) Port

The optional wireless LAN converter is a wireless terminal connected with a wired LAN cable. The wireless LAN kit ,the wireless kit and the wireless kit2 are wireless terminals that perform wireless LAN communication when connected to the MFD.

These wireless terminals support countermeasures to WPA/WPA2's vulnerability known as KRACKs. The Wireless LAN Kit 2 allows users to securely use the device , as it supports WPA3-SAE, which was formulated by Wi-Fi Alliance in June 2018.

Furthermore, as these wireless terminals do not have a routing function, they do not perform communication between each network interface (TCP/IP).

Accessing an MFD Folder and unauthorized access countermeasures are the same as those for Secondary Ethernet. Consequently, information leakage due to unauthorized use of these wireless terminals is averted.

Preventing Attacks, Eavesdropping, and Data Breaches via USB Port

With print jobs imported via USB port, data is handled as printer job language (PJL) and image data. If data other than PJL and image data is received, the job will be suspended due to a job error.
In addition, the relay function establishing a connection to communication lines including network and fax line from USB port is not implemented.

Preventing Attacks, Eavesdropping, and Data Breaches via Virus-infected Files on USB Memory

For the following reasons, MFDs and PCs on the network connected to MFDs are virus-free at execution of scan jobs and print jobs with USB memory.

1. With scan jobs, no access will be attempted to the files on USB memory.
   Due to this, MFD will not be infected by virus even if the files on the memory are infected.
2. With print jobs, the files on USB memory are handled as image data.
   Assuming the files have been infected, that print job will be suspended due to an image processing error as the format does not match that of image data. Malicious programs will not automatically run.
3. Since MFDs will not be infected by virus as described above, PCs on the network will not be infected by virus via MFDs.
4. Communication method directly connecting to PCs on the network from USB memory is not implemented.

Table 3. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
3. Unauthorized access to administration functions Unauthorized operations may be performed if identity authentication to distinguish authorized users cannot work on the rules (security policies) set for document data to be handled and functions that manage user information on the device.	**C) Protection of administration functions** ● **System administrator's password** When operating with the default value, a warning message prompts you to change the password. ● **Account Lock** To be performed in case of consecutive administrator login failures. ● **Customer Engineer Operation Restriction Function** Prevent attacks such as setting changes of MFDs. ● **Centralized user profile management** ApeosWare Management Suite 2 can realize configuring access control based on organizations or locations of the devices. ● **Centralized control of user permissions by organization or installation location** ApeosWare Management Suite 2 can realize configuring usage restrictions based on organizations or locations of the devices.

C)Protection of Administration Functions

Security Warning Message for Default System Administrator ID & Password

To use the device with higher security, a warning message appears to prompt the administrator to change the password when he/she log in as the system administrator mode with default setting of system administrator ID and password.

Account Lock in case of Consecutive Administrator Login Failures

The function to handle the authentication failures is provided for the system administrator authentication which is performed before accessing the system administrator mode.　In case the system administrator fails to login for the predetermined number of times, login attempts can be blocked until the device is restarted.

Customer Engineer Operation Restriction

Operations performed by a customer engineer having special permissions can be restricted with settings configured by the system administrator.　A password can be set to enter the customer engineer mode to prevent unauthorized access to the device by a person impersonating a customer engineer.

Centralized Permission Control for Organization or Physical Location

ApeosWare Management Suite 2 can centralize user profiles for permission control and apply them based on organizations by user group or physical location by device group. The user profile can also control access permission by security levels or services available on ApeosWare Management Suite 2. Furthermore, it can be used on mobile devices that install ApeosWare Management Suite 2 Mobile application, as well as devices.

Feature and color restriction of devices

Part-time employee A	Employee B	Manager C	HR group
Only black & white Only copying	Color available Copy / print available	Color available No restrictions	Color available No restrictions (Requires password entry)

Table 4. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
4. Software tampering If tampering of software occurs, security policies defined may not be executed properly. With no mechanism to verify that the update program of the product is legitimate, unauthorized software or system files may be uploaded and it leads to disabling the encryption function or installing unauthorized applications.	**D) MFD Software Integrity** ● **Vulnerability detection and software update** Regularly performed ● **Ensures the integrity when updating software** Prevents unauthorized controller software and add-on applications from being installed on MFDs. ● **Ensures the integrity at startup** Prevents unauthorized controller software from being executed at startup. ● ● **Ensures the integrity during operation** Prevents unauthorized operation by monitoring the operation of the controller based on the White List.

D)MFD Software Integrity

Periodical Vulnerability Scan and Updates

Actions against attacks on a device are taken on a regular basis with vulnerability scanners and necessary measures are released as controller software updates. At FUJIFILM Business Innovation, vulnerability verification is performed with multiple vulnerability scanners during new product development. If a vulnerability is detected, measures such as security patch application are implemented. Regarding vulnerability scanners, as vulnerability information and database are updated daily, verification can be always performed with the latest status. Verification and support are implemented also on existing products on a regular basis and software upgrade is performed as required. In addition, functions like SSH with which remote operation is possible are not installed to prevent unauthorized operations from the outside.

Ensures the integrity when updating software

When updating the controller software or add-on application, the digital signature verification function prevents the software from being rewritten to the unauthorized one created by a malicious third party. If tampering is detected, the event is recorded in the audit log without starting up the MFD.

As a security level enhancement, you can disable the software updating function from the network to prevent unauthorized software updates over the network.

Furthermore, you cannot update the software from the fax line.

Ensures the integrity at startup (tampering detection function at startup by secure boot function)

When booting the MFD, it verifies the electronic signature of the controller software, and if a falsification is detected, it recovers automatically from golden master (resilience).
Achieves more robust security (HW Root of Trust) by using immutable hardware at the reliable starting point.

Ensures the integrity during operation (tampering prevention function during operation using White List)

Protects normal applications and prevents unauthorized operation by monitoring the operation of the controller based on the White List to prevent suspicious applications from being executed.

Also, unexpected access can be blocked by controlling the network communication destination using the IP address restriction function.

Table 5. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
5. Audit log tampering If the audit log obtained for tracing unauthorized activities is not protected, the log may be tampered or deleted.	**E) Audit log, protection of the log, and other log related functions** ● **Audit Log** You can trace the history by using the function to record stop / start of the MFD, configuration changes, and job progress status. ● **Audit Log Protection** **You can disable viewing, editing, and deletion of audit logs by unauthorized persons.** ● SIEM linkage of audit logs Collective management and analysis of audit logs become possible by linking MFD's audit logs with SIEM products using the Syslog protocol. ● **Restrictions on job information display** You can also set to hide job log record that indicates job execution result from other users. ● **You can print document-specific identifier "UUID"** You can trace a specific user in the event of data breach. ● **Traceability for Job Transactions** You can centralize traceability for job transactions with ApeosWare Management Suite 2 and ApeosWiz Image Log.

E) Audit Log, Protection of the Log, and Other Log-related Functions

Audit Log

You can download "audit log" from Internet Services via web browser. This log shows you detailed history including system data changes, user login/logout, power on/off and job progress status to help you enhance system management and trace the history of unintended changes. It is also useful to raise users' awareness about security.

Operations related to the following items are recorded on the audit log:

- Status Change: Power on/off of the device, start/end of user operation, etc.
- Login Status: User login, logout, authentication lock of the system administrator, etc.
- Job Status: Job completion, etc.
- Setting Change: Time setting, Security setting change, user information setting, opening Folder, etc.
- Data Change: Certificate change, Address Book change, etc.
- Configuration Change: Storage replacement, ROM version change, etc.
- Communication Result: Communication error, etc.

Audit Log Protection

Audit Log should not be viewed/edited/removed by third parties because of its objective. The following measures are applied for its protection.

- There is no interface to edit/delete the audit log.
- Only administrators can access it. And encrypted communication with SSL/TLS is required to download it.
- Also the audit log information can be protected with the Storage encryption feature even when it is replaced/removed from MFD.

SIEM linkage of audit logs

Early detection and analysis of security threats are supported, as it becomes possible to collectively manage and analyze MFD's audit logs by using the function to transfer MFD's audit logs to the outside using the Syslog*1 protocol and linking with SIEM*2 products.

*1: Syslog is a standard protocol that transmits chronological records (logs) through an IP network.

*2: SIEM (Security Information and Event Management) is security software / services that collectively stores and manages records (logs) of the operating status of devices and software, and quickly detects and analyzes events that pose security threats.

Restriction on Job Information Display

This feature allows you to configure settings for restricting information to be displayed such as making it impossible for unauthenticated users to view information on jobs in execution, awaiting, or completed states.

Display restriction can be also set for authenticated users so that they can view only their own jobs and cannot view those of other users. You can enjoy privacy protection and data breach prevention.

Printing Job Log Identifier UUID

This feature allows you to print a document-specific identifier called "Universal Unique Identifier (UUID)" on copy, print or fax documents. You can use it when searching for or identify a certain document. As it shows "when" "by whom", and "how" documents were handled for check, it helps you identify a certain user in the event of data breach.

Traceability for Job Transactions

ApeosWare Management Suite 2 collects job log information for transactions and allows the system administrators to trace job history from reports generated.

It is also possible to trace jobs' image data with another server base software, ApeosWiz Image Log using the Image Log feature that stores image data of documents processed on the device with user information or UUID feature. ApeosWiz Image Log also monitors the image data and automatically alerts the system administrator to prevent data breach when it hits certain security criteria configured.

Table 6. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
6. Breach of document data stored on the device (at return after lease end or device disposal) Document data used for print, copy, or fax are temporarily or permanently stored to the storage . That data may be compromised from the device when it is returned after lease end or it is disposed. This document data may be restored if it has not been physically deleted, even if it seems that access to the data cannot be made on the surface.	**F) Protection of document data stored on the device** ● **Encrypting data stored on Storage** Prevent third parties from analyzing the storage removed from an MFD. ● **Batch deletion of data in MFD Storage** Batch deletion of the setting information and document information can be performed before reusing an MFD at another organization or disposing it, so that prevent the leakage of information in the MFD.

F) Protection of Document Data Stored on the Device

Encrypting Data Stored on Storage[*1]

When data is written to the storage, it is encrypted with a very robust method[*2] to prevent unauthorized access to stored data.　In addition, it prevents the data from being analyzed by a third party when carrying out the MFD.

This cryptographic key itself is not stored in non-volatile memory but generated for use every time the MFD is booted. For this reason, this key will not be compromised even if non-volatile memory is removed from the storage.

In addition, in some models, the encryption key used to encrypt the data stored in the storage is further encrypted with the root encryption key inside the security chip (TPM: Trusted Platform Module) independent of the storage. The root encryption key is securely protected without being read from the outside due to the tamper resistance of TPM.

*1 HDD and SSD

*2 AES-256

For more details about the strength of encryption for each MFD model, refer to Security Target that is available from the following website.

For details on certified products, please contact your regional sales.

https://www.fujifilm.com/fbglobal/eng

Batch deletion of data in MFD Storage*1

The administrator can delete all information registered and set in the MFD when disposing of or moving it to another department. It prevents the leakage of data in the MFD at the time of disposal.

For HDD-equipped machines, data accumulated in the HDD storage is overwritten (batch deletion) when the optional Data Security Kit or Secure Deletion Kit has been installed. You can only initialize (format) the machines in which the option has not been installed.

For SSD-equipped machines, data is erased by formatting (Secure Erase). When the data accumulated in the SSD storage is encrypted, the encryption key is also deleted by performing batch deletion. By deleting the encryption key, you cannot decode (read) the encrypted data accumulated in the SSD storage, so it has the same effect as when the data itself is deleted (Cryptographic Erase).

*1 HDD (Secure Deletion), SSD (Secure Erase)

Table 7. Security Threats and Measures for Office Multifunction Devices

Security threats to office devices	Security measures implemented by FUJIFILM Business Innovation
7. Data breach caused by careless mistakes of system administrators or users Even if system administrators or users think that they configured settings or performed operations with no mistakes, wrong operations lead to unexpected data breach.	**G) Preventing configuration / operation mistakes and improving the awareness of document handling** ● **A security warning message for global IP address** Encourage the administrator to change the IP address or use the user authentication mode. ● **Scanned documents to be delivered to / stored in fixed destination** You can prevent users from sending data to wrong destination / data breach by limiting the communication destination (including fax) to a specific destination. ● **Suppressing erroneous fax transmission** Suppress mistakes by reentering destinations, manual redialing, etc. ● **Block Fax Reception** Prevent annoying direct mails. ● **Print Lockout Duration** You can prevent printouts left unattended. ● **Suppress data breach from printed documents** Provide Annotation, Copy Management Output (Analog Watermark), and Secure Watermark features.

G)Preventing Configuration/Operation Mistakes and Improving the Awareness of Document Handling

Security Warning Message for Global IP Address

In case a global IP address is assigned to the MFD and [No Login Required] is set as the [Login Type], a warning message appears when a system administrator logs in.　This function encourages system administrators to change the IP address or to apply user authentication modes.

Scan to Fixed Destination

This feature allows to automatically fix the destination address or sender to the authenticated user's own email address. You can use it to prevent wrong email transmission and external email transmission in an effective way.

The document storage location can be fixed to a folder on your PC and moreover, once you store a scanned document on the device, you can send an email with the URL of the storage location attached to the authenticated user. It will be a great help also for reducing loads on network or mail server as well as for secure mail delivery to the authenticated user itself.

* Operation in Authentication mode is required.

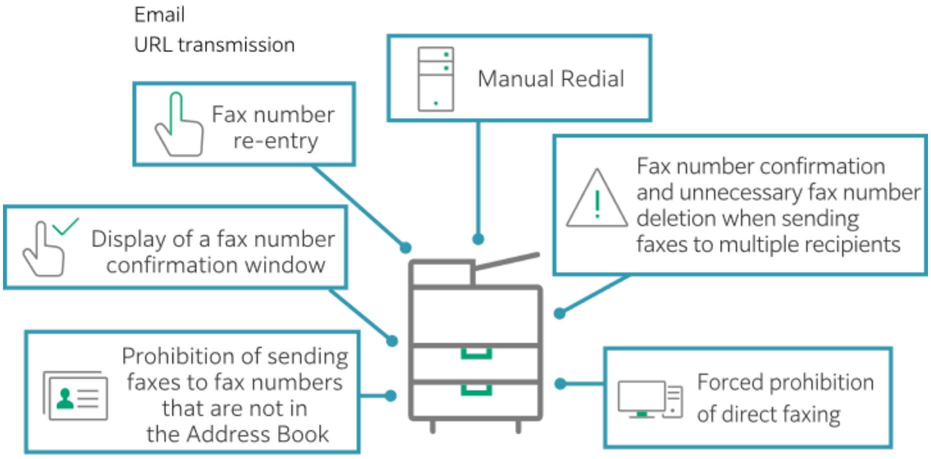
Preventing End Users from Sending Faxes Wrongly

Sending a fax to a wrong destination - anyone could make this mistake. However, it could lead to catastrophic consequences. Some functions including the following have been enhanced to prevent wrong fax transmission. These functions are compliant with "FASEC 1*", which is the guideline for security functions of fax for business use.

- Re-entry of FAX Destinations: Enter the destination twice for verification

- Manual Redial: Send a fax by selecting a destination from the list of transmission history

- Fax number re-entry
  Avoids input error by entering the destination number twice.
- Prohibition of sending faxes to fax numbers that are not in the Address Book
  Restricts users from sending faxes to numbers not listed in their address book.
- Forced prohibition of direct faxing
  Prohibits fax transmission from PC.
- Display of a fax number confirmation window
  Displays the confirmation screen before sending fax and allows you to delete the destination if it is wrong.
- Fax number confirmation and unnecessary fax number deletion when sending faxes to multiple recipients
  Allows you to delete or correct destinations for broadcast fax.
- Manual redial
  Records the destination once a fax is sent to a destination. Ensures correct fax transmission with a text fax transmission in advance.


Email
URL transmission
Fax number re-entry
Manual Redial
Display of a fax number confirmation window
Fax number confirmation and unnecessary fax number deletion when sending faxes to multiple recipients
Prohibition of sending faxes to fax numbers that are not in the Address Book
Forced prohibition of direct faxing

* Established by Communications and Information Network Association of Japan (CIAJ) to promote the enhancement of security functions for facsimile communications via telephone lines.

Furthermore, the following functions are also applicable against wrong fax transmission.

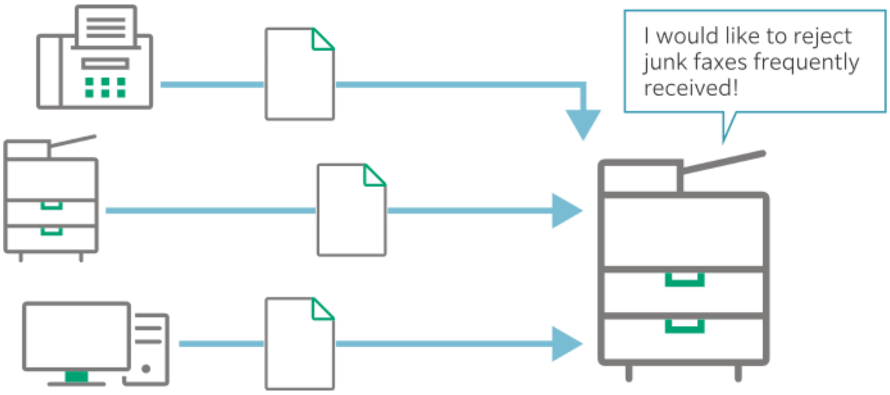
- Wrong fax transmission can be avoided by prohibiting broadcast fax.
- The relay broadcast and transfer functions can be prohibited for fax transmission.

Block Fax Reception

Annoying fax prevention function

Prevent receiving junk faxes by an incoming call rejection function.
You can reject senders from whom you do not want to receive faxes or faxes sent from unknown fax numbers. Eliminate useless print by junk faxes unspecifically sent.

- Block Fax Number: Register G3 ID (phone number) that rejects fax reception. You can register up to 50 fax numbers.
  - Block Unknown Fax Numbers: You can block faxes whose G3 IDs (phone numbers) are unknown.

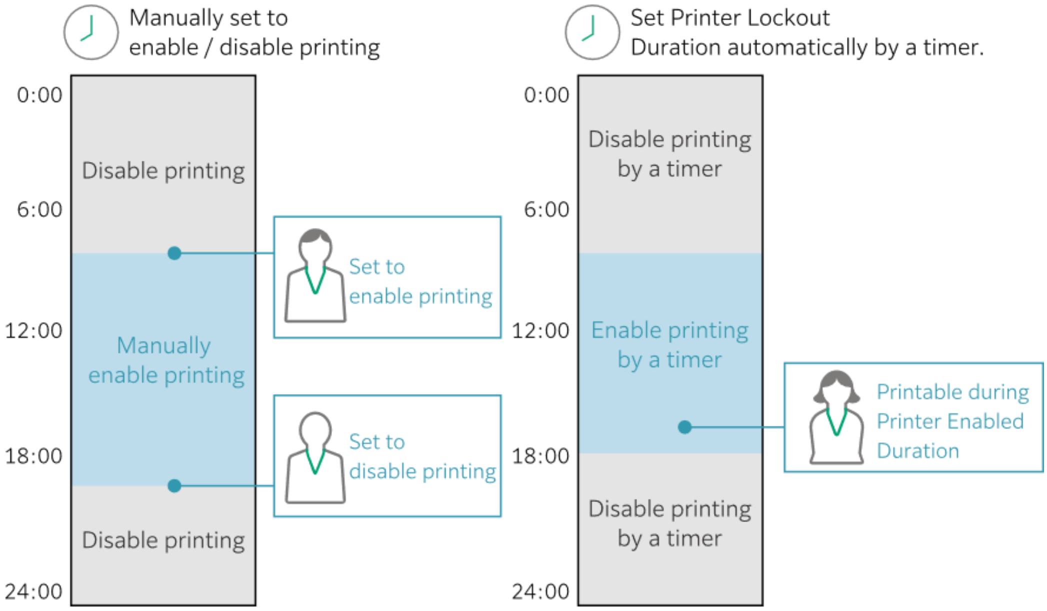


Block faxes received from senders other than those registered in the Address Book

You can block faxes received from senders other than those registered in the MFD's Address Book with settings configured by a customer engineer.

Print Prohibited Time Period

This feature allows you to specify a time zone when printing is disabled and it prevents uncollected printed and faxed documents when no one is at the office.



Even while printing is disabled by Timers, user can change it to be enabled.

Annotations

You can add a stamp such as "DO NOT COPY" to your document when copying it to inform others of the significance of the document.

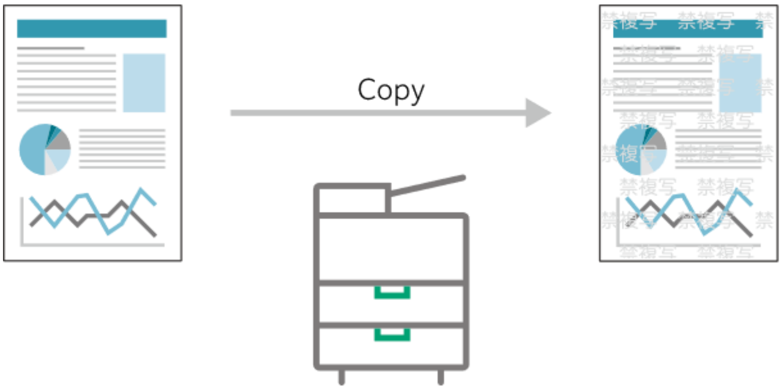
DO NOT COPY
URGENT
DRAFT
CONFIDENTIAL
URGENT
2011/07/21
1/3
2/3
3/3

Force Annotation

With this feature, it is possible to forcibly print user ID, output year/month/date. etc. on copied, printed, or received fax documents. It allows you to identify "when", "who", output the document in an easy way and set four layout template patterns by associating them by print job. It facilitates adequate paper document handling in an easy and hassle-free manner as you can enjoy this feature on the device without any optional functions.

Copy Management（Analog Watermark）

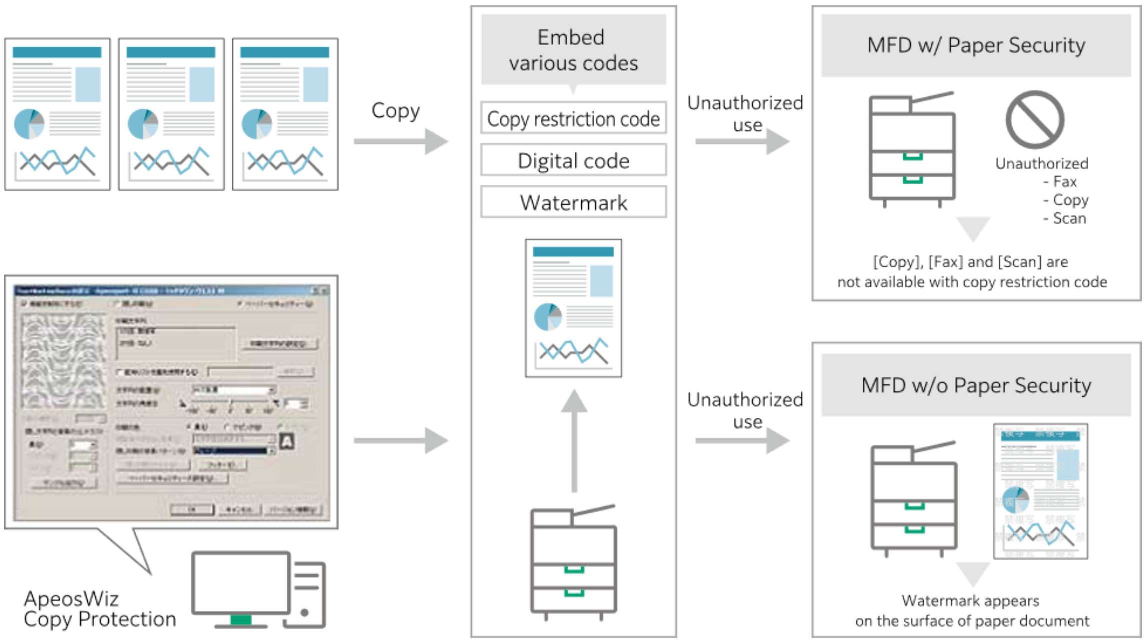
You can output a document by printing a control number or watermark on its background. When copying the document, they appear on the surface and it helps to prevent data breach by unauthorized copying.　This encourages users to deal with the printed documents more carefully.



* Optional. Copy Management Expansion Kit is required.

Secure Watermark

You can specify whether to include digital codes such as copy restriction code or job information whenever you copy or print documents. It can prevent copying itself and realize output history analysis. Further, it allows force embedding of digital codes by the system administrator.　It enables administrators to track information in case a breach happens.



* Optional. Secure Watermark Kit is required.

* Regarding document copy restriction, digital code analysis feature, and suppression effects of watermarks, their features are not always guaranteed. Features may not work as expected depending on the original document or settings.

* PC software ApeosPort Copy Protection is required to optionally embed digital codes at printing.

・This document includes Fuji Xerox product(s), licensed from Xerox Corporation. The distributor of the product(s) is FUJIFILM Business Innovation Corp.

・The contents, product specifications, and overview may change without prior notice due to product improvements.