Konica Minolta
Security Technical Support Paper

Report on Basic Security Guidelines and Technical Support

Ver. 10.7

May 2025

History

Version	Date	Description
1	Aug, 2004	First version
1.1	Sep, 2004	Added supported models
2.0	Feb, 2005	Added supported models
2.1	Feb, 2005	Modified version 2.0
2.2	Mar, 2005	Modified version 2.1
3.0	Sep, 2005	Revised supported features and added supported models
4.0	Jan, 2007	Revised supported features and added supported models
4.1	Aug, 2008	Added only supported models
4.2	Mar, 2009	Added descriptions, added supported models
4.3	Nov, 2009	Added descriptions, added supported models
4.4	Apr 27th, 2010	Added descriptions, added supported models
4.5	Feb 16th, 2011	Added descriptions, added supported models
5.5	Jan 16th, 2012	Added descriptions, added supported models
5.6	Mar 15th, 2012	Added descriptions, added supported models
5.6.1	Apr 12th, 2012	Added descriptions, added supported models
5.7	Sep 12th, 2012	Added descriptions, added supported models
6.0	Nov 30th, 2012	Added descriptions, added supported models
7.0	Feb 26th, 2013	Added descriptions, added supported models
7.0.1	Jul 30th, 2013	Added supported models
7.1	Oct 18th, 2013	Added descriptions
8.0.1	Jun 10th, 2014	Added descriptions, added supported models
8.0.3	Jul 14th, 2014	Added TPM descriptions
8.0.4	Aug 26th, 2014	Added supported models (C3110, C3100P, 4700P, 4000P, 3300P)
8.0.6	Apr 13th, 2015	Added CSRA descriptions, added supported models (bizhub PRESS C71hc)
8.0.7	Aug 19th, 2015	Added supported models (C368, C308, 367, 287, 227)
8.0.8	Jul 27th, 2016	Added descriptions (security for GW integrated into MFP)
9.0	Nov, 2016	Revised document title
9.1	Jun 28th, 2017	Added descriptions (security for Mobile Print, Remote Deployment Tools)
9.2	Sep 5th, 2017	Added descriptions (security for World Wide Remote Service Platform), Modified version 9.1
9.3	Dec 14th, 2017	Added supported models (C759, C659, 658e, 558e, 458e, 368e, 308e, C3080, C308P, C3070, C3070P, C3070L)
9.4	Dec, 2018	Added descriptions (security for data in main MFP unit: when using SSD; security for CS Remote Care: when using an LTE device) Added supported models (C360i, C300i, C250i, C4050i, C3350i, C3320i, C4000i, 3300i, 4752, 4052)
9.5	Jul, 2019	Removed descriptions (feature extensions through linking with PageACSES), added descriptions (security concerning CWH; protection of user information), added details concerning RDT as an attachment.
9.6	Oct, 2019	Added descriptions (C650i, C550i, C450i, 306i, 266i, 246i, 226i, Accurio Press 6136, 6120, 6136P)
9.7	Sep, 2020	Added and revised descriptions (Complete data deletion when discarding HDD and SSD, Feature for overwriting and deleting HDD data, Printing of reports after deleting all data)
9.8	Jun 4th, 2021	Added descriptions (Fleet RMM)
9.9	Apr 20th, 2022	Added supported models (4700i, AccurioPress 6272P, C7100, C7090, C4080, 4070, AccurioPrint 2100, C4065)
10.0	Sep 2nd, 2022	Postscript (Protecting SDD by self-encryption: “always”) Added RSA (Remote Service Agent) to World Wide Remote Service Platform chapter
10.1	Dec 2nd, 2022	Added supported models (bizhub C450iS, C360iS, C300iS, C250iS) Update of Fleet RMM
10.2	Jun 12, 2023	Added descriptions (security for MarketPlace). Deleted the descriptions for older models. Deleted “Alternative Text” descriptions in original MS-Word file.

Version	Date	Description
10.3	Oct 31, 2023	Updated due to Fleet RMM v1.3 release; - Deleted Configuration data (SMB) from Transmitted Data including personal information. - Updated communication protocol type and port number used by Fleet RMM. - Corrected errors in existing descriptions.
10.4	Feb 29, 2024	Added the following descriptions: - Temporary data is protected by MFP's encrypt function, not by SSD's self-encryption - Operational options after a virus is detected - Secure Erase function - Notification when unauthorized access is detected - Detection of signs of unauthorized or unwanted activities Added supported models (bizhub C751i, C651i, C551i, C451i, C361i, C301i, C251i, C4051i, C3351i, C3321i, C4001i, C3301i, 950i, 850i, 751i, 651i, 551i, 451i, 361i, 301i, 4751i, 4051i, 4701i) Added supported models (AccurioPress 7136, 7120, 7136P) Deleted the descriptions for older models.
10.5	May 24,2024	Updated due to Fleet RMM v1.4 release; - Updated communication protocol type and port number used by Fleet RMM. Removed descriptions for RDT (Security concerning Remote Deployment Tools) * RDT had already been discontinued.
10.6	Oct 30,2024	Updated due to Fleet RMM v1.5 release. - Updated the port number of communication protocols used by Fleet RMM. - Added SMB to Data Transmission.
10.7	May 16,2025	Updated the following descriptions: - Version of FIPS from "FIPS140-2" to "FIPS140-3". - Added Elliptic Curve Cryptography (ECC) for protecting information from leakage when using TPM. Updated due to Fleet RMM v1.6 release. - Added new MFP models to communicate to FleetRMM Edge in "Intended Use" column of Table 18-3. - Added the port number of communication protocol for SAML authentication in Table 18-3. Added supported models (bizhub C4751i) Added supported models (AccurioPress C14010/C12010, AccurioPress C5080/5070, AccurioPrint C5065) Deleted the descriptions for older models.

Konica Minolta products have various technologies concerned with security, but they only help if customers operate the products properly in accordance with Konica Minolta's security policy. We ask for understanding in consulting the content of this paper while operating Konica Minolta products. Please see the user manual for each setting. Moreover, please note that the content of this paper does not guarantee perfect security.

Terminology:
MFP: Multi-Functional Printer
GW: Gateway
DB: Database

Trademark:

Index

Attachment:

Fleet RMM edition

Chapter1: Introduction

In our modern societies with network infrastructure in place and widespread IT, vast amounts of information are distributed. And information accumulates at the center of businesses in a variety of forms changing form while utilized as advanced information assets. An important issue for corporate activities is protecting these information assets, in other words managing risk.

This paper introduces the basic security features provided by each series of Konica Minolta.

I. Basic Security Guidelines

1. Adding the newest security technology

Konica Minolta develops and provides the newest security features in order to protect customer information assets from the various threats classified in the following section.

i. Unauthorized access and information leaks via networks
ii. Unauthorized use and information leaks from the direct operation of devices
iii. Tampering, copying, and deleting electronic information and analog information
iv. Information loss from man-made accidents and equipment failure
v. Trace feature through logs

2. Obtaining certification from a third-party institution

In order to objectively demonstrate the implementation of security features, Konica Minolta acquired ISO15408 certification in MFPs (most A4/20ppm models or above) starting in March 2004.
ISO15408 certification was acquired based on each MFP's initial engine firmware. When MFP's engine firmware is released, such as for a maintenance release, the continued warranty system is no longer used, but support is maintained for security features without change.
The integrated MES (RSA BSAFE Micro Edition Suite) encryption module is authenticated with acquired FIPS140-3. The software is thus certified as robust and safe, and sales to institutions that require FIPS140-3 authentication is allowed.

To check the acquisition status of ISO15408 certification, refer to the lists of the certified products shown on the following webpages of the Information-technology Promotion Agency (IPA). The lists always show the latest information, and it is also possible to download the certified product lists.

List of certified products:
https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html (Japanese)
https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/certfy_list_e31.html (English)

List of products under evaluation:
https://www.ipa.go.jp/security/jisec/certified_products/in_eval_list.html (Japanese)
https://www.ipa.go.jp/security/jisec/jisec_e/prdct_in_eval.html (English)

Chapter2: Security and technology support for equipment

I. Security for public phone lines

1. Security for fax lines

The fax line is communication that only uses fax protocol, and other communication protocols are not supported. If invaded externally with a different protocol through a public line, or if fax data which cannot be expanded is sent, the internal software process will produce an error, and the communication will be blocked.

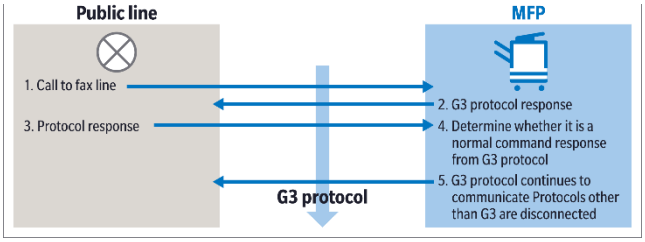


Figure 1-1

2. Enter the address twice

When entering the fax transmission address as a telephone number, enter the telephone number again, and verify that they match, thus avoiding a mistaken transmission due to entering the wrong telephone number.
Also, if registering a telephone number to speed-dial, enter the telephone number again, and verify that they match, thus avoiding a mistaken transmission due to entering the wrong telephone number.

3. Chain dial

When entering the address, speed-dial numbers and direct entry with the numeric keypad can be combined. By registering the area code as a speed-dial number beforehand, input mistakes can be prevented.

4. Address confirmation screen displayed

When entering a send address (speed-dial number, phone number, etc.), first, display the entered address on the operation panel to verify to avoid sending to the wrong address.

5. Multiple addresses prohibited

Configure to permit to enter only one address to avoid sending to an unintended address.

6. Transmission to verify destination device

When sending a fax, verify the destination machine's telephone number through the fax protocol signal (CSI) received from destination machine if they match or not for a more secure transmission.

II. Security for LAN connection

1. Handling network protocol

Each port can be set actions as ON/OFF. Prevent outside intrusions by switching OFF unneeded ports.

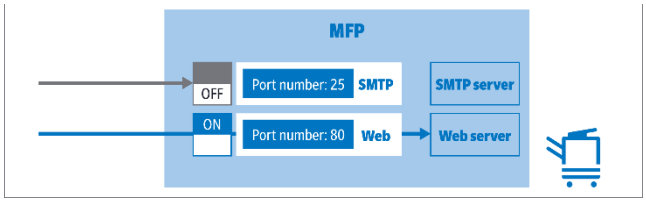


Figure 2-1

With the IP address filtering feature, IP addresses can be specified to permit access and reject access, thus allowing for sorting devices on the network to which access was permitted.

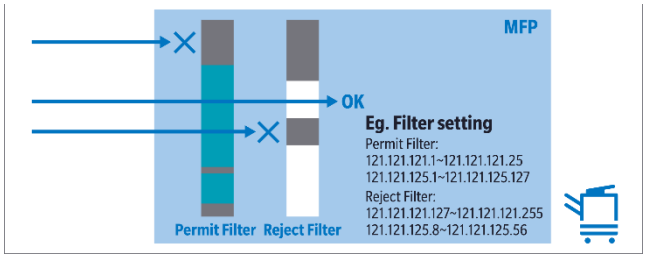


Figure 2-2

2. User authentication

It is possible to authenticate users for features that use the network by using the network authentication which uses the Active Directory service. In addition, not just functions that use the network, but even when using the MFP, if Active Directory authentication is configured in user authentication settings, authentication will be performed with Active Directory.

Usage permission is granted by combining a registered user and password.

Internal data is protected since only registered users can use the device.

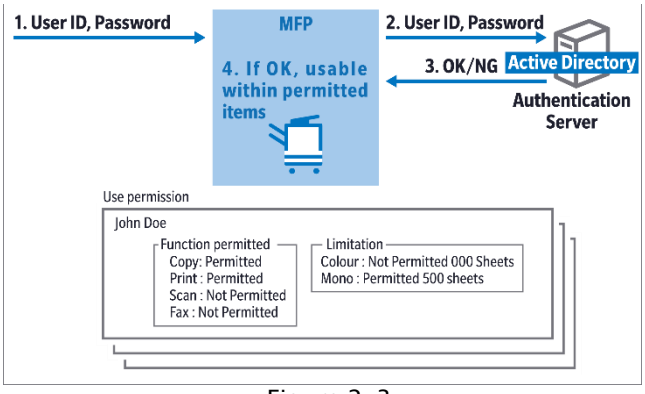


Figure 2-3

3. Device management security through the network

(1) Security when registering whole address book

The administrator password of the device must be entered when registering whole address book from the network. It cannot be registered if the administrator password of the device is not valid.
This feature prevents having the address book registered to the MFP being tampered with all at once.

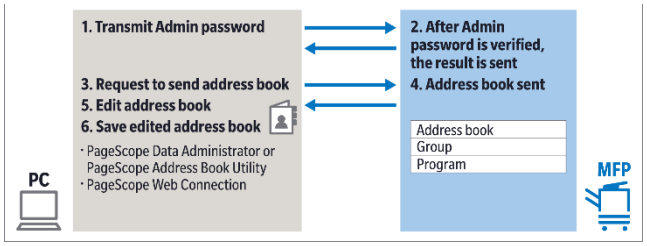


Figure 2-4

(2) bizhub OpenAPI

bizhub OpenAPI allows for using SSL/TLS encryption protocol to acquire and configure device information over the network. And communication can be made more secure by setting a password unique to bizhub OpenAPI.
The device is secured by using bizhub OpenAPI for the settings of user authentication information through the PageScope Data Administrator.

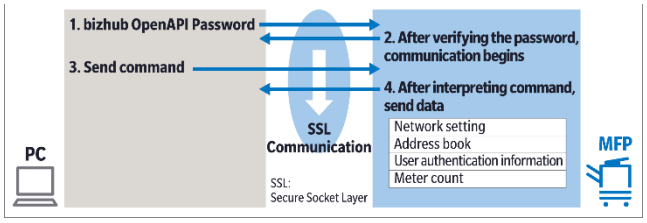


Figure 2-5

4. Encryption of data communication

SSL/TLS encryption protocol is used for data communication between the LDAP server, PageScope Data Administrator (or Address Book Utility), PageScope Web Connection, and the MFP. The content is protected by encrypting data traded between networks. Moreover, IPsec is used, which allows encryption support not dependent on a communication protocol. Communication is encrypted in line with support for IPv6 conversion.

5. Quarantine network support

When connecting to LAN, IEEE802.1X feature is used for authenticating network devices and allows managing MFP connections to LAN for physical ports.
Authentication is performed on the RADIUS (Remote Access Dial in User System) server, and LAN connection control is performed with a supported switching hub.
With this feature, only MFPs for which authentication was permitted are permitted to connect to a LAN environment.

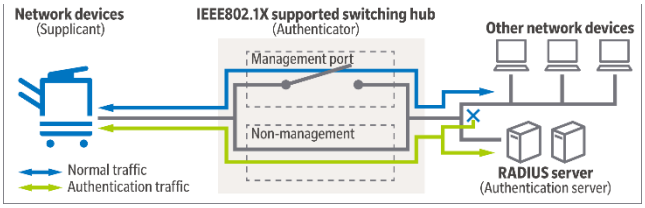


Figure 2-6

6. Bi-directionally certificate verification

Conventional MFPs inform the other communicating device with its certificates to verify the validity of MFPs. And by verifying the validity of the other communicating device bi-directionally, communication control is performed, preventing "impersonation" of an MFP or the other communicating device.

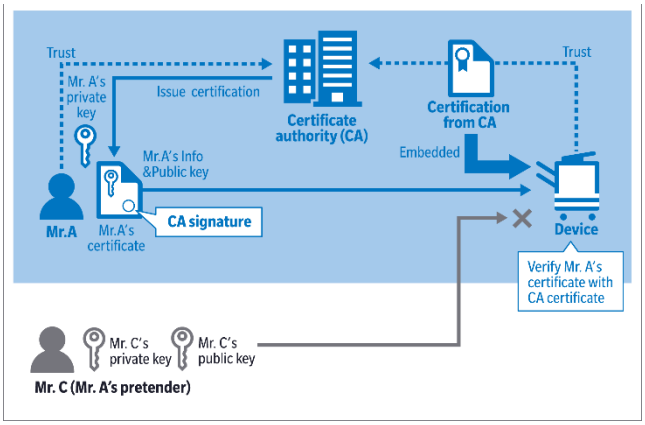


Figure 2-7

7. Dealing with viruses

Linux kernel is used as the OS of the controller integrated into the MFP.
The server type controller of EFI fiery uses Windows OS's, but necessary Windows security patches are provided in a timely fashion, measures are taken against Windows vulnerabilities.

8. Virus scan function

By installing the virus scan function, all detected viruses will be removed.
If a virus is detected in a TX job, the job will be discarded.
On the other hand, if a virus is detected in an RX job, you can now choose whether to execute the job or not. Previously, RX jobs (such as Print and Save in User Box) in which a virus was detected were always executed because viruses would disappear in the process of converting the job data into KM's own format. This change will enable safer and more secure operations.

Options	Virus	Job where virus detected	
		TX job	RX job
“Continue”	To be removed	To be deleted	To be executed
“Delete”	To be removed	To be deleted	To be deleted (except FAX/Email)
“Delete All”	To be removed	To be deleted	To be deleted

9. Dealing with external viruses on USB memory

In most cases, USB memory viruses are run and cause infection by simply inserting the USB memory, and since there is no mechanism in an MFP by which a run file is booted simply by inserting a USB memory, these kinds of viruses have no effect.
There are features on an MFP for connecting to USB memory, printing image data from USB memory, and saving scanned image data and image data saved to the box to USB memory, but since these features are run by user actions, they will not run automatically.

10. Routine monitoring of Linux kernel

For the Linux kernel, we monitor the disclosure of vulnerability information and the existence of security patches to verify whether the disclosed vulnerabilities are affecting the functionality of the MFP.

11. Separating from USB interface path

The USB interface path and network path are separated based on system architecture. Even if an MFP is connected with USB to a PC connected to the Internet, the MFP cannot be accessed from the Internet environment through the PC.

12. Separation of the communication between wireless LAN and wired LAN

The routing function between wireless LAN and wired LAN is not equipped. Therefore, no access is accepted from mobile devices etc. via wireless LAN to the devices connected with wired LAN.

III. Security for data in main MFP unit

1. Security for image processing and output processing

Data read from the scanner (received from the fax PCB) is compressed after image processing and written to the memory in the MFP (volatile memory). Print data is sent to the printer after being decompressed and printed on paper.
Data can be output page by page, or in one bundle after being temporarily stored on HDD or SSD.
Since data is overwritten on memory page by page, it cannot be output again.
When the [2.Feature for overwriting and deleting temporary saved HDD data] is enabled, job data (compressed data) is deleted from memory at the same time as output and transfers are completed, and further output or transfers by third parties are prevented.

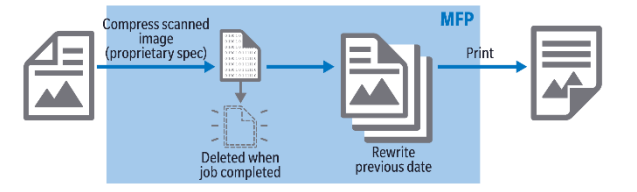


Figure 3-1

When saving on the HDD, when protection of HDD data by password and encryption (5) is enabled, in addition to the original compression process, all job data is encrypted and saved, so even if the HDD is removed, confidentiality of the data is maintained. (This feature is optional for some models.)
In addition, since all data on the HDD is saved in encrypted form, even if it happened to be taken off the HDD, its confidentiality is preserved. (This feature is optional for some models.)
If the secure print feature was used, once the print job is saved temporarily on the MFP's memory, print will start after the password is entered on the operation panel. This feature prevents others from taking away the printed paper.

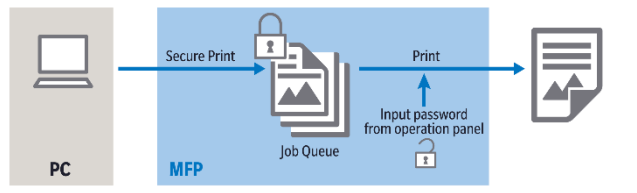


Figure 3-2

2. Feature for overwriting and deleting temporary saved HDD data

■ HDD (Hard Disk Drive)
Through settings of the HDD overwrite deletion feature, data saved temporarily to the hard disk can be deleted by overwriting when the image data is no longer in use, such as at the end of a print or scan job, or when box-saved documents are deleted.
Reduces the risk of no longer needed image data on the hard disk being reused.

[Mode 1]

1. Overwrite with 0x00

[Mode 2]

1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with the letter “a” (0x61)
4. Verify

Reference: Feature for overwriting and deleting HDD data is not supported for SSD (Solid State Drive). The flash memory used in SSD cannot be rewritten the data directly. To rewrite the data, it is necessary to delete before rewriting. In addition, while writing is done in units of pages, deletion is done in units of blocks composed of multiple pages.
When new data is written, the wear leveling function (*) avoids writing to the cells where the data was recorded last time. Data is deleted by creating a space in block units by the garbage collection function (*). However, the data being written is compressed in a KM-only format, so no meaningful information can be recovered. If MFP’s encrypt function is enabled, data will be compressed and then encrypted.

*** Wear leveling function:**
SSD and microSD record data in cells of flash memory. If the same cell is used continuously, the cell will deteriorate. In order to extend the life of SSD and microSD by leveling the use of cells, a controller built into SSD and microSD automatically changes the cells used. Therefore, SSD and microSD users are normally not allowed to write data by specifying a cell.

*** Garbage collection function:**
Garbage collection function automatically creates blocks only with unnecessary data and deletes data efficiently in order to increase the number of pages in which data can be written. At this point, valid data is moved to another block.

3. Complete data deletion when discarding HDD, SSD, and microSD

■ HDD (Hard Disk Drive)
The internal data of the hard disk can be deleted by overwriting with random numbers through the settings. This will prevent confidential information from leaking after the hard disk and the main MFP unit have been discarded.
The hard disk may have trace of previous data due to residual magnetism (*) on the disk. For more secure data deletion, a method of overwriting multiple times is implemented.

*** Residual magnetism:**
HDD is a method of recording data by magnetizing magnetic material coated on a disk with a magnetic head. Even if new data is written, the mass of magnetic material at the points corresponding to each bit does not face in the same direction at the boundary, leaving traces of previous data as residual magnetism.
Therefore, a threshold value is used to determine 1/0 in normal use of HDD.

[Mode 1]: Recommended by Japan Electronics and Information Technology Industries Association (JEITA) / Russian Standard
1. Overwrite with 0x00

[Mode 2]: US National Security Agency (NSA Standard)
1. Overwrite with random 1-byte numbers
2. Overwrite with random 1-byte numbers
3. Overwrite with 0x00

[Mode 3]: US National Computer Security Center (NCSC-TG-025) / US Navy (NAVSO P-5239-26)/ US Department of Defense (DoD5220.22-M)
1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with random 1-byte numbers
4. Verify

[Mode 4]: US Army (AR380-19)
1. Overwrite with random 1-byte numbers
2. Overwrite with 0x00
3. Overwrite with 0xff

[Mode 5]: Former US National Security Agency (NSA Standard)
1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with 0x00
4. Overwrite with 0xff

[Mode 6]: North Atlantic Treaty Organization (NATO Standard)
1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with 0x00
4. Overwrite with 0xff
5. Overwrite with 0x00
6. Overwrite with 0xff
7. Overwrite with random 1-byte numbers

[Mode 7]: German Standard (VSITR)
1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with 0x00
4. Overwrite with 0xff
5. Overwrite with 0x00
6. Overwrite with 0xff
7. Overwrite with 0xaa

[Mode 8]: US Air Force (AFSSI5020)
1. Overwrite with 0x00
2. Overwrite with 0xff
3. Overwrite with 0x00
4. Overwrite with 0xff
5. Overwrite with 0x00
6. Overwrite with 0xff
7. Overwrite with 0xaa
8. Verify

■ SSD (Solid State Drive), microSD
Write 0x00 by “overwriting and deleting all sectors”. Unlike magnetic data such as HDD, data on flash memory used in SSD and microSD can be completely deleted with a single overwrite.
There are some parts that is not accessible in SSD and microSD when writing 0x00 due to the wear leveling function, but it is difficult to read the data from these parts because they cannot be specified by logical address.

Additionally, using the feature “5. Protecting HDD, SSD, and microSD data by encryption” prevents all data from leaking including the data that cannot be overwritten by “overwriting and deleting all sectors”.

If stricter "complete data erasure" is required, you can erase it with the Format NVM command (Secure Erase). This method of erasure complies with the Purge level of NIST SP800-88 Rev1, which makes it completely impossible to recover the data. After erasure, a log will be generated as a proof.
* Please request your service representative to execute this function as executing this function will make the MFP not be able to start.

4. Feature for outputting reports after deleting all data

You can print a report of the results after deleting data.

5. Protecting HDD, SSD, and microSD data by encryption

Konica Minolta's MFP encrypt data in one or both ways.

- Use SSD's self-encryption function
- Use MFP's encrypt function

Both encryption methods are with AES256. The encryption key is generated by Konica Minolta's unique key generation algorithm when MFP is turned on. Therefore, it is not possible to recover data from HDD, SSD, and microSD that had been removed from MFP.

6. Protecting SDD by self-encryption

Konica Minolta's MFP equipped with SSD uses self-encrypting SSD. Self-encrypting SSD always encrypts the data in SSD using an encryption key generated in SSD (DEK: Data Encryption Key) except temporarily saved data.
SSD data is protected by encrypting this DEK by Authentication Key (AK) generated by MFP. AK is generated using a lock password when MFP is turned on. In addition, AK is also used to authenticate the use of SSD itself.
By setting a lock password, you can manage SSD use and protect SSD data.

7. Encrypting PDF files

When saving data scanned with the MFP in a PDF format file, it can be encrypted with a common key. When opening an encrypted PDF file with Adobe Acrobat, the common key must be entered.

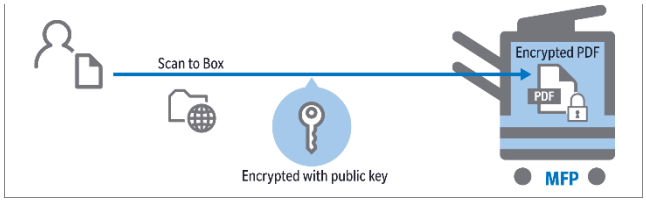


Figure 3-3

8. User authentication

MFP supports authentication that uses the authentication feature, or external servers such as Active Directory, or the PageScope Authentication Manager. Aside from password authentication, authentication is possible through a contactless IC card or biometrics, using the PageScope Authentication Manager.
It is possible to restrict the use of MFP copy, print, scan, and fax functions, and the color function, by restricting usage permission of the MFP combined with user authentication. Moreover, depending on the permissions level, registered addresses can also be restricted such as accessible fax and E-mail.

i. It can perform authentication using an external server, but even if an external server cannot be provided on the network, the user authentication feature is available since there is an authentication feature within the device.
ii. It can restrict the usage by setting an upper limit for output sheets data by user or department.
iii. Can also set different output permissions and upper limit for color and monochrome.

If authentication fails a specified number of times within a specified time, MFP determines that there is a possibility of a password attack, records those attempts in the job log and notifies the administrator by SNMP Trap or e-mail. This allows you to detect signs of unauthorized access at an early stage.
Similarly, if there are a specified number of authentication requests within a specified time*, MFP determines that there is a possibility of an authentication access attack, records those requests in the job log and notifies the administrator by SNMP trap or e-mail. It also delays the authentication response. This allows you to detect signs of an attack at an early stage, avoid overloading the MFP and keep it running.

* Regardless of whether the authentication was successful or not

9. Box security and utilization

In order to securely protect box data, user authentication and access to the box are password protected.

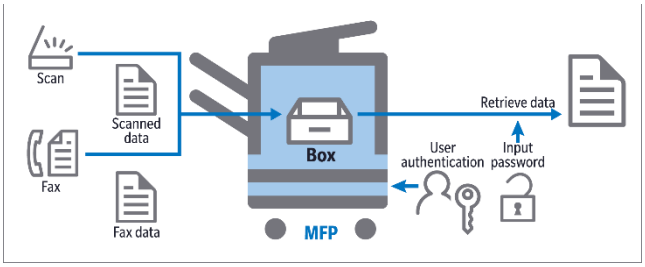


Figure 3-4

10. Encrypting E-mail data

When the sender transmits an E-mail with the MFP, he/she can use the receiver's certificate (public key: can register to address book) to encrypt the E-mail, and then the receiver can use their own private key to decrypt the E-mail on their PC. This allows for secure sending and receiving, without the content of E-mail being intercepted by others. Certificate registered to the LDAP server is used to obtain the public key from the network.

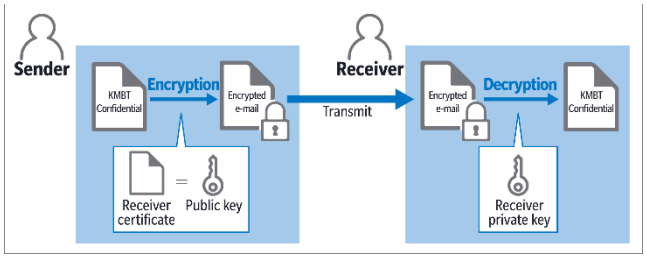


Figure 3-5

11. Signature feature for E-mail

The sender can add a signature to an e-mail with the MFP private key, and the receiver verifies the signature with the MFP certificate. This allows the receiver to verify that there was no tampering.

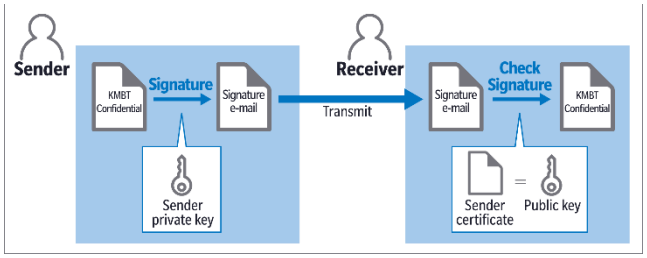


Figure 3-6

12. Scan to Me, Scan to Home & Scan to Authorized Folder

The scan data can be sent easily to oneself.
When configuring user authentication, the "Me" button will be displayed in the registered address column, and the "Home" button by enabling the feature in administrator settings.
If "Me" was selected for the address, it is sent to the e-mail address of the authenticated user, and if "Home" was selected, it is sent to the PC folder registered in advance, allowing for sending files simply and reliably with one touch.

SMB authentication can be restricted to SMB addresses other than one's own by not registering anything in the [user ID] and [password] columns of the SMB address, if a logged in user selects their own SMB address from the address book and sends, since the user authenticated user name and password are used without change.
Moreover, by restricting and prohibiting the register scope and direct input of addresses through administrator settings, it can be regulated such that send destinations can only be sent to addresses managed by the administrator.

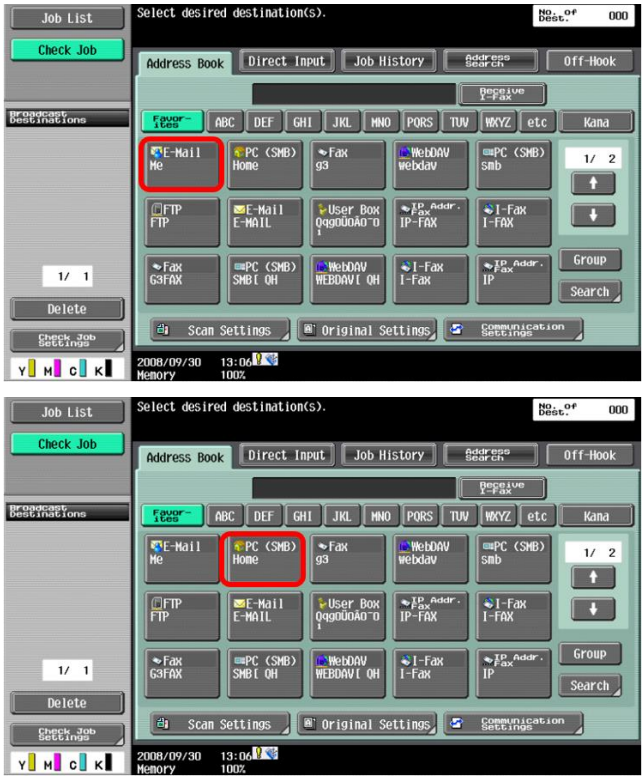


Figure 3-7

13. Access management with audit log

The history of actions is saved as an audit log. It can trace unauthorized access.

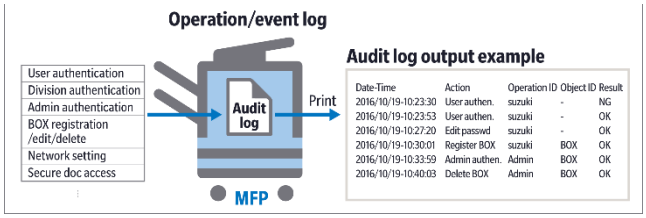


Figure 3-8

In addition, logs that record information such as login attempts and configuration changes can be sent using the Syslog protocol. This makes it possible to manage MFPs together with other IoT devices in an integrated manner with SIEM (Security Information and Event Management) products. The log format corresponds to CEF/LEEF.
Furthermore, when the MFP detects an operation that leads to an incident not intended by the administrator, it can notify the administrator by SNMP trap or e-mail. This allows you to quickly respond to unauthorized or unwanted activities even in environments where SIEM products are not implemented.

14. Using a certified encryption module

MFP has a built-in encryption module such as OpenSSL/MES (RSA BSAFE Micro Edition Suite), successfully implementing an encryption and authentication feature. The main features that use the MES encryption module with FIPS140-3 certification are listed below.

(1) Encryption communication when sending scan data
- During SSL/TLS communication such as Scan to WebDAV, TWAIN, etc.
- During S/MIME transmission for Scan to E-Mail.

(2) During SSL/TLS transmission for PSWC

(3) PDF encryption file generation feature

15. Protecting data with TPM

1. Purpose

When information such as passwords leaks to a malicious user through physical analysis in the MFP or eavesdropping on network packets, there is a risk of the MFP being accessed without authorization, and important internal data leaking.
Data encrypted using the root key always requires a TPM chip to decrypt since the key (root key) generated in TPM cannot be removed to outside the TPM.
Information such as passwords can be prevented from leaking by using TPM.

[Protected data]

i. Certificates registered by the administrator.
ii. The administrator password or password set by the administrator.
iii. The password set when the MFP provides services as a server.

2. TPM protection mechanism

Usually, information such as passwords on the MFP is protected using an AES key (256bit) or RSA key (2048bit) to prevent leaks. If TPM data protection is enabled, the RSA key is encrypted using a TPM root key as in the below figure.

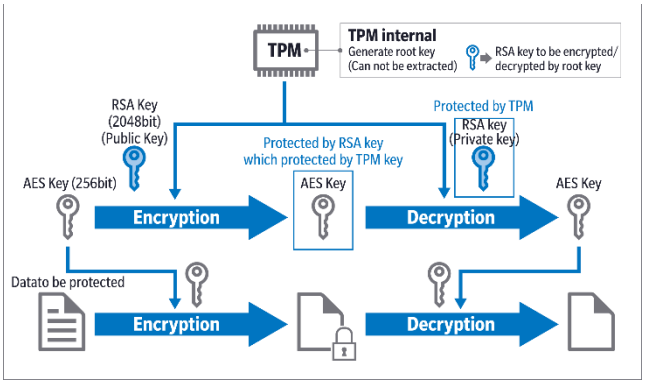


Figure 3-9

Since the root key cannot be copied from the TPM, a TPM chip is needed to decrypt the RSA key. If the RSA key cannot be decrypted, the AES key also cannot be decrypted, so that protected data such as passwords cannot be decrypted.

Therefore, by using TPM, even if a malicious user tries to analyze or eavesdrop on password information, the encrypted data cannot be decrypted without the TPM chip, thus preventing password information from leaking.

3. TPM key backup

By setting aside a backup of the RSA key in advance on the USB memory in case of a TPM chip failure, encrypted data can be saved.
(For security reasons, store the RSA key securely by encrypting it).

4. Elliptic Curve Cryptography (ECC)

AES key that has been protected by RSA so far as described above is now protected by Elliptic Curve Cryptography, which is safer than RSA. This will more strongly protect information from leaking.

IV. Output data security

1. Copy Protect feature

1. Copy protection print feature

A pattern can be embedded to the copy or print document (original copy) and highlighting patterns such as "Copy" on the copied documents, it can be clearly differentiated between original and copies. In addition, the serial number or output time of the MFP used for output can be set as the pattern. By combining the copied documents with serial number and output time with the above audit log, it is possible to identify users who made unauthorized copies.

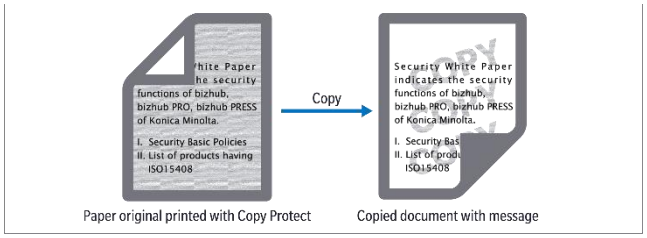


Figure 4-1

2. Copy guard feature / Password copy feature

Even if one tries to twice copy a manuscript outputted with a special security pattern added during copying or printing, the copy guard feature will produce a message stating that copying is prohibited, and it will not be copied. Moreover, if and only if a password set in advance using the password copy function was entered, the second copy with a security pattern will be permitted.

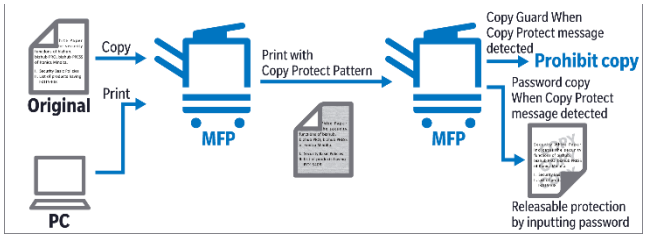


Figure 4-2

V. Authenticator

1. Security for data involved with biometric authenticator

Since the data for the biometric authenticator and AU-101/102 is managed under exceptionally tight security, illegal use is not possible.

- Using finger veins for biometric data

Forging vein is exceptionally difficult since they are inside the body and cannot be inadvertently read like a finger print.

- Data processing techniques used in this system

This system complies with security guidelines based on the "U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0". Various important security and privacy specifications are supported with this system.

- Replicating biometric data

Random number data calculated based on read data (from registration) is registered on the HDD. Replicating the original vein data from the data on the HDD is logically impossible.

- Data structure on the HDD

The data structure on the HDD is not disclosed. Therefore, forging and impersonation are not possible.

- Delete data on the authenticator

Data on the device is encrypted when it is stored temporarily to RAM and deleted after being transferred to the MFP. Forging veins is exceptionally difficult because they are inside the body and cannot be inadvertently read like a finger print.

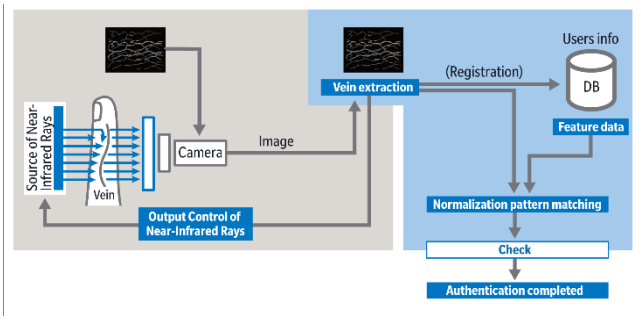


Figure 5-1

* U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 1.0: See https://www.commoncriteriaportal.org/files/ppfiles/pp_bvm_mr_v1.0.pdf

2. Authentication and print (one-touch security print)

By linking with the user authentication feature, simple and strictly confidential print work is successfully implemented. Printed work is no longer taken away or peeked at by others. Moreover, by using the biometric authenticator or card authenticator, performing authentication is simple.

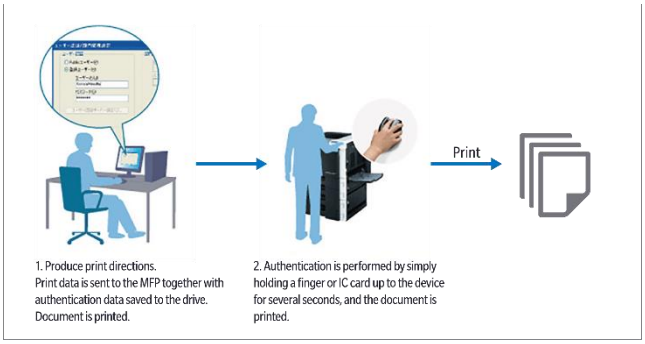


Figure 5-2

VI. Security for connectivity with mobile devices

Konica Minolta offers a wide variety of security features protecting connectivity between mobile devices and MFPs/printers. This section gives an overview of each security feature and any related information security threats and countermeasures.

1. Security for AirPrint

AirPrint is an iOS standard print feature, requiring no applications and drivers, and allows simple-operation printing from an application. Security threats and countermeasures are explained below.

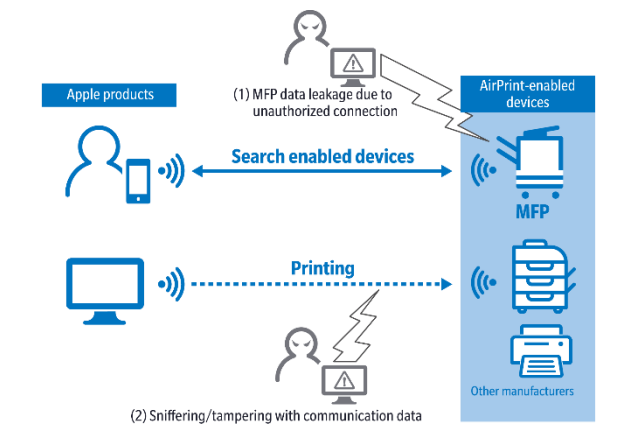


Figure 6-1

Threat	Countermeasure
(1) MFP data leakage due to unauthorized connection	Prevention of unauthorized connection by IPP authentication
(2) Sniffing/tampering with communication data	Data encryption by SSL/TLS

2. Security for Mopria

Installing a Mopria plug-in into an Android device allows simple-operation printing from an application. Security threats and countermeasures are explained below.

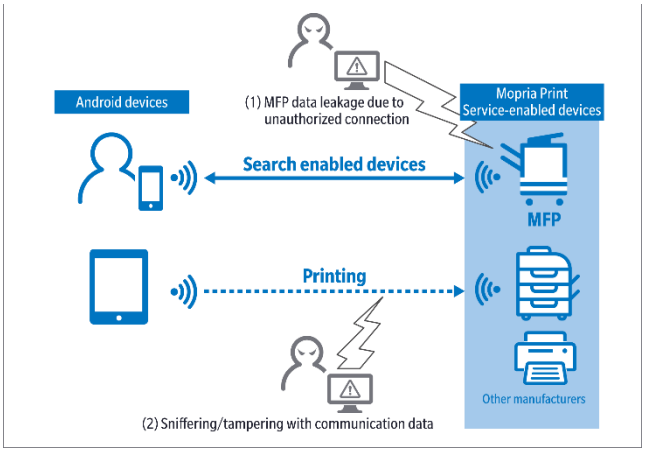


Figure 6-2

Threat	Countermeasure
(1) MFP data leakage due to unauthorized connection	Prevention of unauthorized connection by IPP authentication
(2) Sniffing/tampering with communication data	Data encryption by SSL/TLS

3. Security for Google Cloud Print

Google Cloud Print is a service that enables printing from an MFP via the Internet. Security threats and countermeasures are explained below.

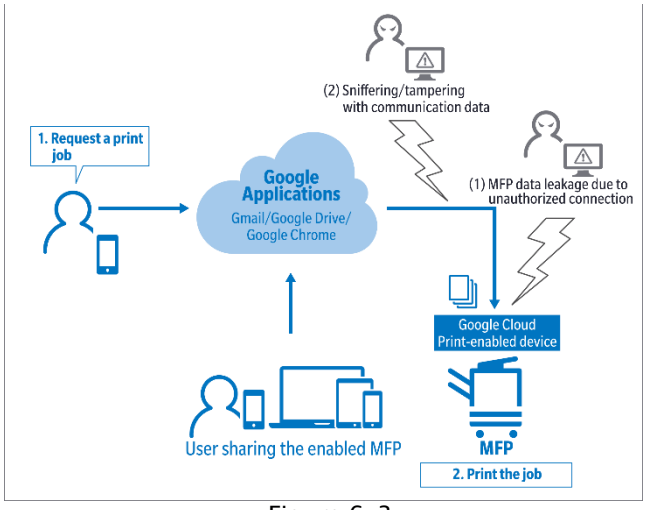


Figure 6-3

Threat	Countermeasure
(1) MFP data leakage due to unauthorized connection	Access restriction by setting IP filtering
(2) Sniffing/tampering with communication data	・Data protection by WEP or WPA authentication of the main unit wireless network ・Data encryption by SSL/TLS

4. Security for Konica Minolta Print Service

Konica Minolta Print Service enables printing from an MFP by installing Konica Minolta's plug-in into an Android device. Security threats and countermeasures are explained below.

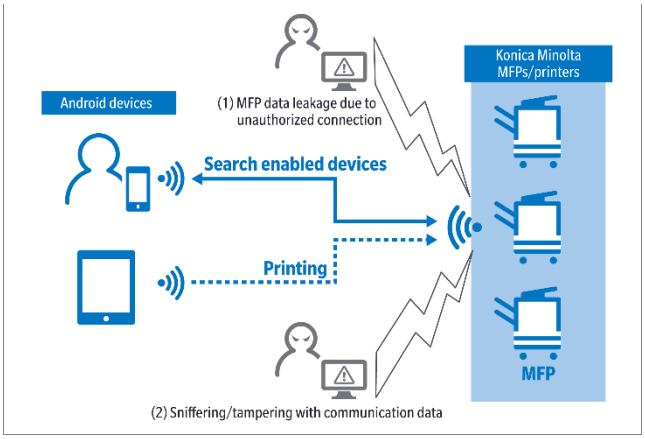


Figure 6-4

Threat	Countermeasure
(1) MFP data leakage due to unauthorized connection	Access restriction by setting IP filtering
(2) Sniffing/tampering with communication data	Data protection by WEP or WPA authentication of the main unit wireless network

5. Security for Konica Minolta Mobile Print and PageScope Mobile

Konica Minolta Mobile Print and PageScope Mobile uses Wi-Fi and enables printing from an MFP, e.g., documents in mobile devices or online storage, or webpages or email content viewed with Konica Minolta Mobile Print or PageScope Mobile. Security threats and countermeasures are explained below.

- Scanning and printing with Konica Minolta Mobile Print or PageScope Mobile

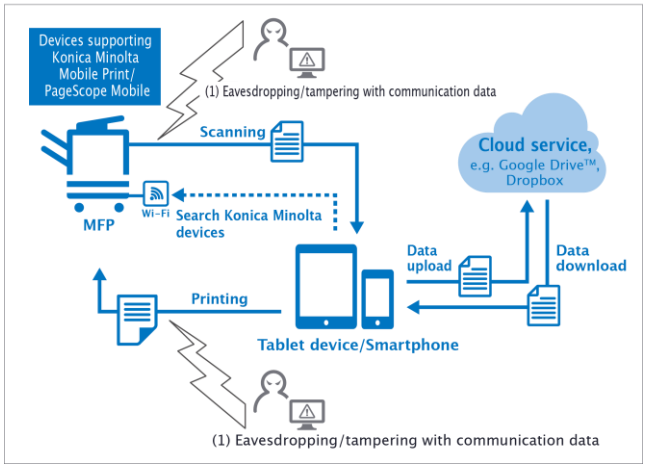


Figure 6-5

- Pairing by NFC, Bluetooth LE, or QR code reading

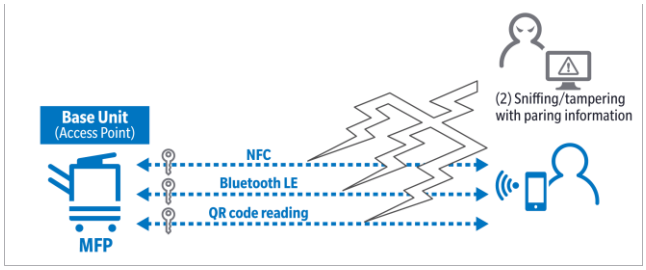


Figure 6-6

- NFC authentication

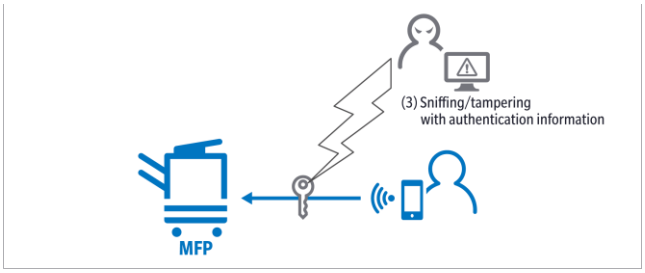


Figure 6-7

Threat	Countermeasure
(1) Sniffing/tampering with communication data	Data protection by WEP or WPA authentication of the main unit wireless network
(2) Sniffing/tampering with pairing information (NFC, Bluetooth LE, QR code)	Data encryption using a private key
(3) Sniffing/tampering with authentication information (NFC)	Data encryption using a private key

VII. PKI card authentication system

< Overview >

The PKI card has encryption/decryption and electronic signature features. By linking this card with MFP features, it is possible to build an MFP usage environment with a high security level.

1. Log-in using PKI card

Insert the PKI card into the card reader and enter the PIN to perform authentication to Active Directory. At that time, the digital certificate sent from the Active Directory to the MFP can be verified with the MFP.

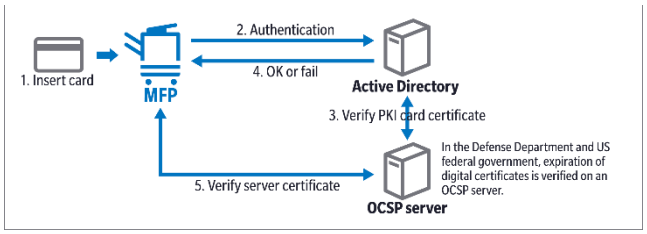


Figure 7-1

2. LDAP search using PKI card

Use the Kerberos authentication ticket acquired from Active Directory authentication to log into the LDAP server when performing an address search on an LDAP server. Since it can be accessed with a single authentication, a very easy-to-use single sign-on environment can be built.

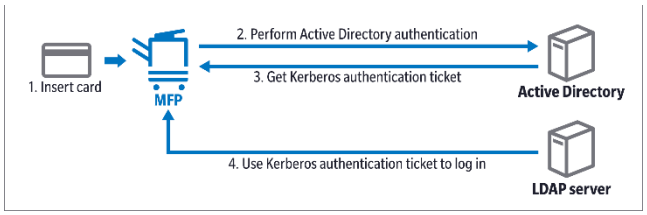


Figure 7-2

3. SMB transmission using PKI card

Use the Kerberos authentication ticket acquired from the Active Directory authentication to log into the computer of the address when sending scanned data via SMB. Since it can be accessed with a single authentication, a very easy-to-use single sign-on environment can be built. Moreover, by using the authentication ticket, since it allows for the password to not be circulated on the network, SMB transmission can be performed securely.

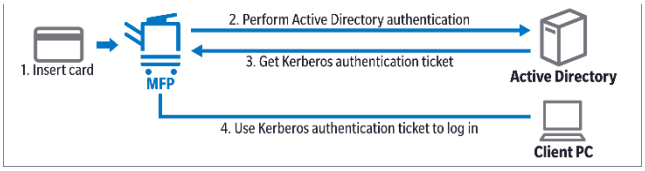


Figure 7-3

4. E-mail transmission using PKI card (S/MIME)

Using a PKI card when sending E-mail, it is possible to implement a digital signature. By implementing a digital signature, the sender of an E-mail can be certified.

Moreover, if the address certificate is registered, it can be combined with E-mail encryption and sent. By sending the E-mail encrypted, one can prevent information leaking to a third party on the transmission path.

Figure 7-4

5. PKI card print

Encrypt print data from printer driver with a PKI card and send to MFP. Print data is stored in the PKI encryption box of the MFP, and by the same user performing PKI card authentication with MFP, it can be decrypted and printed.
Since print data can only be printed if authentication by a PKI card on the MFP succeeds, the confidentiality of data is preserved.

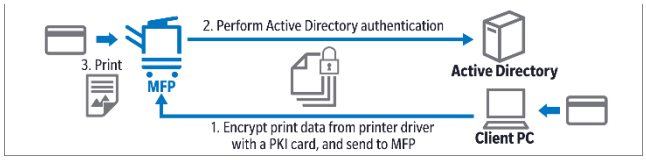


Figure 7-5

6. Scan to Me / Scan to Home

This feature allows for sending scanned data to one's own E-mail address and computer. Since one's own E-mail address and the path of the home folder are obtained during Active Directory authentication, it can be easily sent.

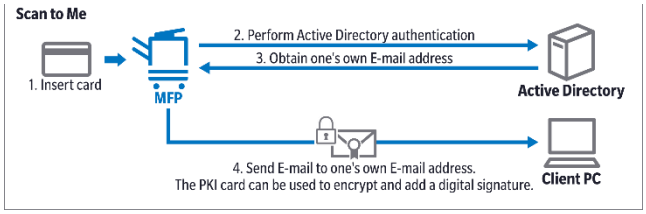


Figure 7-6

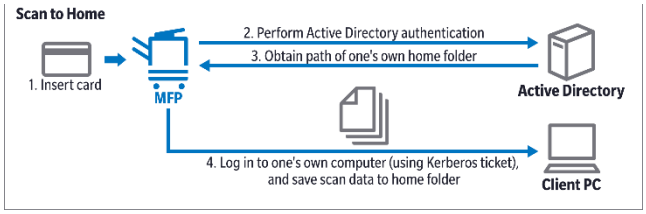


Figure 7-7

VIII. Security concerning MFP self-protection

1. Firmware verification feature

When rewriting the main MFP unit's firmware, a hash value check is run to check if the firmware data was tampered with. If the hash values don't match, an alert is issued, and the firmware is not rewritten.
In addition, if enhanced security mode is used, hash value checks are performed when the main power source is turned ON. If the hash values don't match, an alert is issued, and starting the main MFP unit is prohibited.
Hash values for firmware data are checked against digitally signed hash values.

FW data is private. In addition, if the client's administrator prohibits the rewriting of firmware, service personnel from Konica Minolta cannot update it either, so it cannot be rewritten by a third party.

IX. Security for CS Remote Care

1. Basic security and collected data

During CS Remote Care (henceforth, CSRC), to send the main unit data and change the main unit settings, the CSRC host communicates with the MFP.
To communicate with the remote diagnosis system, an ID registered in advance on both the CSRC host and the device is to be used, and perform connection communication. The registered details of the CSRC host and the transmission content of the device are to be verified to if they match with this communication.
And once communication terminates normally, it will from then on be possible to perform remote diagnosis communication. Remote diagnosis communication is performed after verifying the ID of each communication. If the IDs do not match at the time of communication, the communication will not be performed.
In addition, data collected by CSRC is service information such as count values, and no content is included related to fax addresses or personal information.

The communication protocol via a public line is shown below.

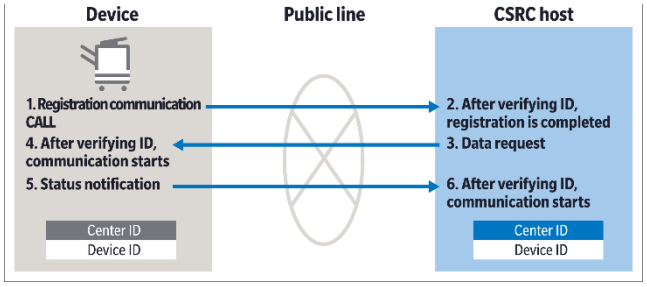


Figure 9-1

2. Security when using an LTE device

When an LTE device is connected to the MFP, the built-in SIM can only communicate with a closed network.
In addition, since the LTE gateway server authenticates the ID to establish whether the LTE device is connected to the MFP, communication is only allowed with LTE devices to which prior permission has been given.
AES and SNOW3G encryption ensure air communication security from an LTE device to a base station.

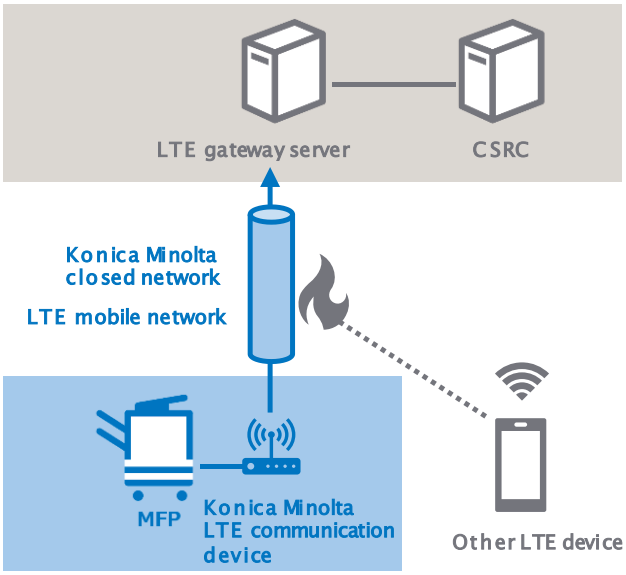


Figure 9-2

3. E-mail security

- Encrypt transmission data

Use the encryption key (common key) on the MFP and CSRC host to encrypt data.
* The encryption can be configured at the MFP and center.

With the common key encryption method, the same key is used for encryption and decryption at the main unit and center. This allows for secure sending and receiving, without the content of E-mail being intercepted by others.

- Verify ID

Information (Center ID and serial number) is included in sent and received E-mails that allows sender and recipient to be verified. This information is used to verify if the sender and recipient are correct.
In addition, an E-mail ID is assigned to E-mails sent from the center. The E-mail ID of the responder E-mail is used for the response E-mail from the MFP. ID will be verified with E-mail ID the center sent.

- Removing unauthorized E-mails

The sent or received E-mail is considered unauthorized data and removed in process of verifying the above ID if the information (Center ID and serial number) for verifying the sender and recipient and the E-mail ID do not match.

4. HTTP communication security

- Encrypt transmission data

The same as E-mail mentioned above, data is encrypted by using the encryption key (common key) on the MFP and CSRC host.
With the common key encryption method, the same key is used for encryption and decryption for the device and CSRC host.

- Communication between CSRC and MFP

All HTTP communication between CSRC and MFP uses certificates issued by the respective Konica Minolta license management servers (LMS), with HTTPS (TLS) communication carried out by means of client and server authentication (product authentication). Only MFPs with a certificate issued by the LMS are allowed to communicate, ensuring secure communication without spoofing.
TLS combines security technologies such as public key encryption, private key encryption, digital certificates, and hash functions to prevent eavesdropping or tampering with data.

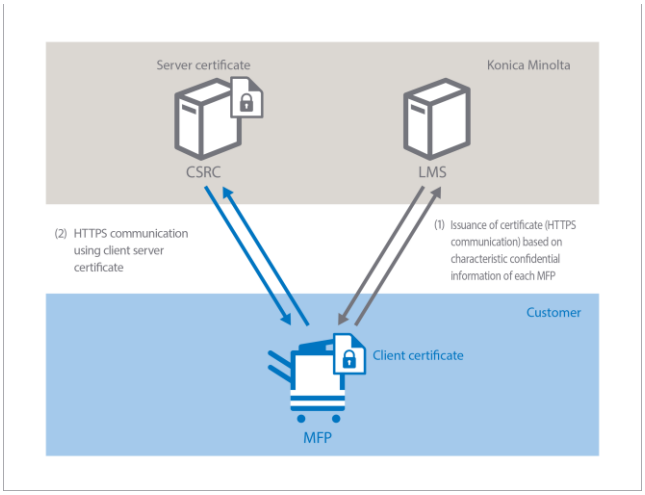


Figure 9-3

5. DCA security

- SNMPv3 communication between DCA and devices

The DCA (Device Collection Agent) supports SNMPv1 and SNMPv3 communication as method of communicating with devices.
Since with SNMPv1, unencrypted data circulates on network paths, an environment in which packets may be captures from the outside is at risk of having communication data eavesdropped on.
In addition, if the "community name", the only authentication in SNMPv1 communication, is leaked at the same time, it will be possible to access all data stored on the MIB of devices managed under the leaked "community name".
The "user name" corresponding to the community name in SNMPv1 communication and mechanisms for authentication are added to increase the robustness against access to devices in SNMPv3 communication.
In addition, all data circulating on communication paths is encrypted, and as long as the same encryption methods and encryption key are not known, it is difficult to eavesdrop on data.

- Communication between DCA and CSRC host

Communication between DCA and the CSRC host uses SSL/TLS on the HTTP protocol and is encrypted.
Moreover, a unique ID is allocated to DCA, and for each communication data is transferred after this ID is verified.
If this ID does not match during communication, data transfers will not be performed.

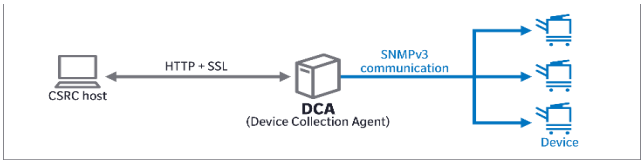


Figure 9-4

X. Security involving bizhub Remote Panel

1. Communication, connection trigger

The bizhub Remote Panel does not allow HTTP communication without encryption. Encryption with SSL/TLS is performed without fail for the communication, and HTTPS used.
Moreover, it is not possible to connect to a device from the bizhub Remote Panel Server side. Since connections can only be made from the device side, customer security is ensured.

2. Authentication

More secure communications are performed when a certificate issued by a CA (certificate authority) is assigned to the device and bizhub Remote Panel Server to perform communication.

3. Access Code

bizhub Remote Panel Server allows for multiple devices and multiple users (clients) to connect and use it at the same time. The user selects the device they would like to connect to from a list of multiple devices and enters a 4-digit Access Code to connect. The Access Code notifies the client (serviceman, operator) permitted by the customer of the 4-digit Access Code displayed on the panel of the device in advance.

4. Audit log

The log records when the device and bizhub Remote Panel Server are connecting, and when the client (user) begins and finishes remotely operating the device. By tracking the log, the administrator can monitor the access of bizhub Remote Panel users.

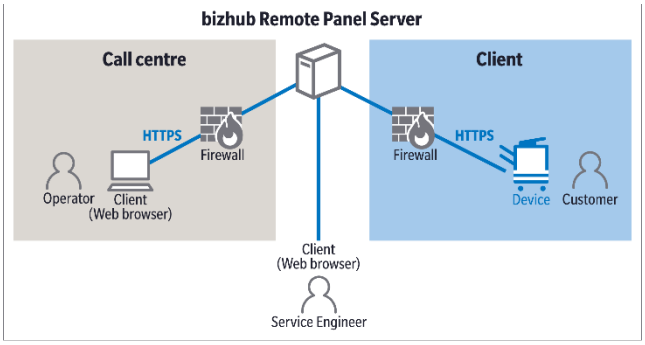


Figure 10-1

XI. Security for World Wide Remote Service Platform

< Overview >

WWRSPF (World Wide Remote Service Platform) carries out SSL/TLS communication and data storage in communications between all communicating devices and systems. It also delivers secure communication by preventing spoofing through measures such as client server authentication, Global IP address restriction for senders, and native XMPP IDs, etc.

1. Communication between WWRSPF and MFP

All communications between WWRSPF and MFP use certificates issued by the respective Konica Minolta license management servers (LMS), with HTTPS communication carried out by means of client and server authentication (product authentication), ensuring secure communication without spoofing.

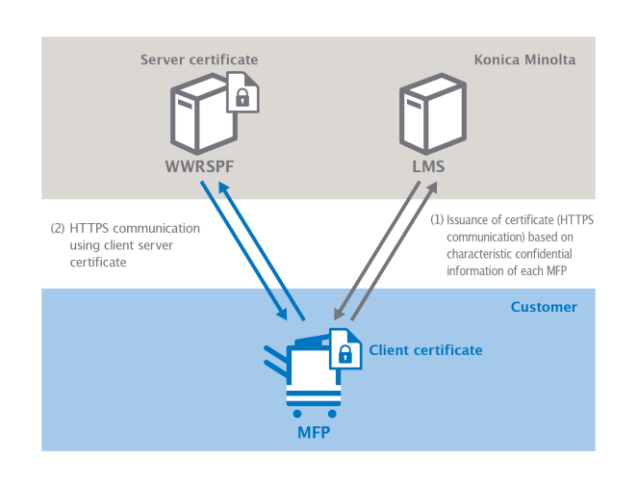


Figure 11-1

2. Communication between WWRSPF and XMPP PF

Two-way communication is carried out between WWRSPF and XMPP, and data is encrypted. IP addresses are limited to those which only the respective WWRSPF and XMPP PF sender Global IP addresses will recognize.

3. Communication between XMPP PF and MFP

At the time of initial connection from MFP (a), WWRSPF registers in XMPP PF (b) and sends the XMPP PF access point URL, login ID and password, etc. to MFP. In turn, MFP uses these pieces of information to carry out two-way encrypted communication with XMPP PF and XMPP over BOSH or XMPP.

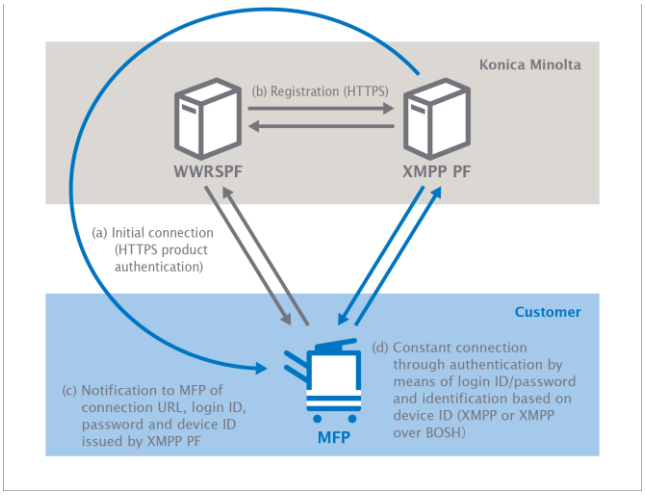


Figure 11-2

4. Communication from WWRSPF to MFP

WWRSPF encrypts and sends ticket ID via XMPP PF (a) to MFP. MFP connects to WWRSPF (b1, b2), delivers the ticket ID, and acquires detailed instructions. At this time, WWRSPF compares the ticket ID and confirms whether the instructions are the same as the instructed response from MFP.

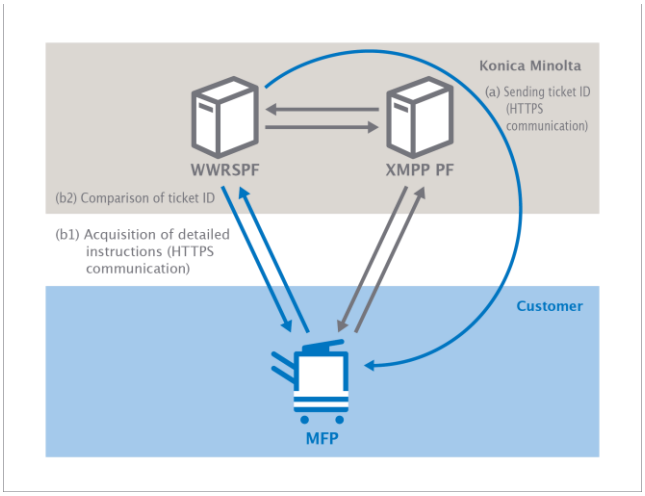


Figure 11-3

5. Linking WWRSPF and CSRC

CSRC and WWRSPF fulfill items (1) and (2) below, and carry out HTTPS communication, ensuring secure data communication without data leakage.

(1) The WWRSPF administrator must register the Global IP address of CSRC in advance.
(2) CSRC accesses WWRSPF by using the User ID and Password required for login to WWRSPF.

Also, information instructed by the user from the UI of WWRSPF or CSRC is saved as an audit log.

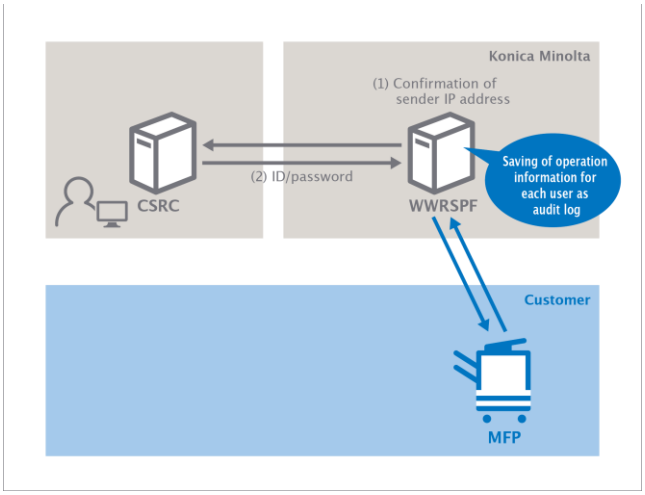


Figure 11-4

6. Communication using RSA (Remote Service Agent)

By going via RSA (Remote Service Agent) Cloud / Edge, communications between multiple MFPs installed on the customer network and WWRSPF on the internet can be concentrated (Fig. 11-5). By concentrating communication, it will be easier for IT managers to manage communication and, in turn, identify unauthorized external communication.

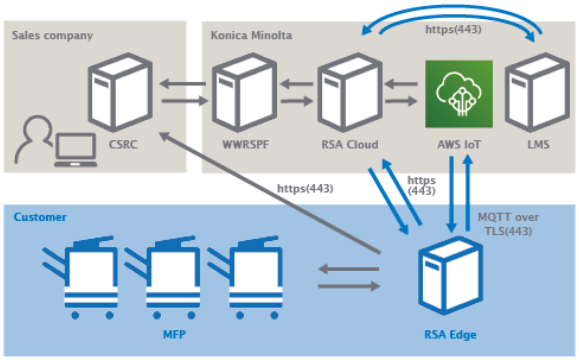


Figure 11-5

7. Registration of RSA Edge, and acquisition of information required for connection of RSA Cloud and AWS IoT

When directing RSA Edge registration on CSRC (a-c), RSA Cloud acquires the RSA Edge product authentication certificate from LMS (d).
RSA Cloud uses a different AES private key for each Edge to encrypt the acquired RSA Edge certificate and the private key for RSA Edge signature created using this certificate, the RSA Cloud certificate, and the activation key issued for each RSA Edge, and compiles these in a single data file. This data file can be downloaded on CSRC.

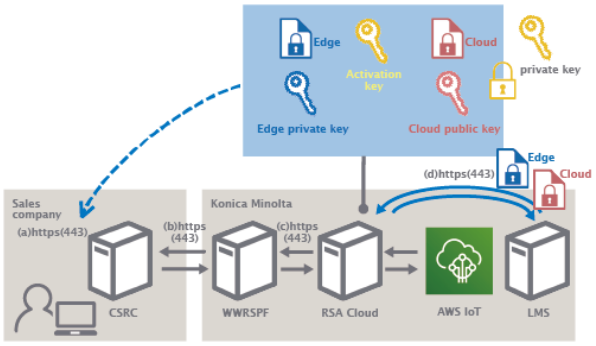


Figure 11-6

8. Communication between RSA Edge and RSA Cloud

(a) When installing RSA Edge, the data file downloaded on CSRC is decrypted and read with the AES private key.
(b) When RSA Edge carries out HTTPS communication with RSA Cloud, the RSA Edge certificate is sent to RSA Cloud and the validity of RSA Edge is confirmed by means of client authentication.
(c) Also, RSA Edge signs the activation key with the RSA Edge private key and sends this to RSA Cloud. RSA Cloud carries out decryption with the RSA Edge public key and confirms the validity of (activates) RSA Edge by means of decryption and the activation key. Provided that there is no problem, RSA Cloud issues an access key (access token) and returns this to RSA Edge. Thereafter, RSA Edge communicates using the generated access key when communicating with RSA Cloud.

When sending the instruction script sent from RSA Cloud to RSA Edge, it also sends the script's hash value, which is signed using the public key created from the RSA Cloud certificate. RSA Edge confirms the signature with the RSA Cloud public key and checks for any falsification in the script. In this way, RSA Edge and RSA Cloud provide secure communication ensuring integrity and confidentiality.
Incidentally, if you want to rebuild RSA Edge with the same RSA Edge ID, since the activation keys issued for each RSA Edge cannot be reused, it is necessary to reissue activation keys from CSRC. When reissuing, it will no longer be possible to use the access key (access token) generated in the previous activation, nor will it be possible to communicate with RSA Cloud.

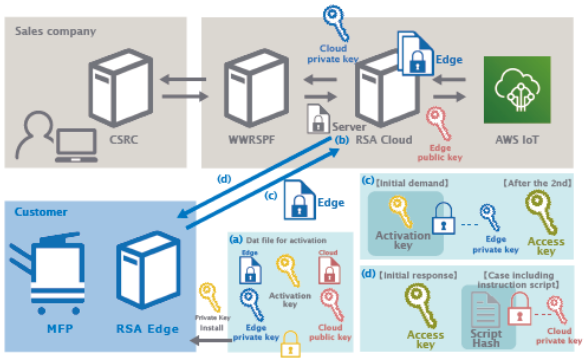


Figure 11-7

9. Communication between RSA Edge and AWS IoT

(a) When RSA Edge establishes "MQTT over TLC" communication with AWS IoT, an RSA Edge certificate is sent to AWS IoT, and the validity of RSA Edge will be confirmed by means of client authentication.
In this way, RSA Edge and AWS IoT conduct secure communication.

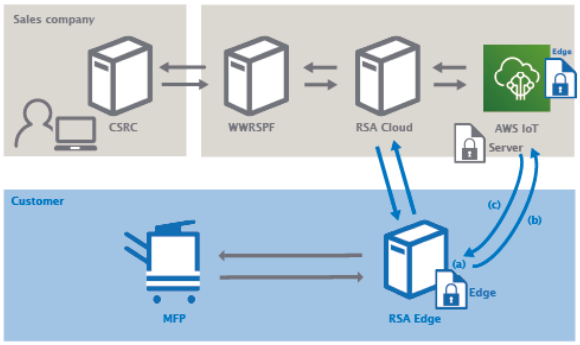


Figure 11-8

XII. Security involving bizhub Remote Access

< Overview >

By installing bizhub Remote Access to a smartphone or tablet device from Google Play or the AppStore, the main unit panel screen of the multifunction printer connected through the network can be remotely displayed on the screen of the smartphone or tablet device. By touch operating the main unit panel screen displayed on the terminal, the multifunction printer can be remotely operated.

1. Pairing

Eavesdropping/tampering with NFC, Bluetooth LE, or QR code pairing information is prevented by data encryption using a private key.

2. Communication, connection trigger

The MFP rejects remote connection from bizhub Remote Access as long as the bizhub Remote Access function is not enabled. It thus prevents unpermitted MFPs from being remotely operated.

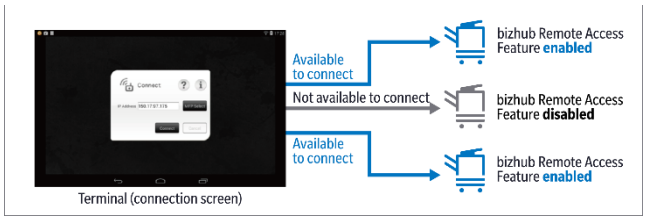


Figure 12-1

3. Automatic disconnect from timeout

If left standing by for a long time during a remote connection with bizhub Remote Access, the MFP will automatically disconnect from bizhub Remote Access, safeguarding users separated from the terminal during remote operation.

4. Security in administrator mode

The MFP offers safeguards in administrator mode by rejecting remote connection from bizhub Remote Access.

5. Security following a disconnection during remote operation

If bizhub Remote Access is disconnected during remote operation, by resetting the screen, the MFP ensures security even when viewing a password protected box or entering a password.

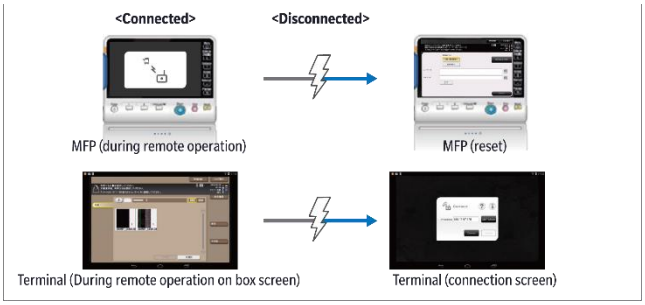


Figure 12-2

6. Security when using both user authentication and department authentication

When bizhub Remote Access is trying to connect to an MFP while authenticating a user or authenticating a department, the MFP will reject connections from bizhub Remote Access.
Moreover, if bizhub Remote Access is disconnected from the MFP during authentication, the MFP automatically logs out.
These features provide safeguards for authenticated users and authenticated departments.

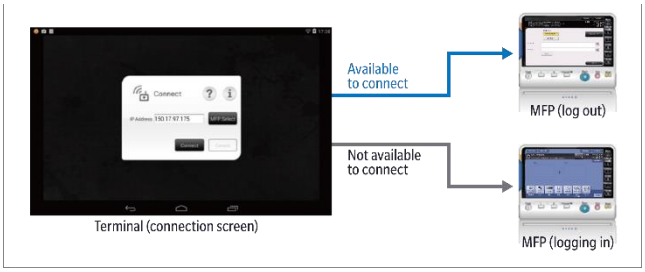


Figure 12-3

XIII. Security for CSRA (CS Remote Analysis)

< Overview >

CSRA regularly collects sensor data of the copying machine. The system analyzes the collected data to analyze and predicts bugs and predicts part life. When maintenance is performed, bug cause analysis and countermeasures can be prepared before the visit, allowing for smooth maintenance work.
In addition, data collected by CSRA is machine control information such as sensor data values, and no content is included related to personal information.
Setup by a serviceman is needed to turn ON CSRA features.

1. HTTP communication security

CSRC communication must be established in advance in order to perform communication with CSRA. The CSRC connection verifies whether the connected devices are correct.

- One-way communication

Only one-way communication in which data is sent regularly to the specified server from the main MFP unit is supported. No feature is provided for accepting communication requests from external servers.

- Encrypt transmission data

SSL/TLS can be configured with HTTP communication. (HTTPS)
Using SSL/TLS, encryption is performed with the communication data of "Device <-> WebDAV server" and "WebDAV server <-> CSRC host".

- The many secure features of the HTTP protocol can be applied

HTTP protocol is not environment dependent, allowing for many secure features such as authentication, Proxy, and SSL/TLS to be used.
SSL/TLS combines security technologies such as public key encryption, private key encryption, digital certificates, and hash functions to prevent eavesdropping on and tampering with data, as well as impersonation.
By using these secure features even at the center, security measures can be implemented that match with the client environment.

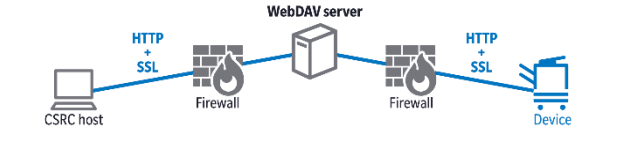


Figure 13-1

XIV. Security concerning MFP integrated SaaS GW

< Overview >

MFP integrated SaaS GW is formed from integrating the Gateway function that links the Konica Minolta cloud and office devices and is implemented in connection with HTTPS and XMPP communication features.
MFP integrated SaaS GW provides the following functions.

- Provides services in the cloud and two-way real-time communication
- Manages the local devices which can be specified from services in the cloud

In order to turn ON MFP integrated SaaS GW functions, a service engineer or administrator needs to configure it.

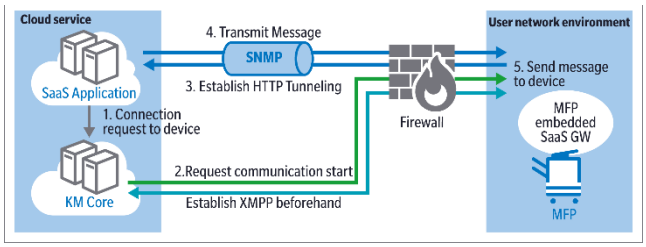


Figure 14-1

1. Communication between SaaS GW and the cloud

Connection information of the cloud service is registered in advance to the MFP.
Moreover, corresponding information is saved and managed on the cloud side as well.
By verifying the other device two-way, and specifying the recipient in this way, the risk of false connections from impersonation or tampering on the communication path is eliminated.

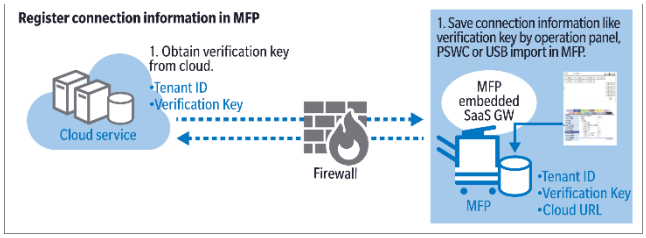


Figure 14-2

2. Communication protection and encryption

The communication between the SaaS GW and the cloud service is HTTTPS, and data for authentication is encrypted using an RSA private key.

3. Preventing impersonation

When registering SaaS GW to the cloud, notify the cloud of the Tenant ID and verification key from the SaaS GW, and after crosschecking the data on the cloud side, send the GW ID and private key to the SaaS GW.
The corresponding list of the GW ID and private key is managed on the cloud side.
Then, SaaS GW uses the private key at the start of communication with the cloud to send the encrypted data for authentication and GW ID, and the cloud determines whether the recipient is authorized by decrypting it with the private key corresponding to the GW ID.

(1) Register SaaS GW to cloud

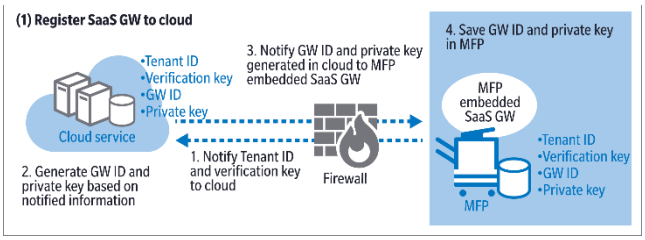


Figure 14-3

(2) At the start of communication to cloud

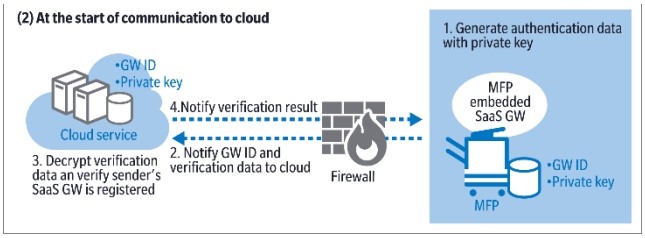


Figure 14-4

XV. Security concerning CWH

< Overview >

Center Warehouse (hereinafter referred to as CWH) is a system which periodically collects data such as MFP sensor data, and based on analysis of that data, analyzes and predicts malfunctions, and predicts part life. When maintenance is performed, analysis of malfunction causes and countermeasures may be prepared before the visit, allowing for smooth maintenance work.
In addition, the data collected by CWH is CSRA and CSRC data which includes machine control information such as sensor data values and does not include content related to personal information.
To enable CWH functions, configuration by service personnel is required.

1. 2-way HTTPS communication security

All communication between the MFP and Precheck Server uses certificates issued by respective Konica Minolta license management servers (LMS), with HTTPS communication carried out by means of client and server authentication (product authentication), ensuring secure communication without spoofing.
The MFP and Bridge Server are connected via HTTPS without product authentication. However, since communication uses Bridge Server information provided by the secure Precheck Server, the security level of this communication is equivalent to that which uses product authentication.

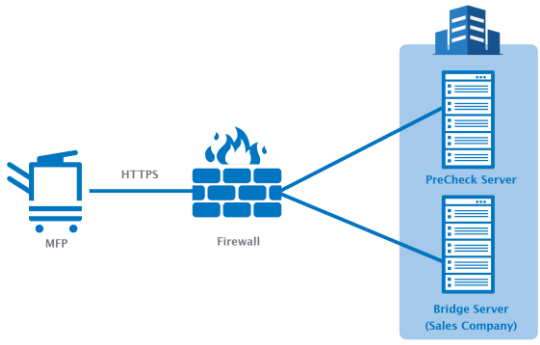


Figure 16-1

2. 1-way HTTPS communication security

All communication between the MFP and Bridge Server uses certificates issued by respective Konica Minolta license management servers (LMS), with HTTPS communication carried out by means of client and server authentication (product authentication), ensuring secure communication without spoofing.

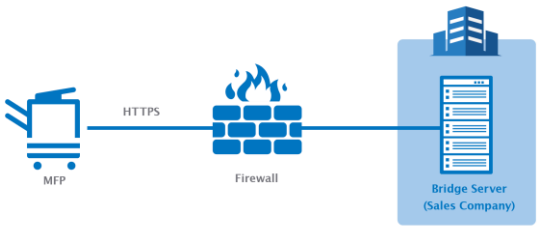


Figure 16-2

XVI. Protection of user information

At time of shipment from the factory, Konica Minolta MFPs are set to only handle that which is necessary from users' personal information.

1. Restrictions on display of personal information

Items other than login user/department are not displayed on the [Job List] or [Job History] screens during operation.

2. Administrator password settings

If the administrator password has not been changed from the default, or if conditions for password rules are not met, a message will be shown at startup with a prompt to change the default password.

3. Quick IP filtering

For IPv4 addresses, only the one set to this machine and IPv4 addresses with the same upper three bytes are allowed access.

Example)

If this machine's IPv4 address is 192.168.0.134, the range of IPv4 addresses allowed access will be as follows:

192.168.0.0 - 192.168.0.255

For IPv6 addresses, only global unicast addresses (2000::/3) are allowed access. In addition, only the IPv6 address set to this machine and IPv6 addresses with the same upper 64 bits are allowed access.

Example)

If this machine's IPv6 address is 2345:1:2:3:4:5:6:7, the range of IPv6 addresses allowed access will be as follows:

2345:1:2:3::0 - 2345:1:2:3:FFFF:FFFF:FFFF:FFFF

4. Display of shortcut to Quick Security Settings

A shortcut for changing the aforementioned and following settings is displayed.

[Password Rules]

Password rules used by the MFP can be enabled.

- Minimum number of characters, set with [Minimum Password Length] (default:12 characters)
- Alphabetical characters are case-sensitive
- Only one-byte symbols may be used
- Passwords using only the same character are prohibited
- Using the same password as before is prohibited

[Web Connection Settings]

You can set whether to use MFP via Web Connection.

[USB Use Settings]

You can set permissions for use of USB ports.

XVII. Security concerning Fleet RMM

< Overview >

Fleet RMM is a system that performs collective settings of different functions, and views and monitors device information for multiple devices. Users can log in and operate the system from a web browser. Fleet RMM comprises the following applications.

Table 18-1: Fleet RMM Composition

Application	Description
Edge	One or more communication layers which communicate with the device. Following the instructions from the Fleet RMM application, it acquires information from and configures the devices.
Fleet RMM application	Business Intelligence Layer for device data management and implementation of different functions, and Presentation Layer at the interface with users. It executes various tasks by means of user instructions or automatic activation by timer. Fleet RMM application contains a database and retains data such as device information and task execution results. Communication with the device is carried out via Edge.

1. Security of communication

Authentication communication using Fleet RMM uses SSL/TLS to securely send and receive authentication data.

In Fleet RMM, "Super Admin" creates users and user authentication is done with passwords.

(1) Communication with device

Fleet RMM uses SNMP v 3 or SSL/TLS to communicate with the device (MFP), and data can be sent and received securely.

Table 18-2: Details of transmitted data

Transmitted data	Protocol	Cryptography	Note
Configuration data	HTTP	SSL/TLS	OpenAPI Ext/Int
Configuration data (MIB)	SNMP v1/v3	When using SNMP v3, encrypted communication is possible with DES or AES	
Configuration data (XML)	HTTP	SSL/TLS Encrypt and transfer XML files	Data trans-mission via WebDAV
Configuration data (JSON)	SMB	Transfer JSON files with AES-encrypted.	Data transmission via SMB

(2) Port number

Table 18-3: Details of communication protocol type and port number used by Fleet RMM

Source	Destination	Protocol type	Port number (Default)	Communication protocol	Intended use
User (Web browser)	Fleet RMM application	HTTPS	443 *3	TCP	Access to Fleet RMM Web application Access to Fleet RMM WebAPI
User (Web browser)	Microsoft Entra ID	HTTPS	443	TCP	Access to the sign-in screen of Microsoft Entra ID. ※ This is used in case of SAML authentication.
Fleet RMM application	Fleet RMM Edge	HTTPS	5000 *2	TCP	Access to WebAPI of Edge
Fleet RMM application	SQL server	ms-sql-s	1433 *2*3	TCP	Access to SQL server
Fleet RMM application	Mail server	SMTP	25 *3	TCP	E-mail sending to mail server
Fleet RMM application	AD server	Active Directory Web Service (ADWS) Active Directory Management Gateway Service	9389	TCP	Access to AD server
Fleet RMM application	AD server	msft-gc	3268 *3	TCP	Access to AD server
Fleet RMM application	AD server	msft-gc-ssl	3269 *3	TCP	Access to AD server
Fleet RMM application	AD server	LDAP	389 *3	TCP/UDP	Access to AD server
Fleet RMM application	AD server	LDAPS	636 *3	TCP	Access to AD server
Fleet RMM application	AD server	IPsec ISAKMP	500	TCP/UDP	Access to AD server
Fleet RMM application	AD server	NAT-T	4500	UDP	Access to AD server
Fleet RMM application	Microsoft Entra ID	HTTPS	443	TCP	Acquire attribute information of users from Microsoft Entra ID. ※ This is used in case of SAML authentication.
Fleet RMM application	CA certificate server	RPC	135	TCP/UDP	Access to CA certificate server (AD CS)
Fleet RMM application	CA certificate server	SMB	445, 139	TCP/UDP	Access to CA certificate server (AD CS)
Fleet RMM application	CA certificate server	Randomly assigned TCP port	1024 - 65535	TCP	Access to CA certificate server (AD CS)
Fleet RMM Edge	MFP	HTTP	80	TCP	MFP device capacity acquisition, setting value acquisition/setting, FW update * It is recommended to use https for secure communication. Please refer to the manual of each device for the setting.
Fleet RMM Edge	MFP	HTTPS	443	TCP	MFP device capacity acquisition, setting value update, FW update
Fleet RMM Edge	MFP	SNMP v1/v3	161 *3	UDP	Acquisition of various MFP setting information
Fleet RMM Edge	MFP	OpenAPI Non-SSL/TLS:	50001	TCP	Acquisition of various MFP setting information *4
Fleet RMM Edge	MFP	OpenAPI SSL/TLS:	50003	TCP	Acquisition of various MFP setting information
Fleet RMM Edge	MFP	RAW	9100 *3	TCP	MFP (C3100i / C3120i) FW update

Source	Destination	Protocol type	Port number (Default)	Communication protocol	Intended use
Fleet RMM Edge	MFP	SNMP	161	UDP	Acquisition of various MFP (5020i / 5000i / 4020i / 4000i, 5021i / 5001i / 4221i / 4201i) status
Fleet RMM Edge	MFP	HTTPS	443	TCP	Acquisition of various MFP (5020i / 5000i / 4020i / 4000i, 5021i / 5001i / 4221i / 4201i) setting information
Fleet RMM Edge	MFP	RAW	9100	TCP	Update FW and some MFP (5020i / 5000i / 4020i / 4000i, 5021i / 5001i / 4221i / 4201i) setting
Fleet RMM Edge	MFP	SMB	139, 445	TCP	FW update * Used by bizhub 287 with Storage equipped (Function ver.4.0 and later) Updating various setting values in MFP ※5
MFP	Fleet RMM Edge	OpenAPI Non-SSL/TLS	5001 *2	TCP	Receiving various notification from MFP *4
MFP	Fleet RMM Edge	OpenAPI (SSL/TLS)	5002 *2	TCP	Receiving various notification from MFP
MFP	Fleet RMM Edge	WebDAV	443	TCP	FW Update
Fleet RMM Edge	MFP	SMB	139, 445	TCP/UDP	FW update (bizhub CXX4e and later)
Fleet RMM Edge	MFP	FTP	21	TCP	FW update (4702P series / 4422_3622, 4700P series / 4020_3320)
Fleet RMM application	NDES server	NDES	443 *3	TCP	Access to NDES (Network Device Enrollment Service) server
Fleet RMM Edge	Fleet RMM application	HTTPS	443 *3	TCP	Activation of Fleet RMM Edge, Notification of Device Information

*2. Change of Port number is available only when selecting “Custom” in Installation option.

*3. Change of Port number becomes available after installation completed.

*4. It is recommended to use SSL/TLS for secure communication. Please refer to the manual of each device for the setting.

*5. Used by C360i/C361i/C4050i/C4051i/306i series (Function ver.2.3 and later) with storage equipped.

2. Access control

In Fleet RMM, Super Admin creates users and assigns function permission. Users who are assigned function permission can operate within that range.

3. Data management

Confidential data handled by Fleet RMM (email addresses, passwords, etc.) is encrypted and managed in the SQL database and configuration files within the application.

4. Digital signature

A digital signature is added to installers and executable files of Fleet RMM. It allows the following to be performed.

(1) It is possible to operate on a PC with the setting "User Account Control: Only elevate executables that are signed and validated" enabled.
(2) Users can confirm that the software is provided by Konica Minolta and use it safely.

5. Antivirus

Fleet RMM does not have antivirus function. Please be sure to install commercially available antivirus software when using it.
Also, we recommend using the virus definition database with the setting to automatically update at a fixed time.

XVIII. Security concerning MarketPlace

< Overview >

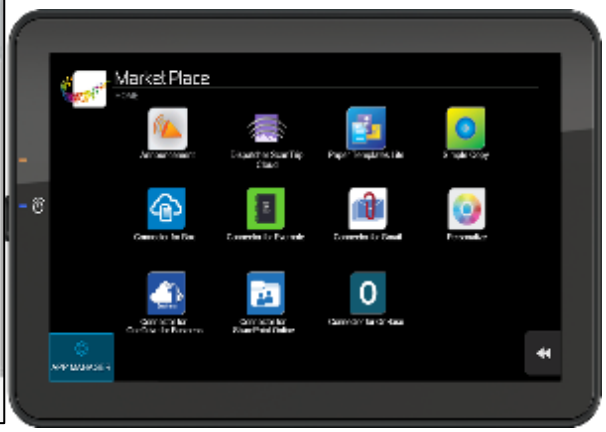
Konica Minolta MarketPlace is an innovative platform for selling software such as MFP apps, connectors, licenses, and custom MFP User Interfaces (UI). These products provide our customers with the tools they need to streamline their workflows at the MFP, and tailor their MFPs to work the way they do. MarketPlace customers can create a free account, browse through a variety of apps/connectors, purchase licenses via credit card (United States and Canada only), manage app operations, install apps and custom UIs, and much more.

Note: MFP User Interface(UI) customization features are not available to all the countries.

Customer information, business data, and payment transactions all contain highly sensitive material that must be protected from unauthorized access. Konica Minolta is committed to protecting our customers by:

- Safeguarding user data (e.g., credit card information)
- Keeping customers' browsing habits confidential
- Ensuring site integrity
- Preventing site imposters

Konica Minolta MarketPlace implements rigorous security protocols in order to inspire trust and confidence in our customers. Our policies are designed to complement the controls provided by our hosting service, Amazon Web Services (AWS). An industry leader in cloud computing, AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.



1. Cookies

Konica Minolta MarketPlace uses web cookies to store information and provide a seamless user interface for our users as they navigate around the site. The use of cookies enables users to access the features and pages within the site.

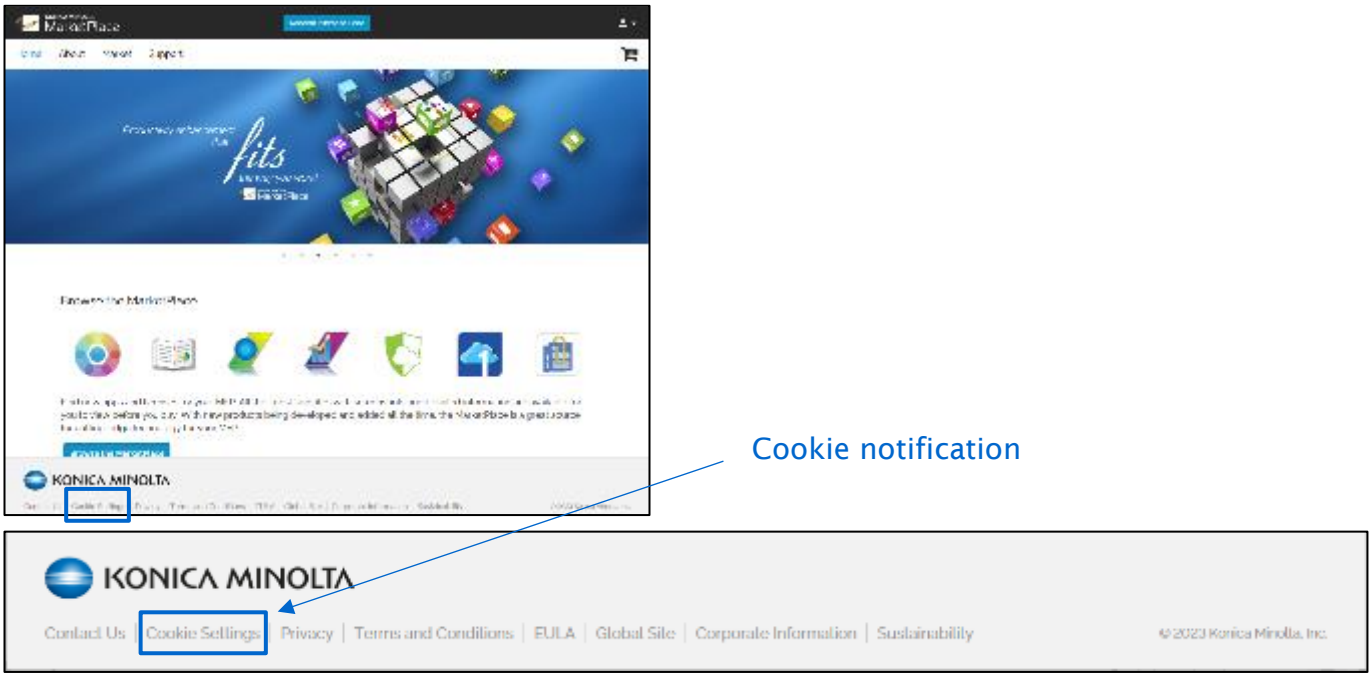
(1) Purpose

Konica Minolta MarketPlace cookies are primarily used for authentication purposes (verifying user accounts and determining when users are logged in). For example, cookies are used to keep users logged in as they navigate between MarketPlace pages, so users do not have to repeatedly log into the Konica Minolta MarketPlace site.

Important Note: Konica Minolta MarketPlace cookies are never used to store sensitive or critical information (e.g., user passwords, etc.).

(2) User Consent

As part of the European Union's e-privacy directive that requires websites to receive user consent for the use of tracking technologies, a cookie notification appears as a footer link on every page of the Konica Minolta MarketPlace site. This provides a way for users to give their consent over cookies usage. See the following illustration:



(3) Cookie Tracking

Since the Konica Minolta MarketPlace does not offer its content to any third parties, there is no special use of the "Do Not Track" feature within the Konica Minolta MarketPlace site. However, the "Do Not Track" setting can be passed through by the browser to all 3rd party websites such as Analytics Tools (Google Analytics, Matomo, etc.). By enabling the "Do Not Track" setting in the browser, users can express their preference not to be tracked across the web. Turning on "Do Not Track" through the web browser sends a signal to every website visited that the user does not want to be tracked from site to site.

2. Encryption

All Konica Minolta MarketPlace interactions are secure via Transport Layer Security (TLS), which is the most common and secure protocol used to protect the confidentiality of web transactions. Using TLS encryption ensures that no third party can covertly slip in to monitor, hijack, or shut down any transactions taking place. In addition, any insecure communication is forcefully redirected to use TLS.

(1) Public Key Cryptography

When connecting to Konica Minolta MarketPlace, the browser asks the server to authenticate itself. The authentication process uses public key cryptography to verify that a trusted independent third party has registered and identified the server. In Konica Minolta MarketPlace's public key encryption system, messages can be decrypted only with the receiver's private key, a computational impracticality.

(2) Secure Communication

TLS encrypts the data that is sent and detects any alteration in transit, so that eavesdropping on or tampering with web traffic is impossible.

(3) HTTPS Connection

The Konica Minolta MarketPlace establishes an HTTPS (Hyper Text Transfer Protocol Secure) connection, which encrypts all communication between the web server and client browser. It also secures the identification of the web server via an industry-leading certificate authority (Amazon).

(4) Proxy Support

Many businesses and organizations secure their printers from unauthorized access by limiting access to the Internet. For those customers who want to restrict their MFPs accessibility to the Internet, the MFP can be configured to have its Internet connection require a proxy. A proxy would allow a customer to lock down the MFP to only allow for outbound communication with Konica Minolta MarketPlace. Explicit firewall rules can also be specified so that the MFP only talks to Konica Minolta MarketPlace.

3. Account creation

Users must create an account on Konica Minolta MarketPlace to purchase licenses on the Web, access support material, use the MFP UI Design Tool to create custom UIs, install apps/custom UIs on MFPs, and more. To deliver these services, Konica Minolta MarketPlace collects limited user information when users create an account; This information includes email address, hash of the password, and first and last name. All handling of personal information follows Konica Minolta's Privacy Policy which can be found in the MarketPlace footer on all pages.

4. Analytics Tools

Konica Minolta MarketPlace uses third party analytics services to monitor, track, and report website traffic. These services track where website traffic is coming from, how many visitors have come to their site, where the visitors are going, and which search engines and keywords were used to find the site. Google Analytics is used in the United States and Canada. Matomo is used in Europe.

5. DDoS Protection

Konica Minolta MarketPlace is protected from DDoS (Distributed Denial of Service) attacks via its hosting service, Amazon Web Services (AWS). AWS provides DDoS attack mitigation technology called AWS Shield for all of its customers to protect from common attacks, including SYN/ACK floods, Reflection attacks, and HTTP slow reads.

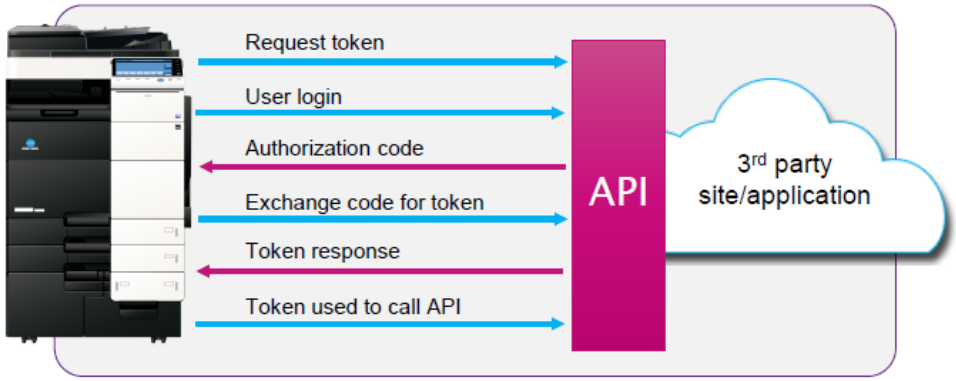
6. Konica Minolta MarketPlace Apps

(1) Storage of Personal Information / Data Encryption

Konica Minolta-developed apps honor the Konica Minolta privacy policies set up under each store. MarketPlace may share user data (first name, last name, email, and country) with Personalize, Shield Guard and ScanTrip Cloud after authenticating into these services using your MarketPlace account.

(2) OAuth Authentication

Those apps that do connect to a third-party application (e.g., bizhub Connector to Box, SharePoint Connector, etc.) use OAuth to log in as a way to access information without getting access to passwords. OAuth (Open Authorization) is a protocol that allows an application to authenticate against a server as a user without requiring passwords or any third-party server that acts as an identity provider. Instead, it uses a token generated by the server.



(3) bizhub SECURE Notifier App

A Konica Minolta MarketPlace app (bizhub SECURE Notifier) is available to provide real-time status of the MFP's security settings. With this app, you can quickly view which of these features have been enabled:

- Admin Password
- HDD Encryption
- Temporary Data Overwrite
- HDD Lock Password
- Auto Document Deleted
- Encrypted PDF Deletion
- ID + Print Deletion
- Secure Document Deletion
- Backup Schedule

KONICA MINOLTA