KONICA MINOLTA

WHITEPAPER

FUNDAMENTALS OF SECURITY

CONTENTS

CONTENTS

SECURITY WITHOUT SACRIFICE

Konica Minolta security standards

Konica Minolta realized early on the importance of security issues in the digital age, where the risk of seriously damaging security breaches rises dramatically alongside rapidly growing worldwide communication possibilities.

In response to these threats, Konica Minolta has taken a leading role in developing and implementing security-based information technology (IT) in our multifunctional products. Ever since the introduction of the first Konica Minolta MFP, Konica Minolta has striven to develop and implement technology that safeguards the confidentiality of electronic documents.

The most important security standard in the world is ISO 15408, also known as Common Criteria certification. Over the years Konica Minolta has maintained generational multifunctional bizhub/Accurio product lines that have been validated to Common Criteria security standards. Common Criteria (CC) is the only internationally recognized standard for IT security testing. Printers, copiers and software with ISO 15408 certification are security evaluated, and guarantee the security levels that company's look for today. With the CC certification users can rest assured that on Konica Minolta's multifunctional devices their confidential data remains confidential.

The Konica Minolta security standards provide protection in more than one respect, securing the network and network access, ensuring secure, authorized access to individual output devices, restricting functionalities where required, and protecting all personal user data and information content processed on the bizhub output systems.

Konica Minolta takes the security concerns of its customers seriously. This is why almost all of Konica Minolta's comprehensive security functionality is standard on the new-generation bizhub systems. After all, users should not have to pay for capabilities that are an essential requirement for protecting customers' sensitive corporate information in the digital age!

This document discusses various generally important security requirements, and explains how Konica Minolta MFPs comply with the rules and regulations set forth in ISO 15408 (Common Criteria).

Common Criteria – What Does This Stand For?

Common Criteria is an internationally recognized set of guidelines for the security of information technology products. It is primarily intended to help buyers be assured that the process of specification, implementation, and evaluation for any certified product was conducted in a thorough and standard manner. In other words, Common Criteria assures a buyer that the product they are purchasing has been independently verified to be used securely, as measured against internationally agreed specifications.

What is the purpose of Common Criteria?

Common Criteria' purpose is to allow organizations to ensure they are purchasing equipment that has been independently verified as meeting specific security requirements. It's a mandatory procurement requirement for the US federal government and for many international governments. And it's also frequently requested by non-government users that take security seriously, such as data centers, internet service providers, financial and other enterprise organizations.

What does it apply to?

Common Criteria can be applied to a variety of computer systems, including operating systems, databases, network devices, smart cards and so on. For each of these categories a protection profile is defined and specifies the type of security requirements for that class of protection profiles (PP). Each PP specifies specific security evaluation criteria to confirm the equipment's conformance to the security requirements for that family of Information System products. For the purposes of this whitepaper we will focus on Hard Copy Devices.

Why would someone buy Common Criteria products?

Common Criteria certified products have been rigorously evaluated by accredited third party security labs in accordance with internationally accepted criteria, and a government managed framework. This means buyers have a greater level of assurance that the products they buy will be fit for purpose. For example, product security functions have been independently verified and validated attesting to security functions outlined by the manufacturer. The product has been assessed for vulnerability and has passed a penetration test, the developer or manufacturers processes have been assessed, and the product meets Common Criteria procurement requirements.

What happens if a Common Criteria product changes?

Common Criteria certification only applies to the configurations and versions specified by the certified security target. So, if for example the product changes from version one to version two the certificate will not apply to that new version. However, there is a process called assurance continuity to allow minor product changes to be evaluated and subsequent product versions documented in the original common criteria set.

Where can I see a list of certified products?

Common Criteria portal is the home for information about Common Criteria and has searchable lists of certified products arranged by protection profile to help purchasers find the right product that will meet their needs.

http://www.commoncriteriaportal.org

https://www.ipa.go.jp/security/jisec/jisec_e/certified_products/certfy_list_e31.html

EAL vs Protection Profile

Evaluation Assurance Level or EAL was a numerical rating that was used to describe the depth and rigor of an evaluation. Each EAL corresponded to a package of security assurance requirements which covered the complete development of a product within a given level of strictness. There were seven EAL levels with EAL 1 being the most basic, least stringent and therefore the cheapest to implement and evaluate. Topping out at EAL 7, being more advanced, more stringent and therefore, the most expensive. In 2012 NIAP (National Information Assurance Partnership), the US organization responsible for implementing Common Criteria, decided to change the evaluation methodology. The problem with the EAL system was that similar products can have different levels within the same protection profile, which makes product comparisons very difficult for purchases. The revised system removes the EAL rated profiles, and instead products have to simply be compliant with the new protection profiles. This ensures security requirements are achievable, repeatable and testable. Ensuring that product comparisons are therefore easier understood and more reliable.

So when making purchasing decisions, buyers can now look for products that are PP compliant, as well as the protection profile that matches their business activity or requirements, rather than trying to understand the meaning of the EAL numbering scheme.

Enhancement of Security Level of MFPs

Recently, an increasing number of IT and information system users are suffering losses and damage caused by problems such as unauthorized access, virus infection, Brute Force Attacks and information leakage, highlighting the importance of taking stronger security measures for MFPs.

Konica Minolta has constantly strengthened measures against security risks by incorporating the latest security functions into its MFPs so that customers can use its products without fear of security threats. To be specific, all Konica Minolta MFPs offer the following capabilities: restricting the use of network protocols; preventing unauthorized access via networks through IP filtering; managing the use of MFPs through user authentication; and encrypting communication data and HDs. Hard Copy Device –Protection Profiles (HCD-PP) requires that the effectiveness of the encryption algorithm for data security and the ability of MFPs to prevent modification of firmware be verified using a real machine.

By meeting these requirements, a manufacturer can objectively guarantee that its MFPs can successfully manage security risks, e.g., preventing document data stored in a leased MFP from being leaked after it is returned to the lessor or disposed of, and protecting against unauthorized modification of firmware.

Konica Minolta has put priority on obtaining third-party certifications, and recognizes the effectiveness of using the latest evaluation criteria to enhance the security features of its products. Thus, Konica Minolta is determined to make its products compliant with HCD-PP.

HCD-PP was developed as security requirements that must be met for the Japanese and U.S. governments when procuring MFPs, under the leadership of the Information-technology Promotion Agency, Japan (IPA), a Japanese certification body, and the National Information Assurance Partnership (NIAP), the U.S. government's IT security certification body, in cooperation with MFP manufacturers and evaluation organizations. Since 2017, HCD-PP has been listed as a certified protection profile (security requirement specifications) on the official website of the Common Criteria Recognition Arrangement (CCRA), an international mutual recognition framework for ISO/IEC 15408. Accordingly, the abovementioned nine HCD-PP-compliant products are recognized as being capable of providing sufficient protection against security threats in 30 CCRA member countries, mainly the U.S. and European countries.

Conclusion

While the Common Criteria certification does not actually "guarantee" the security of a device, it shows that the manufacturer's specifications relating to the security functionality of the evaluated product were independently verified. In other words, a system certification to a Common Criteria standard confirms that the process of specification, implementation, and evaluation has been conducted in a rigorous and standard manner indicating that the manufacturer has taken every measure to provide a highly secure device.

What is GDPR? - in a nutshell

The European Union's General Data Protection Regulation or GDPR is an EU data privacy law that went into effect May 25, 2018. It is designed to give individuals more control over how their data are collected, used, and protected online. It also binds organizations to strict new rules about using and securing the personal data they collect from people, including the mandatory use of technical safeguards like encryption and higher legal thresholds to justify data collection. Organizations that don't comply will face heavy penalties of up to 4 percent of their global annual revenue or €20 million, whichever is higher.

GDPR is peculiar in the fact that it applies to organizations that may have little to do with the EU. For example, you may be a US web development company based in Denver, Colorado, selling websites mainly to Colorado businesses. But if you track and analyze EU visitors to your company's website, then you may be subject to the provisions of the GDPR. The whole point of the GDPR is to protect data belonging to EU citizens and residents. The law, therefore, applies to organizations that handle such data whether they are EU-based organizations or not, known as "extra-territorial effect."

The GDPR spells out the territorial scope of the law:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    b. the monitoring of their behavior as far as their behavior takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 3.1 states that the GDPR applies to organizations that are based in the EU even if the data are being stored or used outside of the EU. Article 3.2 goes even further and applies the law to organizations that are not in the EU if two conditions are met: the organization offers goods or services to people in the EU, or the organization monitors their online behavior. (Article 3.3 refers to more unusual scenarios, such as in EU embassies.)

When does the GDPR apply outside Europe?

As we just mentioned, there are two scenarios in which a non-EU organization might have to comply with the GDPR. Let's take a closer look at each of these.

Offering goods or services

The Internet makes goods and services in far-flung places accessible anywhere in the world. A teenager in Cyprus could easily order a pizza online from a local pizza shop in Miami and have it delivered to a friend's house there. But the GDPR does not apply to occasional instances. Rather, regulators look for other clues to determine whether the organization set out to offer goods and services to people in the EU. To do so, they'll look for things like whether, for example, a Canadian company created ads in German or included pricing in euros on its website. In other words, if your company is not in the EU but you cater to EU customers, then you should strive to be GDPR compliant.

Monitoring their behavior

If your organization uses web tools that allow you to track cookies or the IP addresses of people who visit your website from EU countries, then you fall under the scope of the GDPR. Practically speaking, it's unclear how strictly this provision will be interpreted or how brazenly it will be enforced. Suppose you run a golf course in Manitoba focused exclusively on your local area, but sometimes people in France stumble across your site. Would you find yourself in the crosshairs of European regulators? It's not likely. But technically you could be held accountable for tracking these data.

Exceptions to the rule

There are two important exceptions we should note here. First, the GDPR does not apply to "purely personal or household activity." So if you've collected email addresses to organize a picnic with friends from work, rest assured you will not have to encrypt their contact info to comply with the GDPR (though you might want to anyway!). The GDPR only applies to organizations engaged in "professional or commercial activity." So, if you're collecting email addresses from friends to fund a side business project, then the GDPR may apply to you.

The second exception is for organizations with fewer than 250 employees. Small- and medium-sized enterprises (SMEs) are not totally exempt from the GDPR, but the regulation does free them from record-keeping obligations in most cases (see Article 30.5).

CAUSE FOR CONCERN EVERYWHERE – SECURITY VULNERABILITY

Generally MFPs offer a huge range of combined operations and many ways to execute these operations; therefore they represent a similarly wide range of potential security loopholes if the proper safeguards are not put in place to protect your data and your MFP. The scope of MFP security could be grouped into three main sections:

Access control / Access security

Despite security being high on the agenda in both public and corporate domains, MFPs are often ignored as being a security risk at all. While some risks are perhaps identified, they are often simply neglected, especially where sensitive documents and information is concerned. This is especially risky for those MFPs and printers located in public areas, where they can be accessed by staff, contractors and even visitors.

Because the advanced features available on today's MFPs deliberately make it easy for information to be copied and distributed within and beyond actual and virtual corporate boundaries, the first logical step is to prevent unauthorized persons being able to operate an MFP. Preventive measures are needed, firstly to control access to MFPs, and secondly to establish some kind of security policy reflecting how the devices are actually used in real life. Obviously, none of these measures should restrict or limit the user-friendliness of the systems. Konica Minolta is prepared for this, offering various security features and solutions.

Document security / Data security

Reflecting the fact that MFPs and printers are often located in public areas, where they can be easily accessed by staff, contractors and visitors, it is necessary to implement appropriate data security policies. The situation is after all that confidential data, for example stored on the MFP storage media over a period of time, or simply confidential documents lying in the MFP output tray as printouts, are initially unprotected and could fall into the wrong hands. Konica Minolta offers a range of tailored security measures to ensure document and data security.

Network security

In today's corporate environment, indeed in today's business world, communications and connectivity are indispensable. Konica Minolta offers devices that are designed to integrate into network environments. For example network printers and multi-functional peripherals (MFP) have evolved to the point that they act as sophisticated document processing hubs integral within the network, with the ability to print, copy and scan documents and data to network destinations, send emails and more. This scenario also means that this office technology must cope with and comply with the same security risks and policies as any other network device, and represents a risk if unprotected. In order to avoid any vulnerability from either internal or external network attacks, Konica Minolta ensures that all equipment complies with the strictest security standards. This is achieved using a number of measures.

WITH ITS COMPREHENSIVE RANGE OF SECURITY FEATURES, KONICA MINOLTA PROVIDES PROFESSIONAL SOLUTIONS FOR THE DETECTION AND PREVENTION OF SECURITY BREACHES.

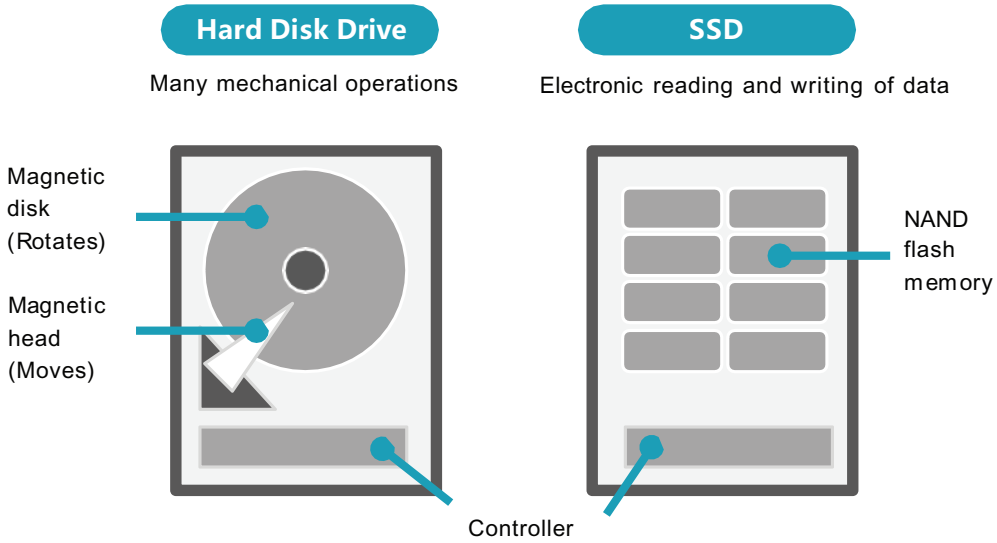
GENERAL SYSTEM SECURITY

Adoption of High Speed Solid State Drive for Storage

Konica Minolta has adopted High Speed Solid State Drive (SSD) technology for storage starting with our bizhub i Series product line as well as our C12000/C14000 and later Production Print product line. When comparing SSD technology to the older HDD technology, the HDD technology stores data as magnetic information on the hard disk drive. This means depending on the magnetic orientation of each cell, the data bit is either a 0 or 1. While overwriting (or clearing) the cells, in this manner, there is no guarantee that all of the cells will react to the magnetic field in the same way. Therefore, it might be possible that some remaining magnetic traces/variations of data could be left behind on the HDD which in turn, could be used to restore the data. This is where the different overwrite modes become effective. By running the magnetic orientation or overwrite patterns multiple times, any remaining traces/variations of data will be neutralized.

With an SSD, it's completely different. Based on the technology used inside an SSD, there is no potential of magnetic traces/variations being left behind as in a common HDD. An SSD is basically built of NAND Flash memories. NAND Flash memory contains "floating gate – field – effect transistors" as memory cells. This Flash memory works by adding (charging) or removing (discharging) electrons to and from a floating gate. When the electrons are present on a floating gate, the current is unable to flow through the transistor, rendering the bit state at level 0 (zero). This is considered the normal state for a floating gate transistor when a bit is programmed.

FUNCTIONS	BENEFITS
Quick data read/write operations	Improved system response speed
Able to withstand powerful vibrations	Improved shock resistance
Few mechanical operations	Improved shock resistance and noise reduction



SECURITY CONCERNING MFP SELF-PROTECTION

Firmware verification feature

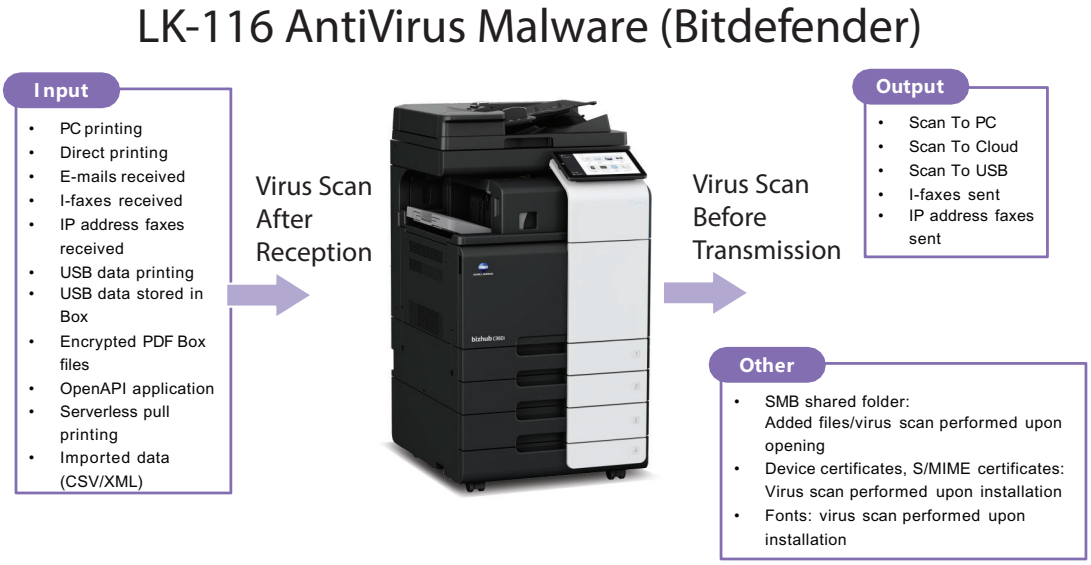
When rewriting the main MFP unit's firmware, a hash value check is run to check if the firmware data was tampered with. If the hash values don't match, an alert is issued, and the firmware is not rewritten. In addition, if enhanced security mode is used, hash value checks are performed when the main 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.

Anti-Virus/Malware Protection by Bitdefender® - Real Time Scanning

In today's network environments, a significant security risk, which is often completely underestimated, is document and information processing via the multifunctional device (MFP). Virtually every manufacturer of printing devices offers a variety of security features for their MFPs. Most competitors in the market use whitelisting as the highest security level for MFPs. The whitelist functionality often suggests a partnership with an anti-virus provider, which, however, is usually not technically implemented on the device but resides within a server on the network.

Konica Minolta has introduced a premier Anti-Virus/Malware protection solution by Bitdefender® starting with the bizhub i-Series MFP's and later. In cooperation with Bitdefender®, Konica Minolta's virus scanning solution is unique in the market, This solution is on-board middleware designed to protect every level of the MFP offering comprehensive protection for the bizhub MFP(s), thanks to:

- **Real-time scanning: Always monitoring all inbound, output data and any data residing within the MFP.**
- **Periodic scanning: Performs virus scan on the specified date or whenever required.**
- **Scan history display: Allows you to view the detected virus history and the performed virus scan history.**
- **Risk log (detected virus history): Contains details such as error codes, time, and risk details.**
- **Scan log (performed scan history): Contains the scan start/end time, and the scan results (good or bad).**
- **Checking for updates to the pattern file: When launched, it automatically checks for updates to the pattern file every four hours.**
- **This reduces security risks such as information leakage due to virus infection.**



PROCESS AFTER VIRUS DETECTION

When a virus is detected, the file is automatically dealt with.

PROCESS	TARGET
Deletion	Scan To PC, Scan To Cloud, Scan To USB, I-faxes sent, IP address fax sent, SMB shared folder, imported data, OpenAP IP address fax sent, SMB shared folder, imported data, OpenAPI application, device certificates, S/MIME certificates, font data
Printing	PC printing (normal printing), emails received (normal printing), USB data printing, direct printing
Box storage	PC printing (saved Box data), emails received (saved Box data), I-faxes received, IP address fax received, USB To Box, encrypted
*Entry to the warning log only. Browsing data, files downloaded with a browser, IWS application	

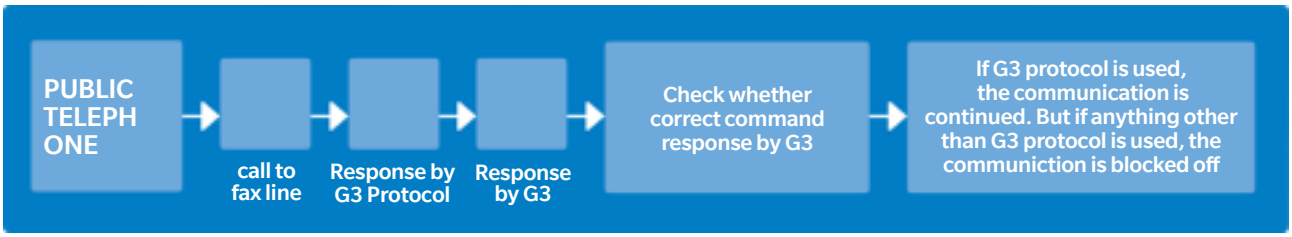
Protection against virus from USB memory

Most of the Konica Minolta devices are equipped with an interface for USB memory sticks. This offers the possibility to print documents directly from the USB memory without a PC. It is also possible to scan documents directly to the USB memory.

Generally, virus infection from USB memory is caused by program files automatically executing when the USB memory is inserted in the device. Konica Minolta devices do not support functionality to automatically execute files by inserting the USB memory. Therefore, Konica Minolta devices are not affected by these types of viruses.

Security for fax line

Konica Minolta has maintained a FAX Separation Function in our fax options for more than ten years and counting. The separation of FAX Public Line and the Network has been included in our Target Of Evaluation for Common Criteria (ISO15408) testing. These Independent Testers have certified that "The FAX Separation Function prevents the fax I/F to be used as a network bridge between PSTN and the Network". Any communication via fax line uses only fax protocol and does not support any other communication protocol. If someone from outside the network attempts to intrude with a different protocol via a public line, or tries to send data that cannot be decompressed as fax data, Konica Minolta products handle the event as an error and block such communication.



Security of RAM

Data theft is the leading concern by end-users, corporations/business' and manufacturers alike. One particular fear is that critical data can be stolen from the MFP Solid State Drive or SSD or RAM, either by accessing the MFP or removing the SSD or RAM and extracting the data after the MFP has been discarded. These concerns have been addressed for each technology, SSD and RAM in the remainder of this statement.

RAM Security

Random Access Memory, there is a RAM currently being used by MFP's:

- Volatile RAM

Volatile_RAM

Typically Volatile RAM would be

- File Memory – electronic sorting
- Work Memory – storing program parameters, temporary data and image conversion of controller
- Fax Memory – working RAM for fax

Data that is written to Volatile RAM is held while the power is 'ON'. The data held in this type of RAM is overwritten by the next page or job being printed. Once the job is printed the data is deleted from RAM. Also, if the power is turned 'OFF' the data in Volatile RAM is deleted.

Volatile RAM is secure, if RAM is removed after an engine is powered OFF all the data on that RAM module would have already been deleted. It would be impossible to remove the RAM while the engine power is ON. The only other way to possibly extract data would be an indirect route or a security hole. These access points have been evaluated and tested by 3rd party security consultants before the KMBS products were sent for ISO 15408 certification. There are no indirect routes or security holes.

SPI-Flash memory

Typically SPI-Flash memory would be

- OS (Operation System) data management
- Data required to start the system, such as device information
- Information on machine total counter (for backup)

SPI-Flash memory stores data that manages the behavior of the MFP system. It is on-board memory within the MFP; it structurally cannot be removed from the circuit board.

Non-volatile RAM (NV-RAM) (Found in models prior to the bizhub i-series)

Typically non-volatile RAM would be:

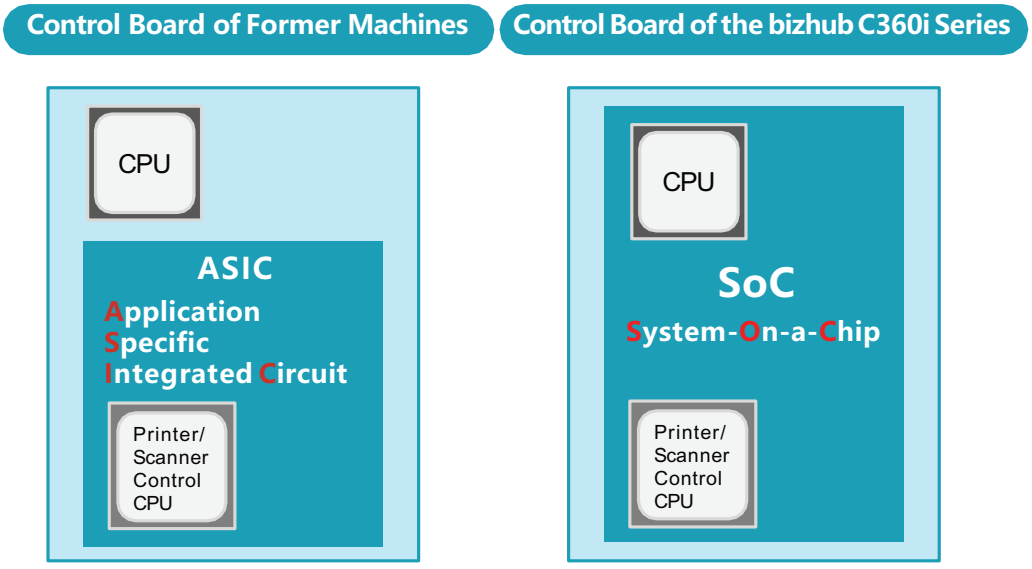
- counter data
- job settings
- utility settings

Adoption of an SoC (System on a Chip)

Introduced with the ip-series MFP's the SoC (System-On-a-Chip), integrates the CPU and the multiple modules needed for system control in a single chip. The processing power in system control, compression and expansion of image data, and the input/output of image data is improved by the integration of multiple modules and the CPU in a single chip. The recovery time from start-up time and power saving mode has been reduced as well.

Benefits of an SoC (System-On-a-Chip):

- In general, an SoC has the following benefitsMiniaturization:
- Miniaturization is achieved as the mounting of multiple modules is not required to be separate, saving a lot of connector spaces.
- Speeding up: Speeds up processes by reducing the time lag of signals between modules.
- Low power consumption: Lowers power consumption by reducing the number of connection terminals between modules.
- Low cost: The cost of the whole product is reduced by the miniaturized board, simplified tests, and reduced number of breakdowns.



FUNCTIONS	BENEFITS
Quick data read/write operations	Improved system response speed
Able to withstand powerful vibrations	Improved shock resistance
Few mechanical operations	Improved shock resistance and noise reduction

Password handling

According to certain Password Rules, registration of a password consisting of a string of a single character or change of a password to one consisting of a string of a single character is rejected for the Administrator Password, User Password, Account Password, User Box Password, Secure Print Password, SNMP Password, WebDAV Server Password, and Encryption Key. For the Administrator Password, User Password, Account Password, User Box Password, SNMP Password, WebDAV Server Password, and Encryption Key, the same password as that currently set is not accepted.

Study the following table for more details of the number of digits and characters that can be used for each password.

TYPES OF PASSWORDS	NO. OF DIGITS	CHARACTERS
• User Password • Administrator Password • Memory RX User Box Password	8-64 characters	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + • Characters with umlaut (95 characters) • Selectable from among a total of 188 characters
Encryption Key	20 digits	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', *, +, -, ., /, =, ?, @, ^, _, `, {, |, }, ~ • Selectable from among a total of 83 characters
Confidential RX Password	8 digits or more	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, #, $, %, &, ', (,), *, ,, -, ., /, :, ;, <, =, >, ?, @, [, \,], ^, _, `, {, |, }, ~, + • Selectable from among a total of 93 characters
• Account Password • User Box Password • Secure Print Password	8 digits or more	• Numeric characters: 0 to 9 • Alpha characters: upper and lower case letters • Symbols: !, $, %, &, (,), *, ,, -, ., /, :, ;, <, =, >, ?, @,[,], ^, _, `, {, |, }, ~, + • Selectable from among a total of 90 characters
WebDAV Server Password		The password rules are not applicable
Encrypted PDF Password		Password is set when PDF documents is created

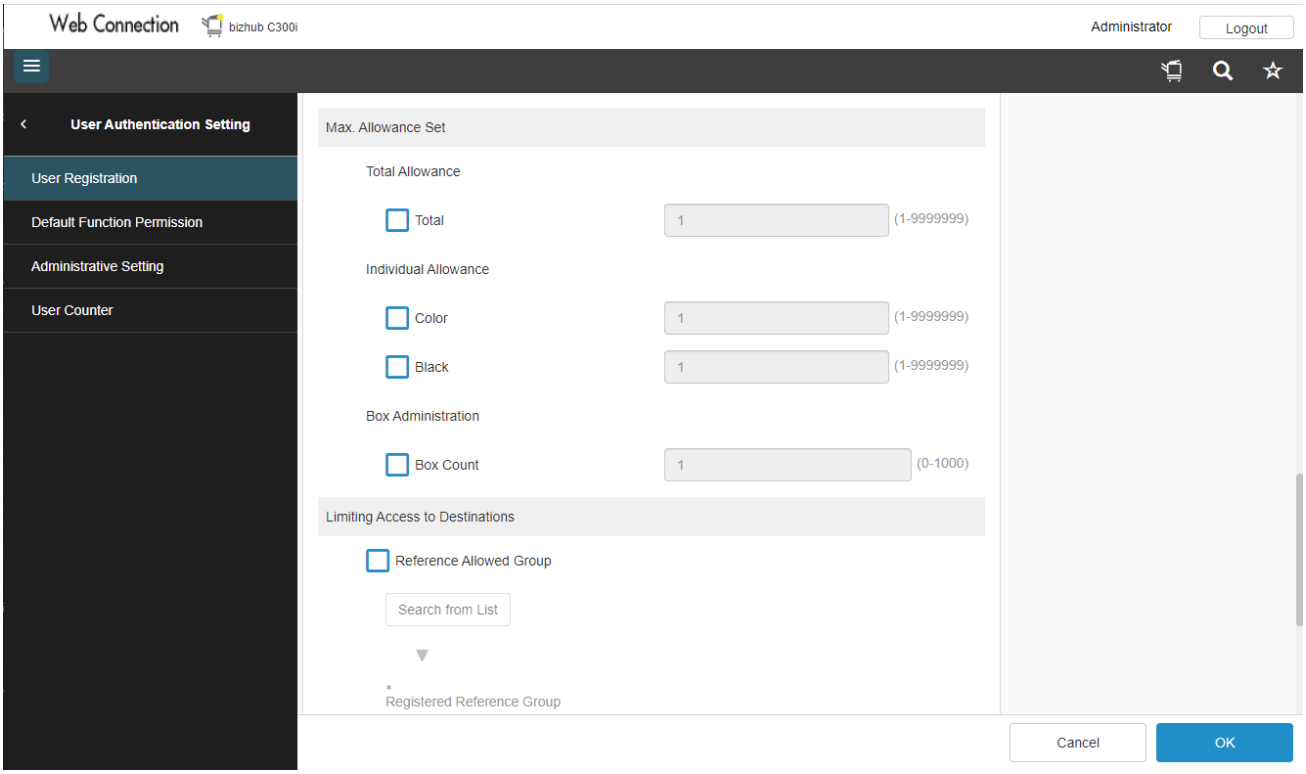
Precautions for Use of Umlaut

- The maximum number of digits allowed for the User Password is 64, if umlaut is used with all characters, however, the maximum number of digits allowed becomes 32 digits.
- Setting or entering an umlaut from the control panel may be disabled depending on the setting made in this machine, but not on the client PC side including Web Connection. If an umlaut is set in a password on the PC side, therefore, the umlaut cannot be entered from the control panel, which means that this particular password is not usable.

ACCESS CONTROL

Copy/print accounting

Konica Minolta bizhub MFPs come with the ability to enable account tracking as standard. When this function is activated, a user is required to enter a 4–8 digit personal identification number (PIN) to gain access to make a copy, send a print, or perform other functions at the MFP. If a user does not submit or enter an authorized PIN (from the print driver), the print job submitted will not be printed. If a user does not enter an authorized PIN at the copier control panel, they will be denied access to the system. When logged in, the user's activities are electronically recorded onto a log file inside the system. An administrator- tor or key operator can access this file. This is a very popular feature for many customers, who use this to invoice departments and audit employees' copier activities. In addition, it is possible to configure individual copy and print limits per user.



This is an example of the accounting screen from the Konica Minolta bizhub control panel.

Network User authentication - ID and Password

Network

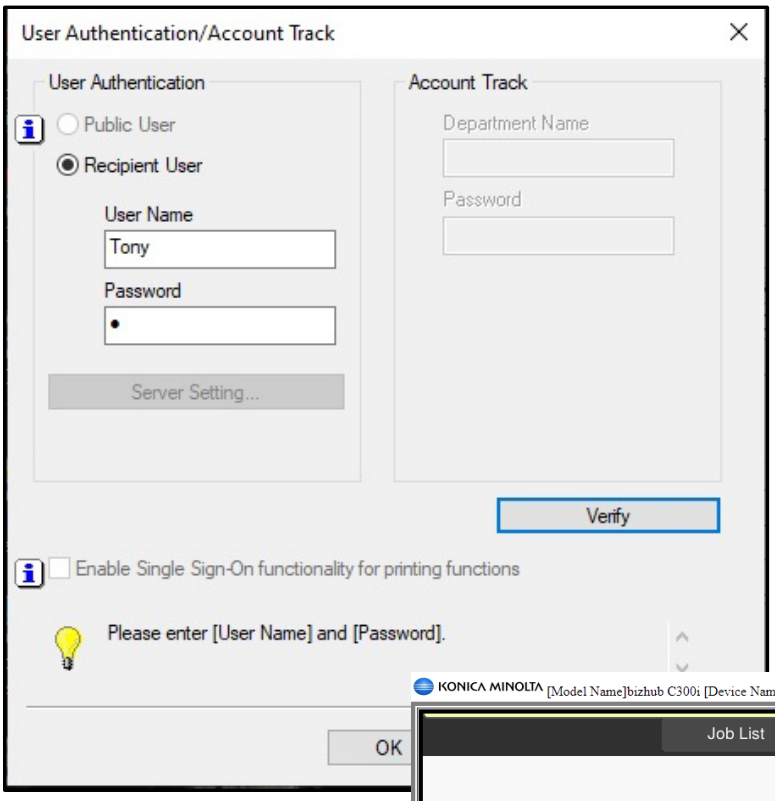
Konica Minolta devices support external servers like Active Directory, LDAP, etc. with a maximum password of 64 characters that can be utilized. Active Directory can support up to 20 domains. In addition, authentication can be centrally managed via Dispatcher Phoenix Pro or Dispatcher Paragon as well as other 3rd party solutions.

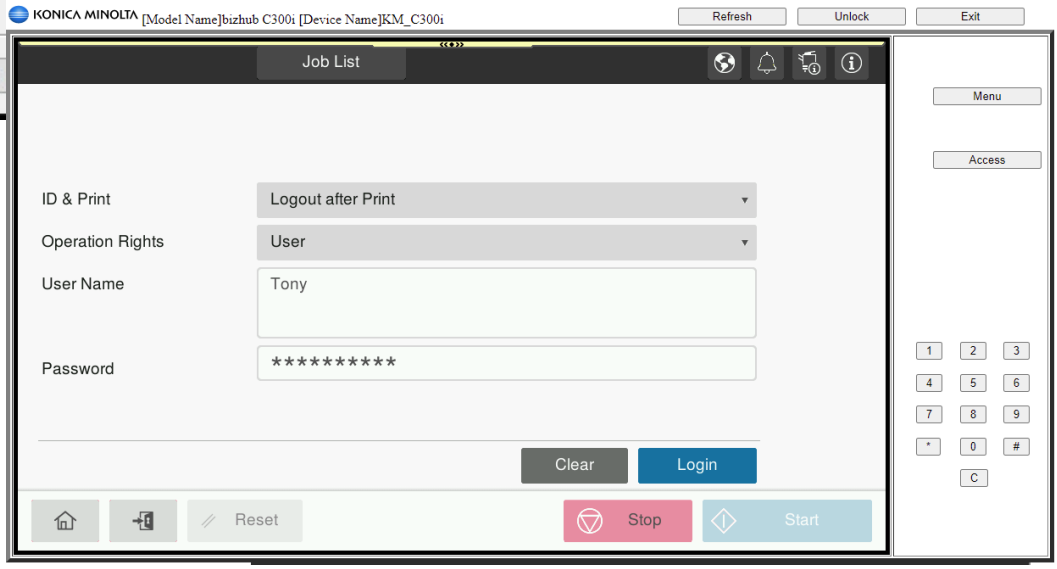
Machine

Internal authentication at the machine can support up to 1,000 user accounts. Passwords can have up to eight alphanumeric characters.

Password protection

Passwords can be created for administrators and users, and can be alphanumeric with up to eight characters. An administrator can maintain passwords. Passwords are protected by the Kerberos system or SSL.





These are examples of the authentication screen from the Konica Minolta bizhub control panel and printer driver.

User authentication – Multi-Technology Card Readers

Konica Minolta' authentication solutions are evolving based on the security demands of the IT professionals to keep their networks and data secure. Konica Minolta MFPs can be equipped with an AU-205H, a Multi-Technology IC card reader compatible with multiple Non- Contact IC Card formats or HID Mobile Access from an iPhone or Android device using Bluetooth Low Energy (BLE) technology. Using the unique code provided by these technologies user authentication can be achieved across the network via Active Directory, using access applications such as Dispatcher® Paragon and other industry leading print management applications with single sign-on to advanced scan workflow applications such as Dispatcher Phoenix and other advanced scan workflow applications or locally authentication at the MFP directly.

The AU-205H reader features:

- DUAL FREQUENCY: Simultaneously supports low (125 kHz) and high-frequency (13.5 MHz) card access credentials.
- SUPPORTS MOBILE ACCESS: Bluetooth interface leverages HID Global's Mobile Credentials to access MFPs, computers, network and Cloud data, as well as secure print release.
- SUPPORTS SEOS AND ICLASS SE PLATFORM: Provides multilayered security that extends beyond the card technology, offering additional protection to identity data. Easy-to-use, straightforward utilization of existing access control credentials for PC login in both CCID and keyboard wedge operation modes.
- KEYBOARD WEDGE EMULATION: Retrieves data from a card and presents the information directly to any application by emulating keyboard strokes.
- SECURITY AND CONVENIENCE ALL IN ONE: It's reported that 60% of companies have lost data due to a printer security breach, costing an average of $400K to address.* But a complex user authorization process can impact user productivity. Today, mobile devices are commonly used to access systems. But typing in complex passwords on a touchscreen can also prove challenging. The AU-205H card reader bridges the gap between high security and convenience.
- HELPS COMPLY WITH REGULATIONS: Maintaining strict compliance with regulations is essential in certain industries. The AU-205H card reader provides secure access to print, scan, copy and fax devices in government, healthcare (HIPAA), legal and education (FERPA).
- ID AND PRINT: How often are jobs printed and then sit at the MFP waiting for the user to pick it up? This feature allows you to hold print jobs at the MFP until the user presents their IC card. This prevents any compromise in security with print jobs containing confidential information sitting in output trays.
- SECURE PULL PRINT: Send print jobs to any printer and hold it in a secure queue until you're ready to pick it up. Simply present the IC card, iPhone or Android device at any compatible MFP on the network to release your print job.
- INTEGRATION: Monitoring and tracking who's accessing your system, and what they're accessing is also vital to your business. The AU-205H card reader integrates with authentication and accounting solutions provided by Konica Minolta so you know who did what by simply accessing information on the card. External Print Management software is highly recommended providing Centralized management of users and their credential's, synchronizing with existing Windows Active Directory to secure user access and Restrict unauthorized access.

- SECURE PRINT RELEASE FROM SINGLE-FUNCTION PRINTERS: Select tabletop single-function printers now support card readers with authentication to secure pull print applications such as Dispatcher Paragon, PaperCut and Equitrac.
- CONTROLLED ACCESS: The AU-205H card reader does more than secure access. It makes it easy to reduce unauthorized operation and minimize unnecessary printing. That's key to saving paper and energy, supporting both public and private sustainability goals.
- MOBILE ENABLED READER FEATURES: The AU-205H card reader allows for adjustable read settings, overall power control and reading a range of mobile IDs. It enables flexibility for both close-proximity "tap" and long-range "twist-and-go" distances, with a directional antenna providing long-range reading up to 2m. Read settings can also be administered using your mobile phone during installation.

User authentication – Government Certified Authentication System

Common Access Card (CAC), Personal Identification Verification (PIV) Card & SIPRNET Authentication

The US Government issued the Homeland Security Presidential Directive (HSPD-12) in August 2004. It called for a mandatory government-wide standard for secure and reliable two-factor identification for all US Government employees to control access to federally-controlled facilities and networks Requirements that flow from this and other government initiatives mandate that MFPs sold to the government be capable of reading cards issued to government employees known as Common Access Cards (CAC) and other Government agencies which have been issued Personal Identification Verification (PIV) cards. These cards, in combination with a personal identification number, satisfy the two factor requirement. In addition, MFPs sold to US Government customers must also be capable of Public Key Infrastructure (PKI) encryption that meets government standards.

FEATURES

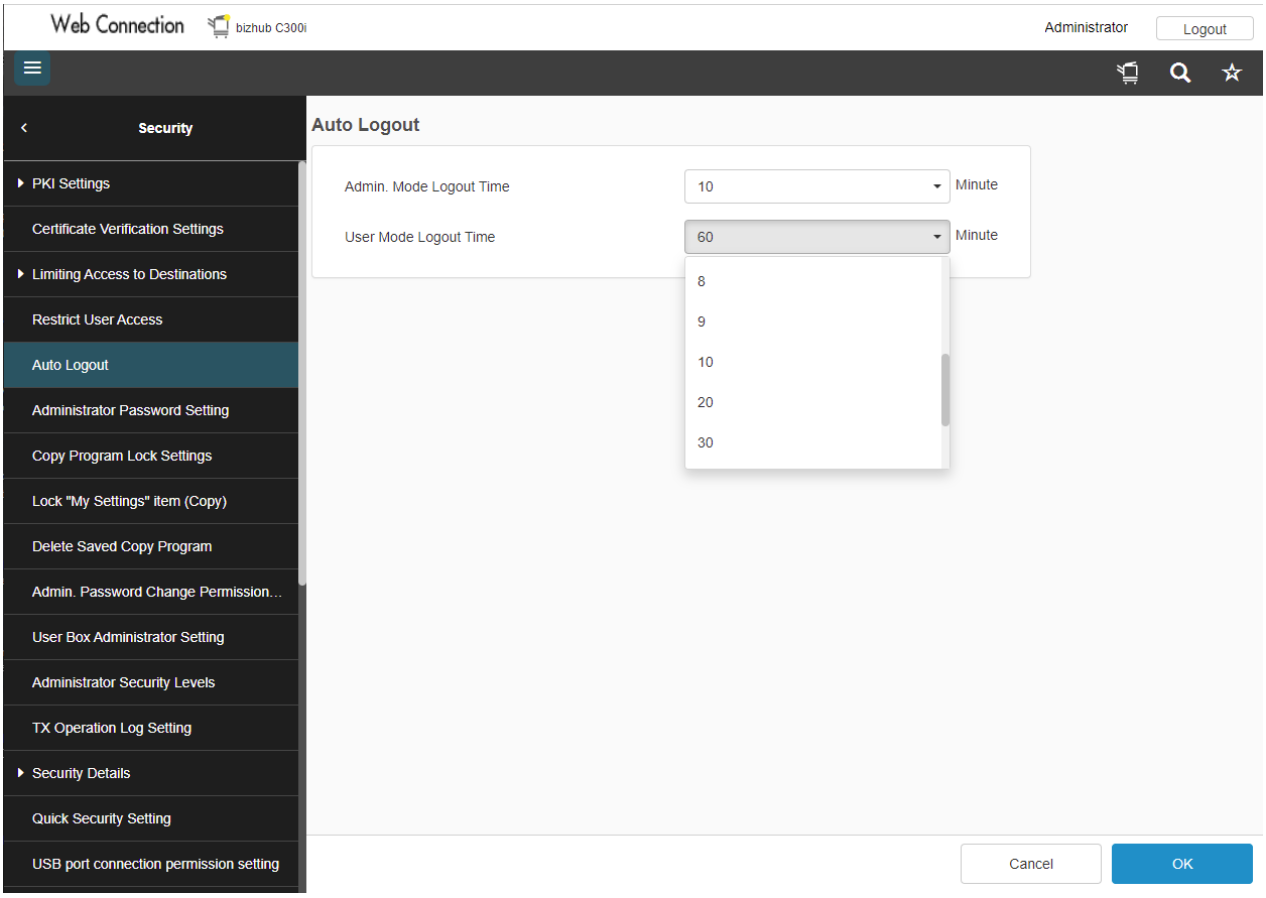
- Meets major standards, including ISO 7816, EMVCo Terminal 1, Microsoft WHQL, USB CCID, PC / SC and HBCI (Home Banking Computer Interface)
- Usage within an application is based on standardized interfaces like PC / SC
- USB CCID support makes integration into an existing system the easiest ever by connecting host and smart card reader without the need for additional drivers
- Attractive, small size fits in an envelope to distribute with smart card, credit card, e-ID card or software for online banking or digital signature applications
- All major operating systems supported
- Meets GSA FIPS 201 requirements
- Supports high-speed data transmission
- UPC barcode for easier logistics

SUPPORTED CARD TYPES INCLUDE:

- CAC v1
- CAC v2
- GSCIS
- PIV Transitional
- PIV End-state (FIPS 201, FIPS 201-1 and FIPS 201-2)
- PIV-Interoperable (PIV-I)
- Commercial Identity Verification (CIV)
- SIPR Cards
- SC650 v1.0 - SC650 v4.2
- G&D SmartCafe Expert 144k FIPS-201 v3.2
- G&D SmartCafe Expert 7.0 FIPS

Auto log off

Konica Minolta MFPs can be programmed to automatically reset to a state that requires password input after a predetermined time of inactivity. This ensures that the MFP will reset to a secure state if a user forgets to log off from an MFP when finished. Note that the reset timer can be set from 1 to 60 minutes – the factory default is 1 minute. Some Konica Minolta MFPs can be programmed to reset in as little as 30 seconds. If the machine has the account tracking function enabled it will enter a state (after a pre-programmed period of inactivity) that requires a user to enter a unique PIN or password. This function should satisfy most concerns about users forgetting to log off after they have finished scanning or copying documents at the MFP.



This screen illustrates the administrator and user auto log-off timer setting that is accessible via the MFP's remote Web browser-based interface (Web Connection).

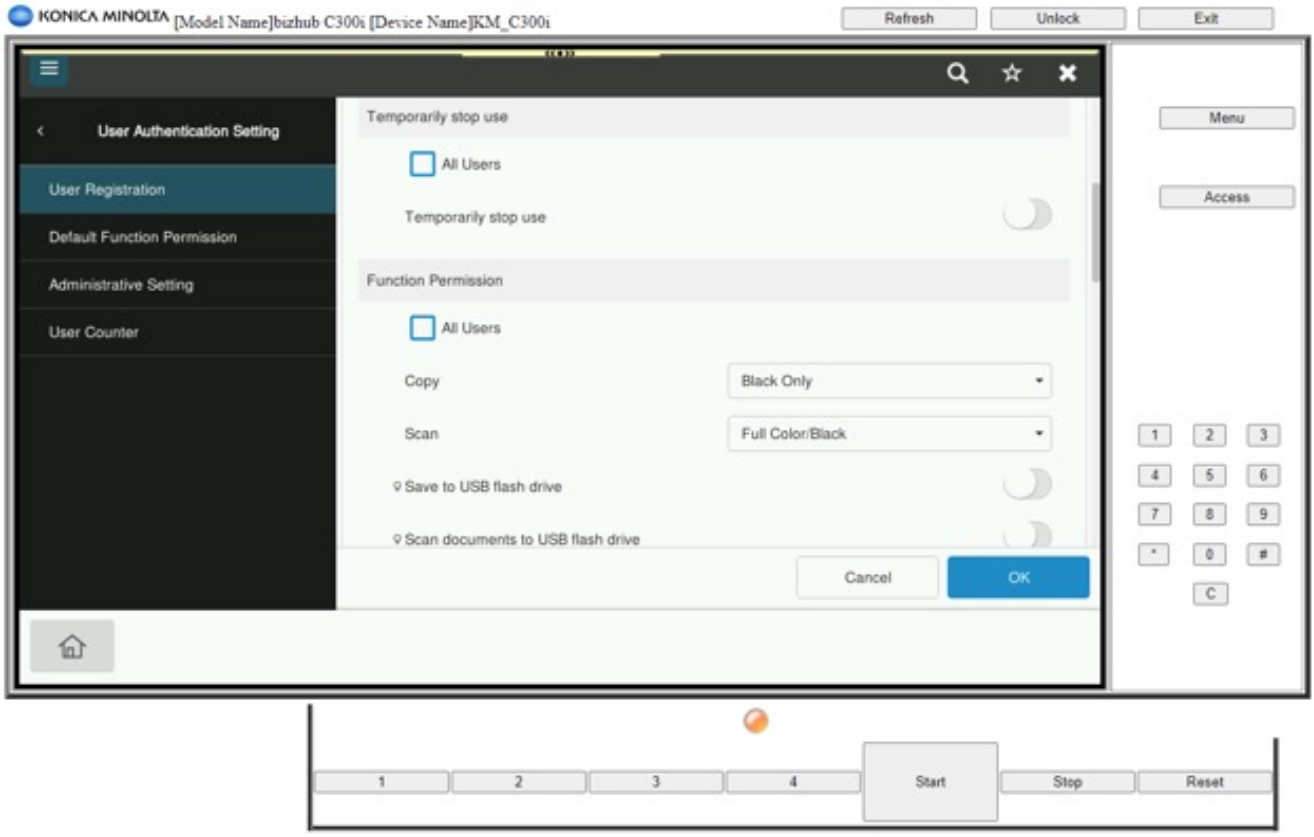
Function restrictions

An advanced level of user security allows or prohibits the use and availability of specific machine features. A user and/or administrator can control these features as needed throughout an organization of any size.

The specific features are:

- scanning from the bizhub as a walk-up function or a remote function
- user box from the bizhub as a walk-up function or a remote function
- copying from the bizhub as a walk-up function, including the restrictions of only b/w copying or only color copying or neither b/w nor color copying
- faxing from the bizhub as a walk-up function or a remote function
- printing as a remote function via the printer driver, including the restrictions of only b/w printing or only color printing or neither b/w nor color printing

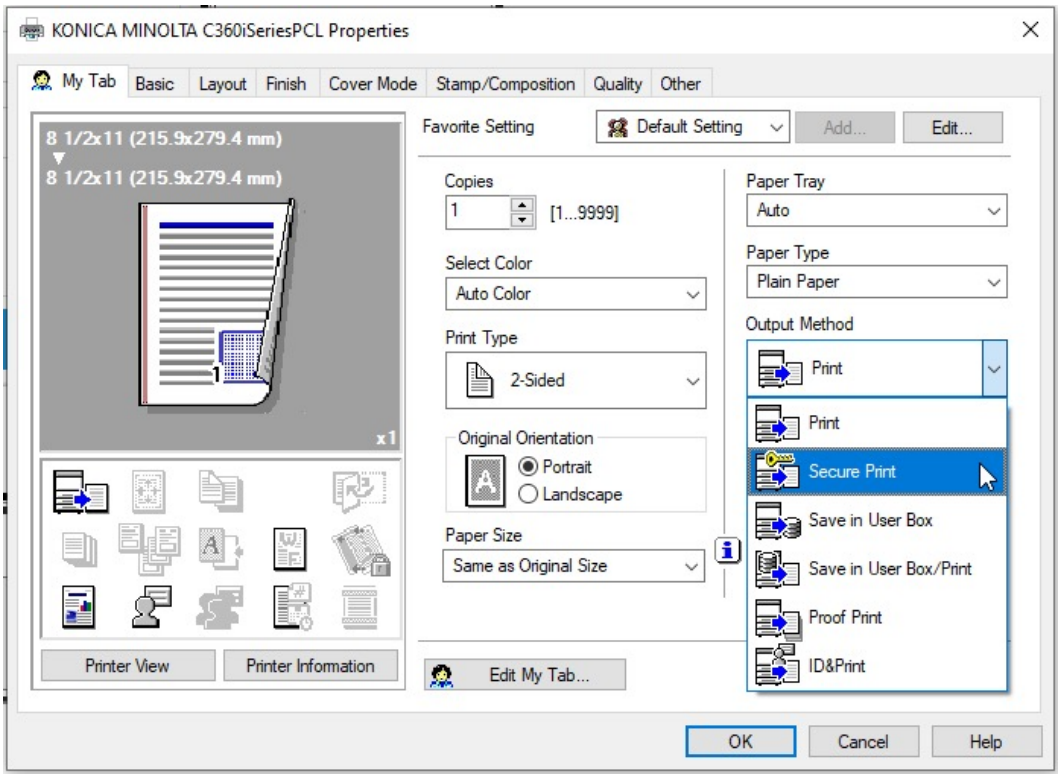
Function restrictions can be set in general either as a walk-up functionality or per user, depending on the user authentication.

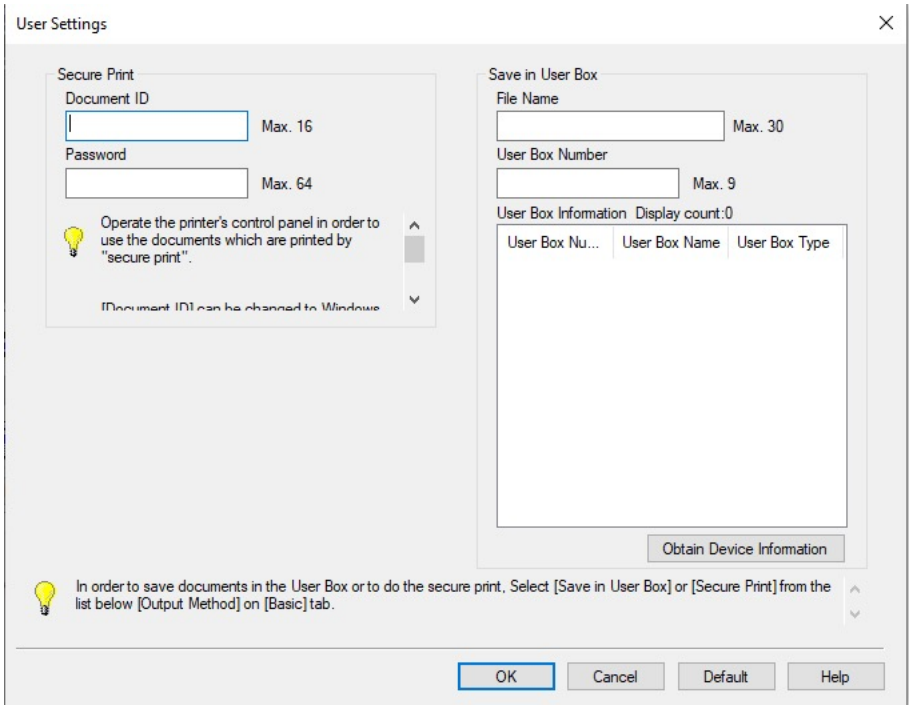


This is an example of the function permission screen from the Konica Minolta bizhub control panel.

Secure Print

Konica Minolta MFPs offer a standard feature called secure printing. This security function is native and embedded inside the bizhub MFP. The feature provides a user sending a print job with the ability to hold the job in the memory of the system until the authorized user walks up to the machine and releases the job by entering a unique secure Print ID and Password at the control panel of the MFP. This code is first specified by the user when he submits his print job from the PC workstation, ensuring that only the sender of the job can access an electronic document that contains sensitive electronic information. In addition, those MFPs equipped with a hard drive have the ability to store digital data inside the system. When these documents are stored – either by sending them from a PC or by scanning them in at the copier – users cannot retrieve the document unless a secure Print ID and Password is entered on the copier's control panel.





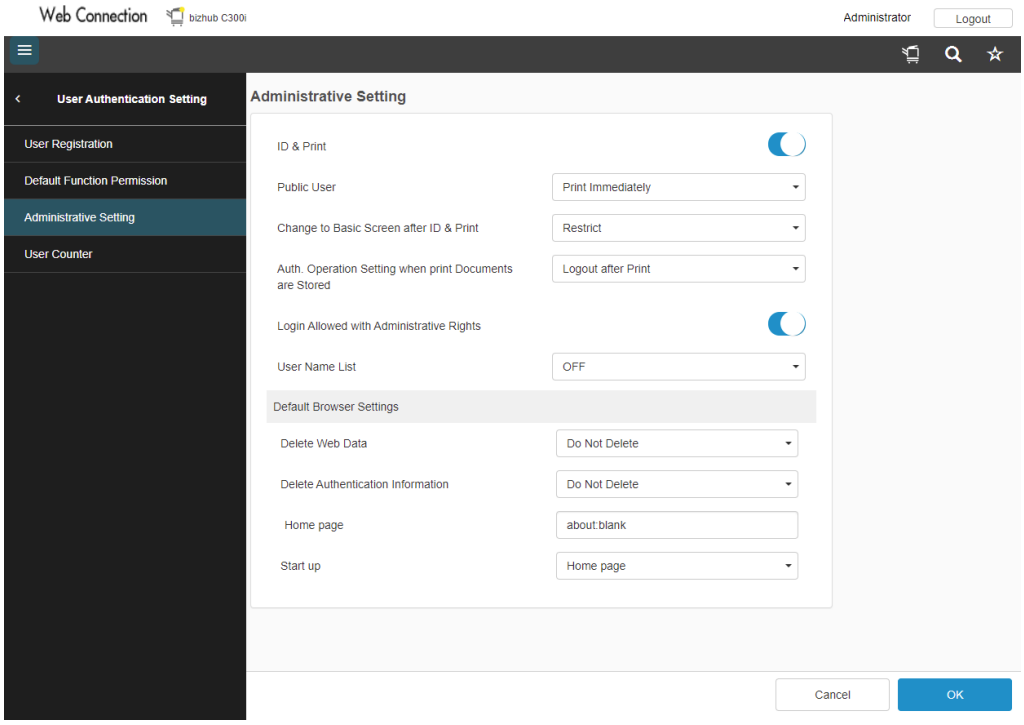
This is an example of the secure print screen from the Konica Minolta bizhub printer driver.

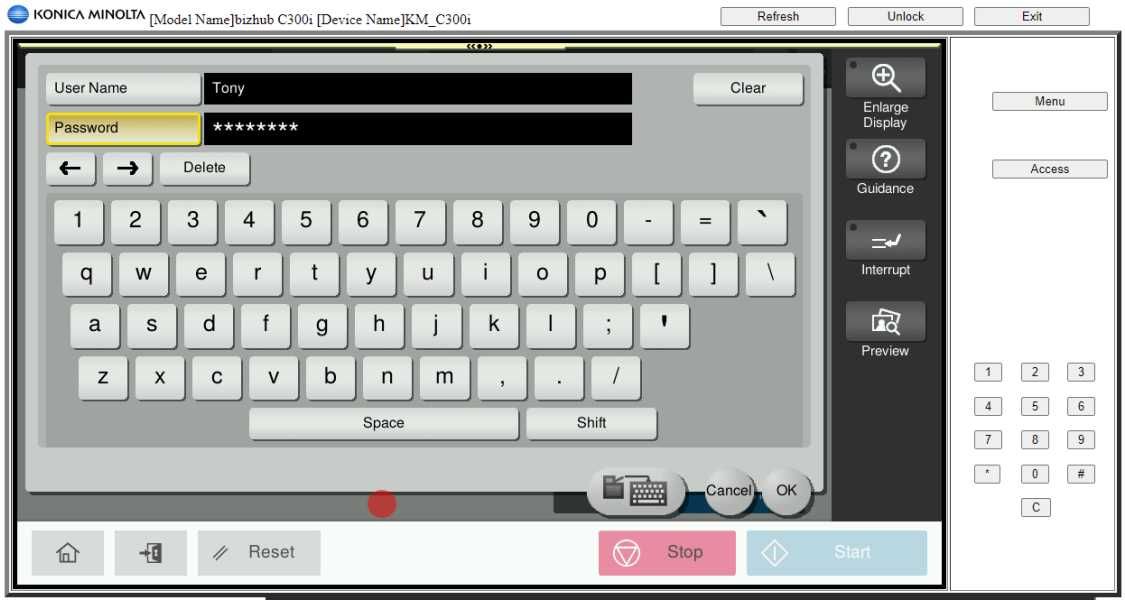
Touch & Print/ID & Print

If the machine is set up with user authentication, server or MFP-based, secure printing can be used via the Touch & Print or ID & Print feature.

Instead of an additional secure print ID and password, the user's Windows Network authentication credentials (typically Active Directory) will be used to identify a stored secure print job, and will release the job after authentication at the device. This will avoid print jobs being released before the user can remove them from the output bin, which will prevent confidential data being viewed by other persons.

Touch & Print is based on authentication via finger vein scanner or IC card reader. ID & Print is based on user authentication via network ID and password.





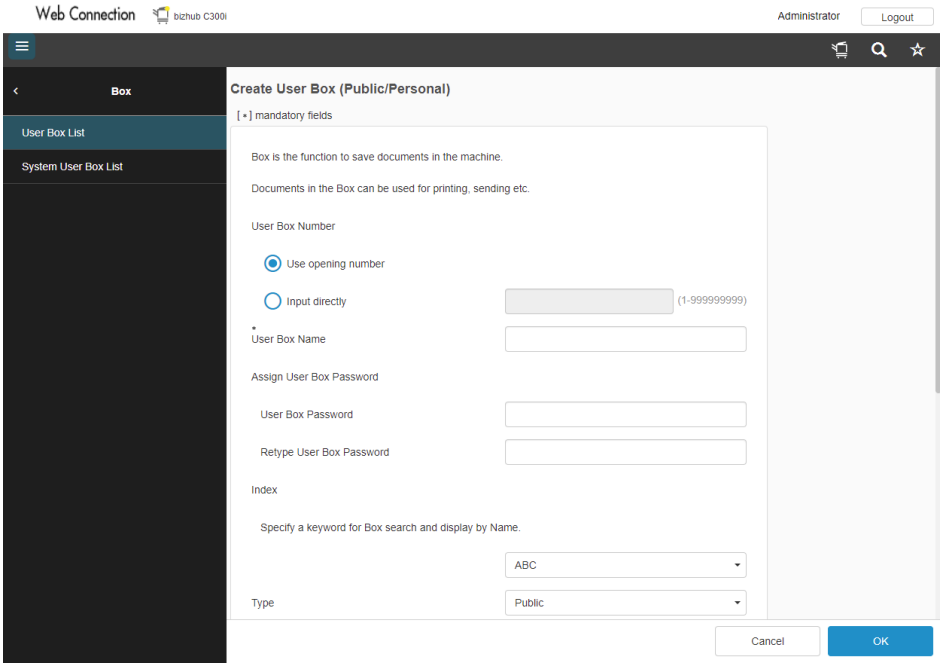
User box password protection

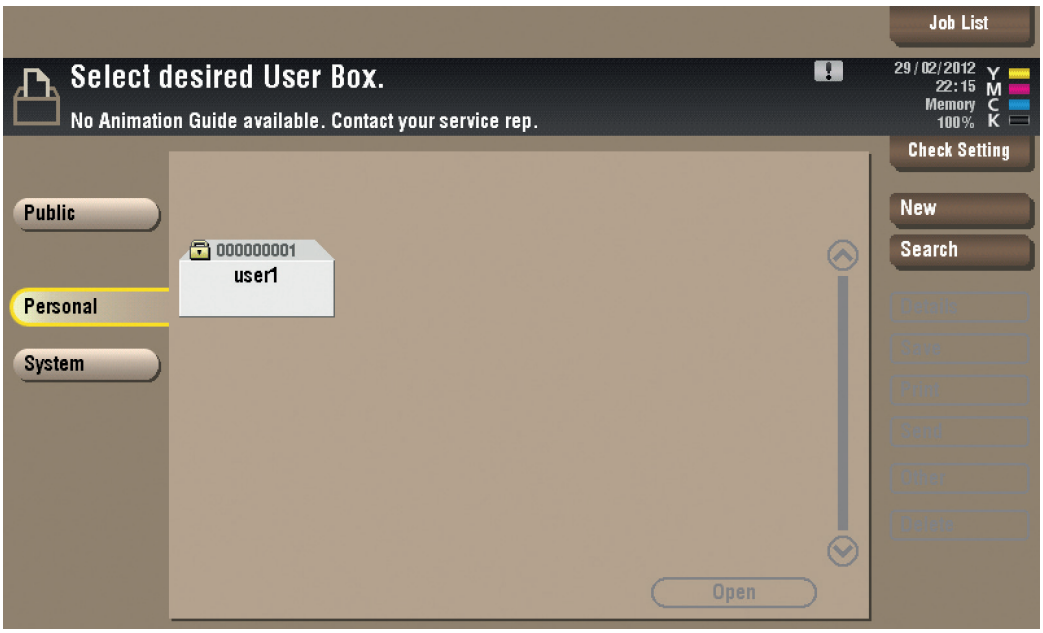
The user box offers the functionality to store commonly used copy, print, scan or fax documents on the hard disk of the MFP. Besides the general security features given to the hard disk, these user boxes can be set with different access levels. On a walk-up MFP the user boxes can be protected by an 16 character alphanumeric password.

If the MFP is set up with authentication, the user boxes can be set as a personal box (only vis- ible for the linked authenticated user), group box (only visible for users who are set up to view the box) or public box.

The access to the user box is automatic via the authentication. But the additional security keeps all users from seeing the box; therefore they have no opportunity to hack into it by trying out passwords. The device can be programmed to delete any documents stored in a user box after a predetermined time period – The factory default is 24 hours – The timer can be set to as little as 5 minutes.

This is an example of set user box registration and user box view on the bizhub panel.

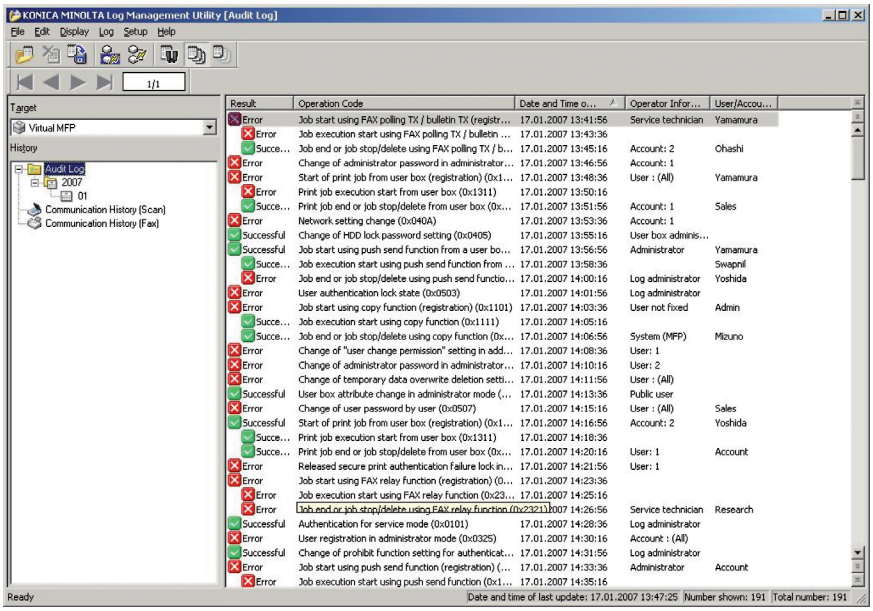




Event log

All Konica Minolta MFPs offer the option to record all actions that have happened on the MFP, (ie.. a print job including sender name, document name and password). These event logs or histories can be downloaded and viewed by the administrator.

To automate the process of event-log downloading, the Log Management utility is available to register and view any actions happening on the MFPs in the network.

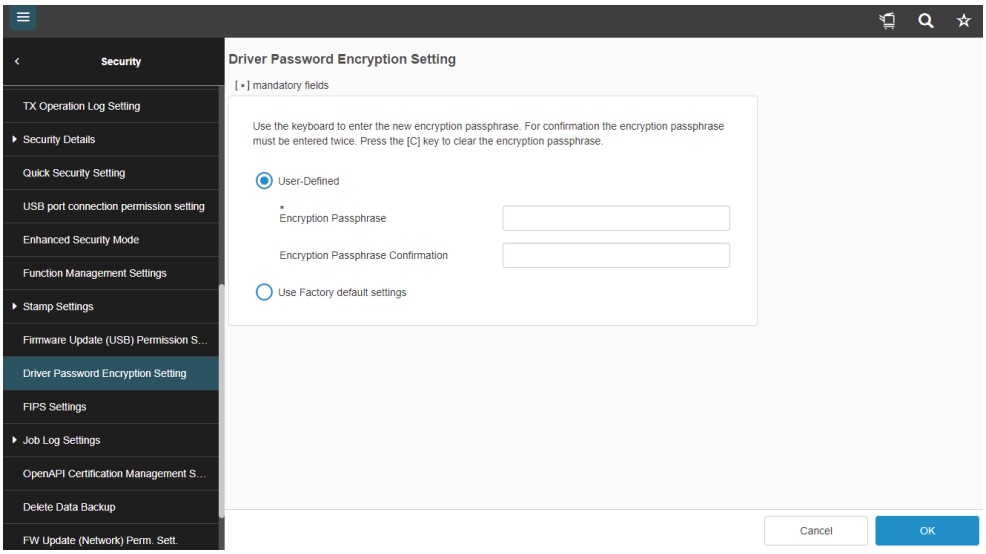


This is an example of the Log Management Utility user interface.

Driver user data encryption

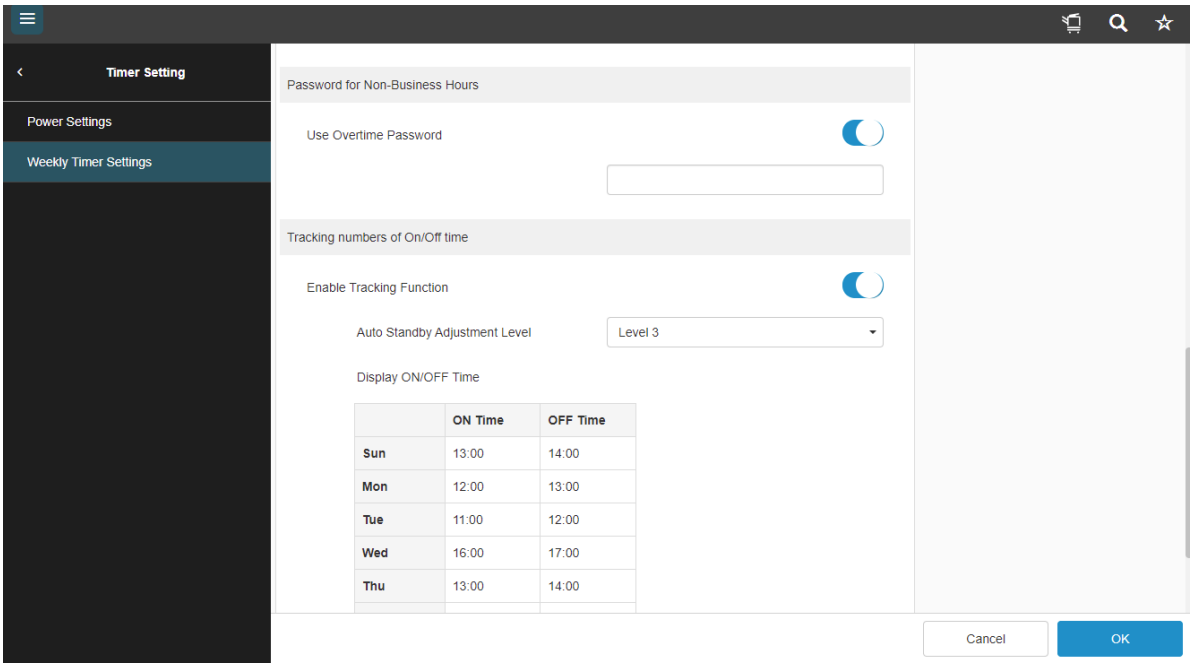
For secure printing, print authentication and print accounting it is necessary for the user to input certain information, ie. user ID and password, in the driver window for transmission to the MFP. To avoid network information from being sniffed, such user data can be encrypted by the printer driver and decrypted on the MFP.

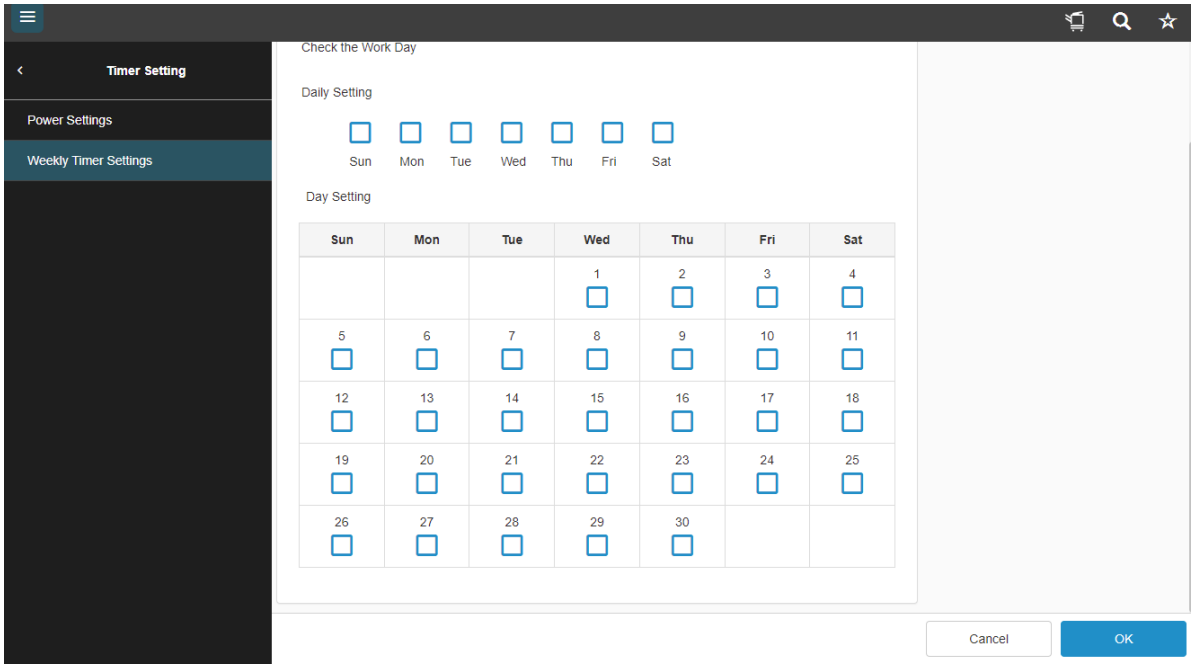
The encryption key can be set individually by the machine administrator with a length of up to 20 digits. If the encryption key is not used by the local user or the print server, print jobs will be printed anyhow. However, confidential user access information might not be safe.



Password for non-business hours

If an MFP is not set up with user authentication, but instead is used as a walk-up device, basically anybody can access the machine and print/send data that is not secure. To prevent this happening, the administrator can program a "business timeframe", during which the machine can be used as a walk-up device, while outside this period a password is necessary to access the machine.



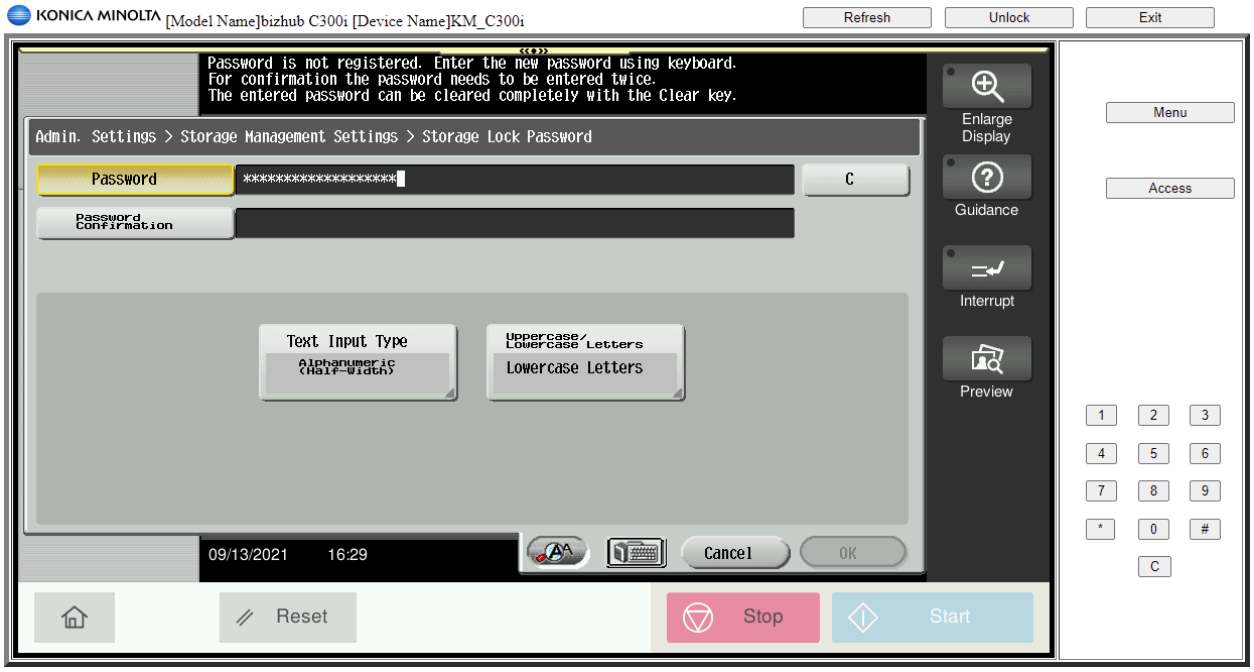


These images are the setup and configuration of the Non-Business Hours feature.

DATA SECURITY

Hard Disk Drive / Solid State Drive password protection

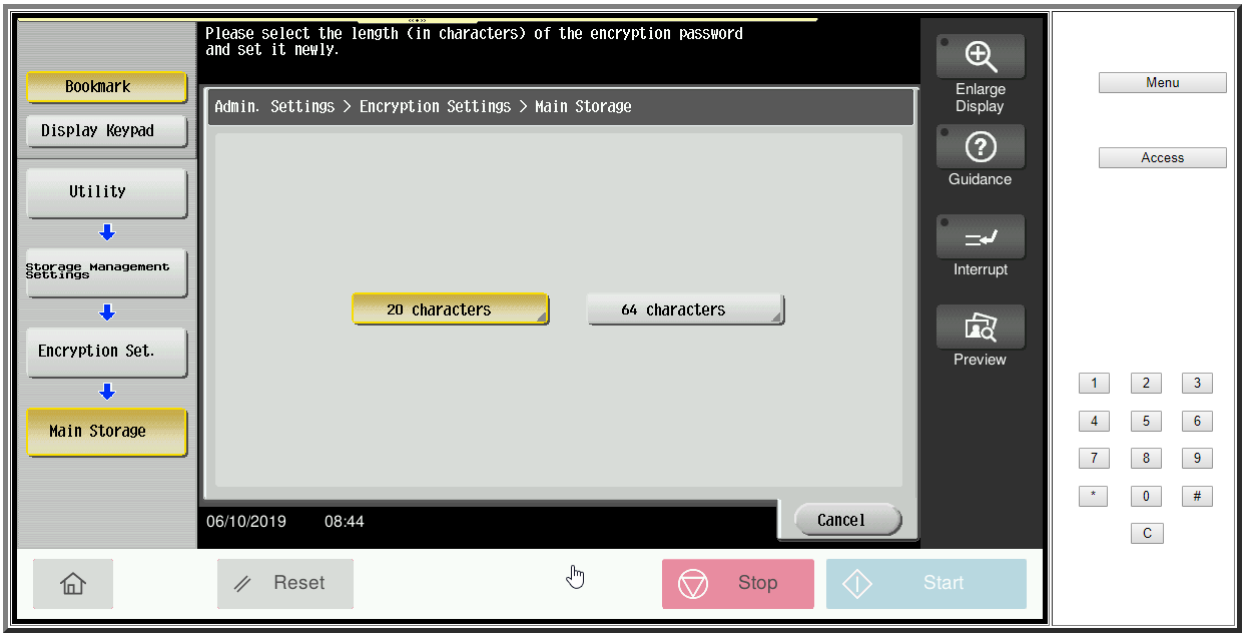
Konica Minolta offers both Hard Disk Drive (HDD) or Solid State Drive (SSD) storage media technology across our product line with the newest models like the i Series MFP devices utilizing SSD storage and our older models using HDD technology. The built-in storage media of the MFP, Printer or Production print device is automatically protected by a password out of the box. This password is stored in the hard disk BIOS and prevents access to the hard disk data, without the correct password being entered. Therefore, even the removal of the storage media and installation of said media into a PC, laptop or other MFP would not give access to the data on the media without entering the correct password. The password is allocated automatically but is recommended to be changed immediately after setup is complete by the machine administrator.

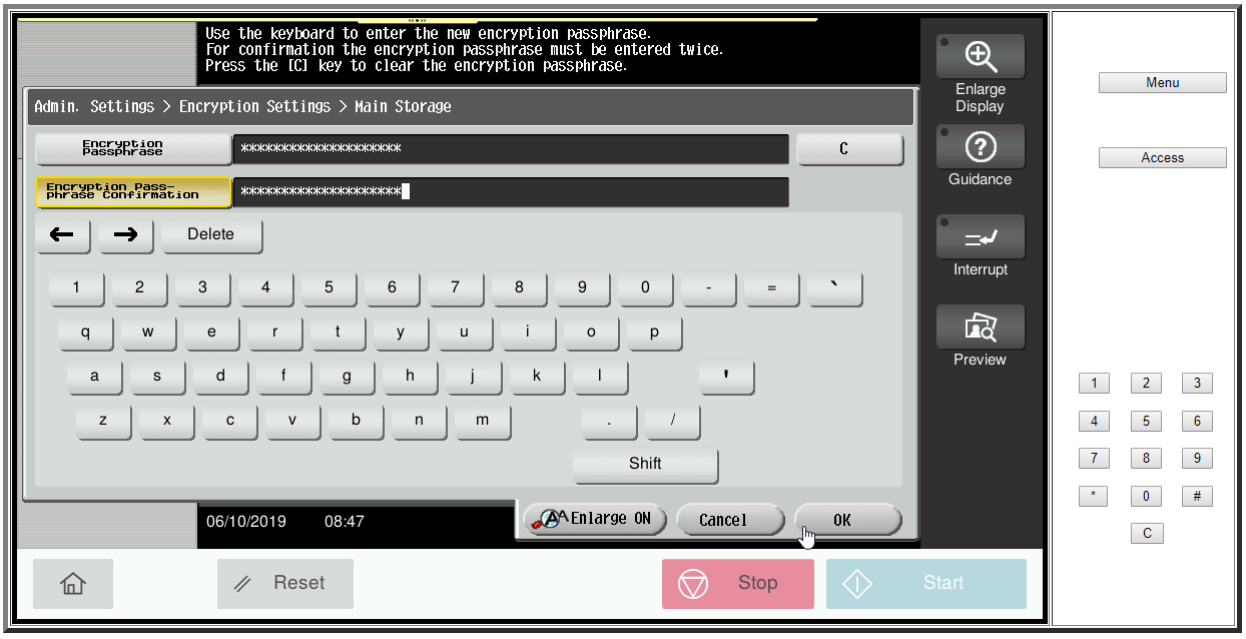


This is an example of MFP password entry in the administration mode for hard-disk protection.

Data Encryption (Storage Media)

Konica Minolta offers a standard, hardened storage media encryption. If desired, electronic documents can be stored in a password-protected box on the storage media. If an organization is concerned about the security of such data, this can be protected by encrypting the storage media and all the data that resides on that media. The stored data is encrypted using the advanced encryption standard (AES) supporting 256-bit key size. Once the storage media is encrypted its data cannot be read, even if the storage media is removed from the Konica Minolta device.

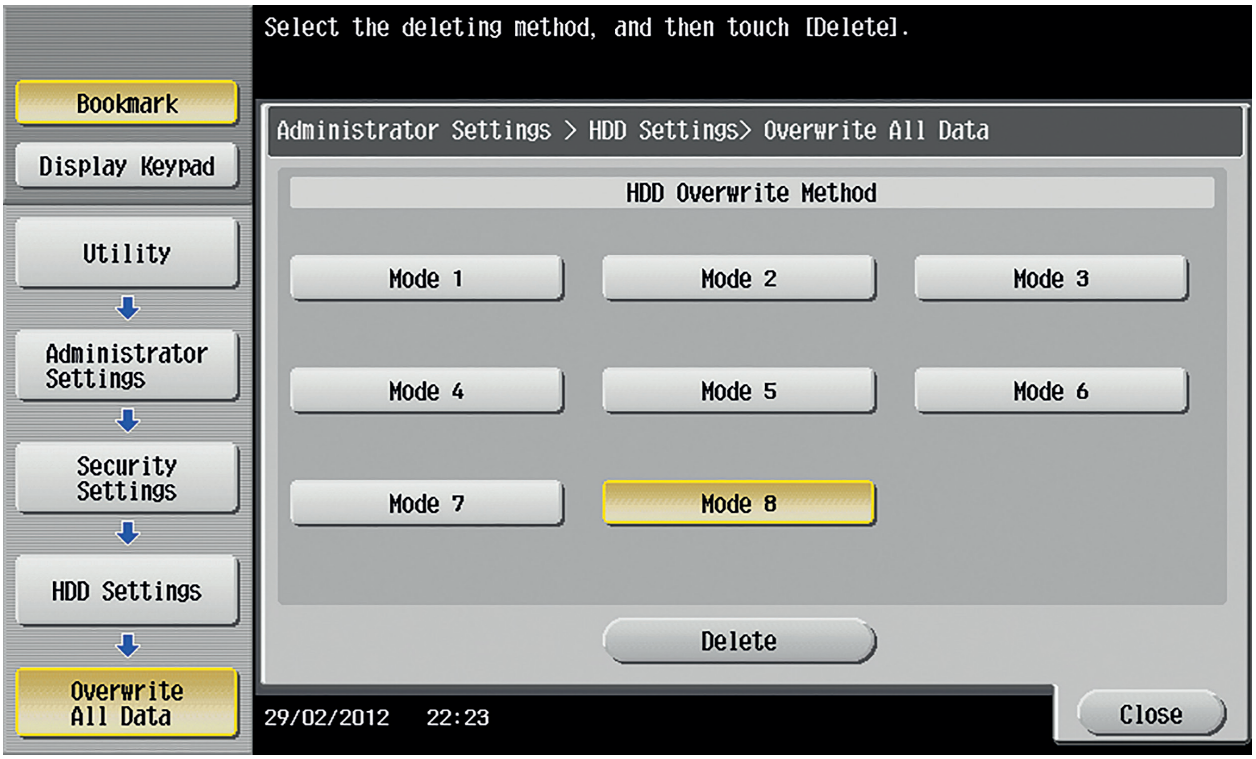




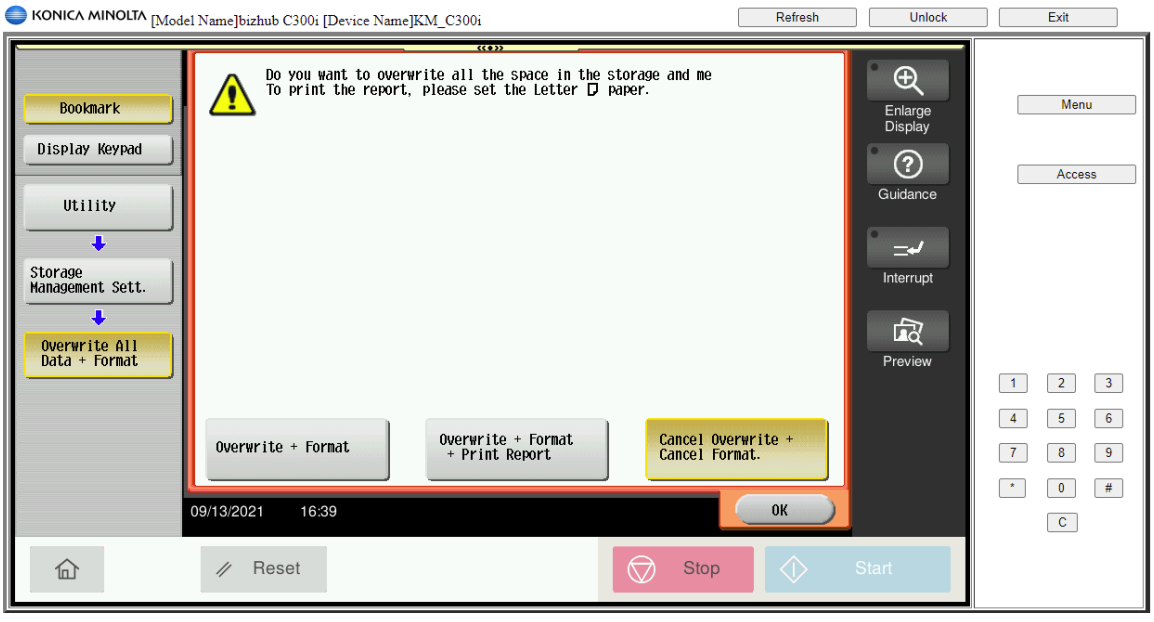
These images are an example of HDD Encryption password character length and setting the encryption password.

Storage Media Overwrite All Data

Another notable difference between HDD vs SSD technology is the Overwrite All Data feature. When equipped with HDD or SSD storage media, Konica Minolta MFPs can store sensitive electronic information. The data can be deleted by those users who own the documents that reside inside the MFP's storage media in password- protected boxes. The data can also be maintained by company security policies that require all data stored in a box location on the MFP be deleted every 30 days for example. For added safety, a key operator, administrator or technicians can physically format (erase) the HDD or SSD if the MFP needs to be relocated or scheduled for End of Life. MFP devices using HDD storage media can be overwritten (sanitized) using a number of different methods conforming to various US governments as pictured to the right. For engines with an HDD, swapping the magnetic orientation multiple times with various overwriting patterns ensures clearing remaining magnetic traces of any stored data.



These examples show the MFP panel of HDD models only for encryption mode selection and the Overwrite + Format start screen. SSD Models do not require these functions



Overwrite All Data Method Specifications are listed in the table below.

Mode 1	Overwrite with 0x00 Japan Electronic & Information Technology Association Russian Standard (GOST)
Mode 2	Overwrite with random 1 byte numbers Current National Security Agency (NSA) standard Overwrite with random 1 byte numbers Overwrite with 0x00
Mode 3	Overwrite with 0x00 National Computer Security Center (NCSC-TG-025) Overwrite with 0xff US Navy (NAVSO P-5239-26) Overwrite with random 1 byte numbers Department of Defense (DoD 5220.22M
Mode 4	Overwrite with random 1 byte numbers Army Regulations (AR380-19) Overwrite with 0x00 Overwrite with 0xff
Mode 5	Overwrite with 0x00 Former NSA Standard Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff
Mode 6	Overwrite with 0x00 North Atlantic Treaty Organization – NATO Standard Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 512 bytes of specified data
Mode 7	Overwrite with 0x00 US Air Force (AFSSI5020) Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa Verified
Mode 8	Overwrite with 0x00 US Air Force (AFSSI5020) Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa Verified

Overwrite All Data Mode only required by HDD Model MFP's

All Konica Minolta MFP devices utilizing SSD media technology use a different "Overwrite All Data" functionality based on the Solid State Drive architecture. At the end of a customer's contract (when customer wants the engine taken away) or the relocation of the MFP to remove any customer-related data the MFP administrator can run the Overwrite All Data function enabling the following processes;

- This function clears all SSD areas used to store any user or admin data by overwriting with a series of 0x00.
- Also initializing all setting data to the original factory default settings.

The overwrite patterns typically used in the HDD Sanitization option are no longer selectable as the pattern for SSD is now fixed to 0x00.For engines with an HDD, swapping the magnetic orientation multiple times with various overwriting patterns ensures clearing remaining magnetic traces. Since an SSD is not a magnetic drive media, 1 time overwrite with 0x00 is sufficient to clear the data completely.

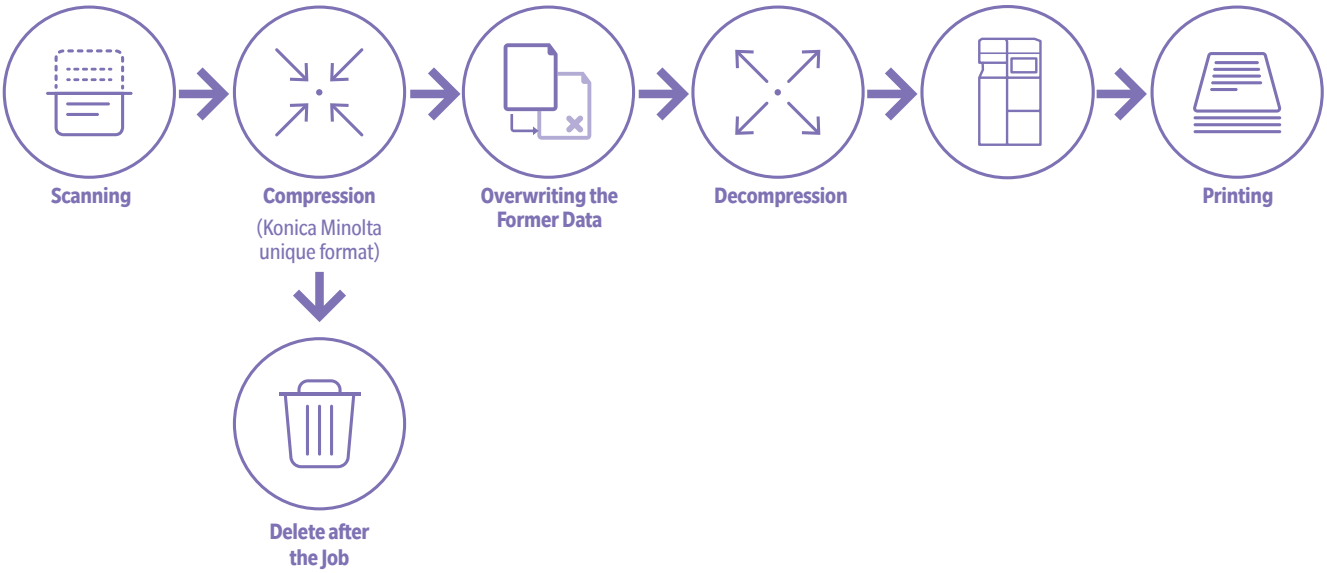
Temporary data deletion (Hard drive based models only)

When utilizing MFP devices using HDD media technology the file size for certain jobs, might use the HDD storage media to swap data for copy, scan, print and fax information during the processing of these jobs. As additional security to protect the information stored on the HDD storage media, the machine can be set to format and overwrite this data on a per-job basis. Under this setting the temporarily swapped data is immediately deleted and overwritten as soon as the data is no longer necessary to end the job in action. This operation runs in the background of the MFP with no effect on MFP performance.

Mode 1	Overwrite with 0x00
Mode 2	Overwrite with 0x00 > Overwritten with Oxff > Overwritten with the letter "A" (=x61) > Verified

For the temporary data deletion two modes are available.

This is an illustration of the MFP copy process with temporary data deletion selected:

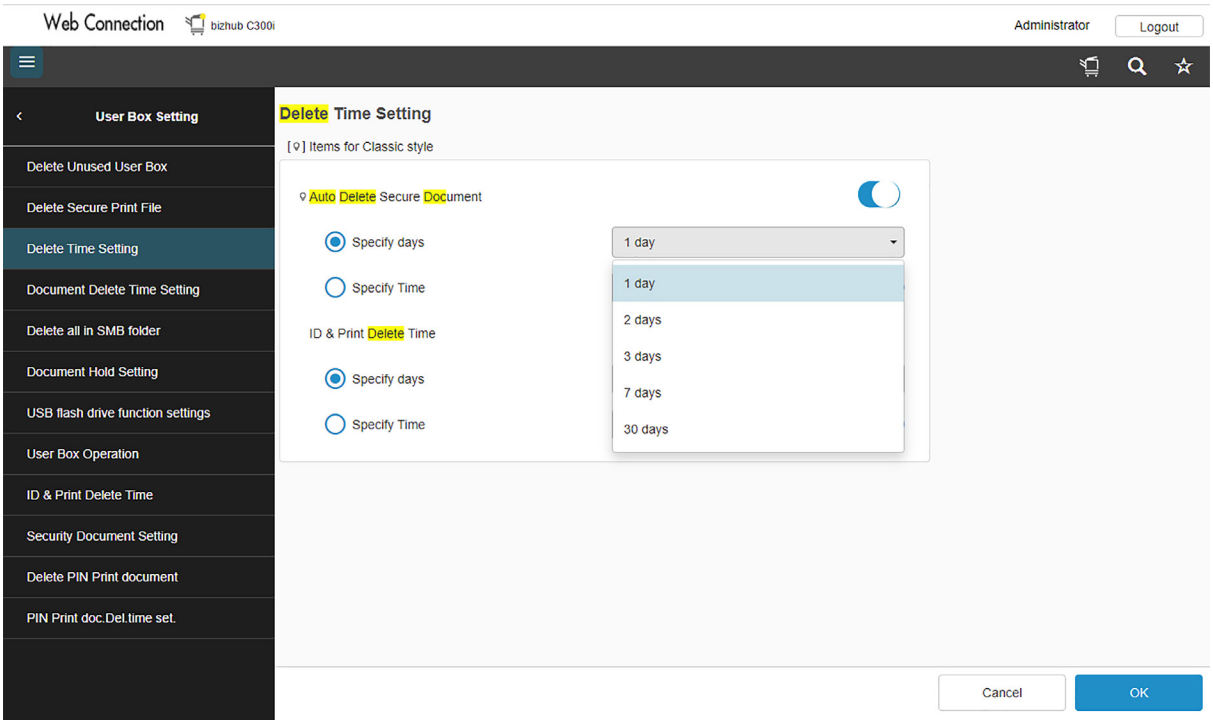


With the adoption of Solid State Drives (SSD) this function is no longer necessary and only pertains to HDD technology. This function is no longer available on MFP devices utilizing SSD media because the SSD implements different technology when compared to an HDD. When temporary data is written in the SSD, it is compressed with a Konica Minolta-owned format where the data is divided into fixed size data blocks. As a result of this process, it is nearly impossible to restore the original image data because:

- The data in NAND flash memory installed in the SSD cannot be directly overwritten. The data must be deleted at the block level, which is a collection of multiple pages. When overwriting, new data is written to a page where data has not been written, and the original address is assigned as if it looks like it has been overwritten. Pages with the old data are assigned different addresses and are marked for deletion.
- The NAND flash memory has a limited number of erase cycles. In order to prolong the life of the SSD, the SSD controller arranges data so that the number of deletions and writes for each page are equalized. This is called "Wear Leveling" (see SSD – "Wear Levelling"). Because of this, the data is saved randomly and separated on the SSD and the address is managed by the SSD itself.
- To maintain optimal SSD performance, some data may be moved to different memory pages than where they were originally saved during the "Garbage Collection" process (see SSD - "Garbage Collection").

Data auto deletion

The administrator can set an auto deletion timer for data stored in the personal or public user boxes, as well as system boxes (e.g. secure print box or encrypted PDF print box). The auto deletion setting will erase the copy, print, scan or fax jobs stored in boxes, depending on the storage period and the timeframe selected for deletion, a little as every 5 minutes to 30 days.

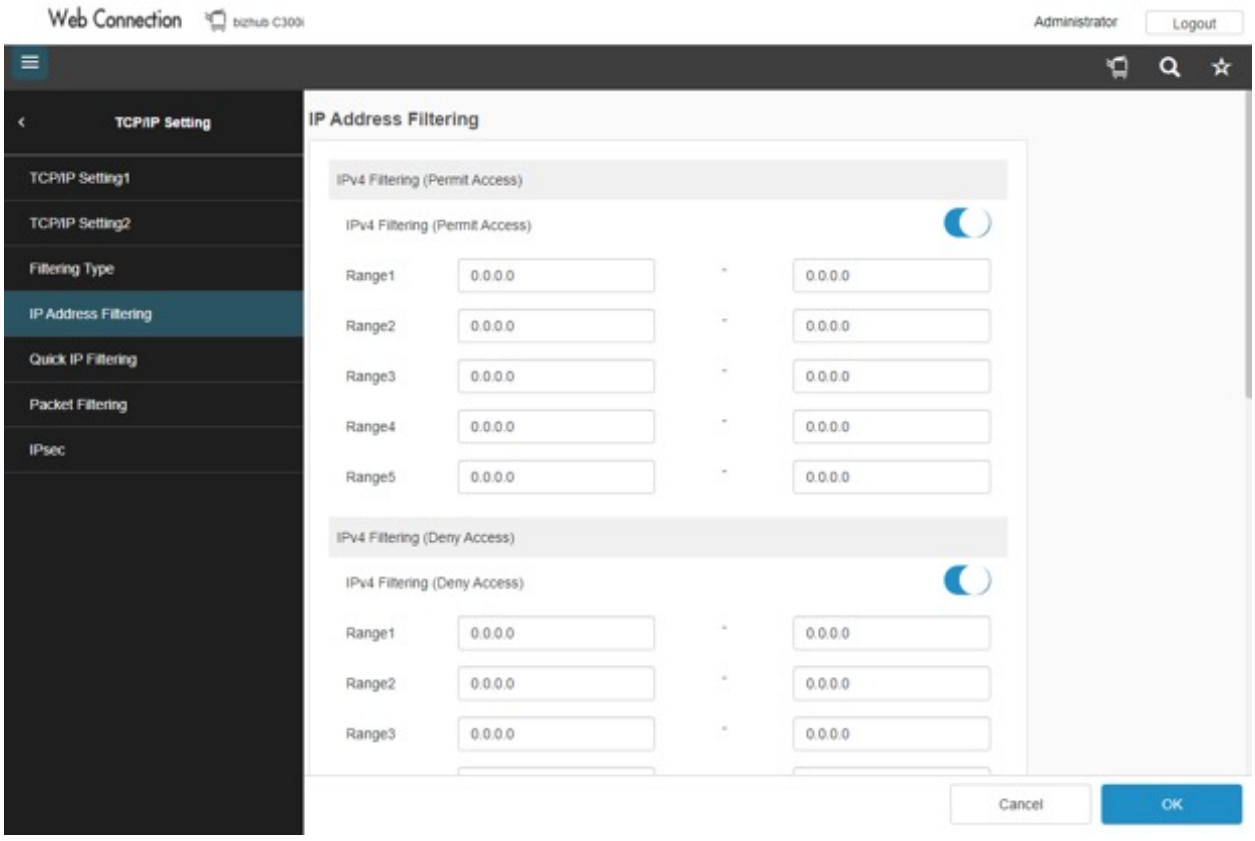


This is an example of the MFP setting for user box document auto deletion.

NETWORK SECURITY

IP Filtering

IP address filtering can be set at the machine where the network interface card of the MFP can be programmed to permit or prohibit access to the device for a specific range of IP addresses for client PCs.



The screenshot illustrates the Web Connection administrator access to a bizhub. Here an administrator can set access permission or refusal to a specific range of IP addresses.

Port and protocol access control

To prevent unnecessary open communication lines on the MFP, open ports and protocols can be opened, closed or enabled and disabled through the administration mode at the machine or remotely via PageScope Web Connection or PageScope Net Care.

The following ports can be opened or closed:

- Port 20 – FTP
- Port 21 – FTP
- Port 25 – SMTP
- Port 80 – HTTP
- Port 123 – NTP
- Port 161 – SNMP
- Port 389 – LDAP
- Port 631 – IPP
- Port 110 – POP3
- Port 636 – LDAP
- for TLS/SSL
- Port 9100 – PDL

The following protocols can be enabled or disabled: SNMP, SMB, POP, FTP, SMTP, IPP, Telnet, LDAP, HTTP

SSL/TLS Encryption (https)

It is VERY important to understand the current environment surrounding SSL(Secure Sockets Layer)/TLS(Transport Layer Security); both are cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network, LAN, WAN, Internet, etc. Both SSL 2.0 and 3.0 have been deprecated by the Internet Engineering Task Force (IETF) in 2011 and 2015, respectively. Over the years vulnerabilities have been and continue to be discovered in the deprecated SSL protocols (e.g. POODLE, DROWN). Most modern browsers will show an insecure user experience (e.g. line through the padlock or https in the URL bar, or other security warnings) when they encounter a web server using the old protocols. For these reasons, you should disable SSL 2.0 and 3.0 in your server configuration!

With the introduction of TLS 1.3 in 2018 TLS 1.0 and TLS 1.1, are now considered deprecated as well. TLS 1.3 makes significant improvements over its predecessors and right now major players around the internet are pushing for its proliferation. Microsoft, Apple, Google, Mozilla, and Cloudflare all announced plans to deprecate both TLS 1.0 and TLS 1.1 in January 2020, making TLS 1.2 and TLS 1.3 the only game in town. Konica Minolta MFPs have supportedTLS v1.2 for many years.

This has been the industry standard and is compatible with most of the popular print management applications including Konica Minolta Dispatcher Paragon.

That being said, Encrypting the data communication between servers, machines, and applications operating over a network is critically important to the security of the network and the data in the network. The encryption of network communication is essential with regard to the transmission of, for example, authentication data or administrator passwords.

Communication can be encrypted for:

- LDAP protocol
- POP protocol
- Windows Active Directory
- Address Book Utility
- SMTP protocol
- IPP (IPPS) protocol
- Data Administrator
- Web Connection (https)

Adoption of TLSv1.x Elliptic Curve Cryptography

Konica Minolta has adopted Elliptic Curve Cryptography (ECC) in support of encrypted communication by SSL/TLS.

Elliptic curve cryptography (ECC) is a public key encryption technique based on an elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation, Diffie-Hellman and RSA cryptographic methods, which are based on the creation of keys by using very large prime numbers. This traditional method of key creation requires a lot of computational power. According to some researchers, ECC can achieve the same level of security with a 164-bit key where other "Traditional" systems will require a 1,024-bit key. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Elliptic Curve Digital Signature Algorithm (ECDSA) based on elliptic curve cryptography is used as an digital signature algorithm for this server certificate.

Also, ECDH (Elliptic curve Diffident–Hellman key exchange) is used as a key exchange algorithm.

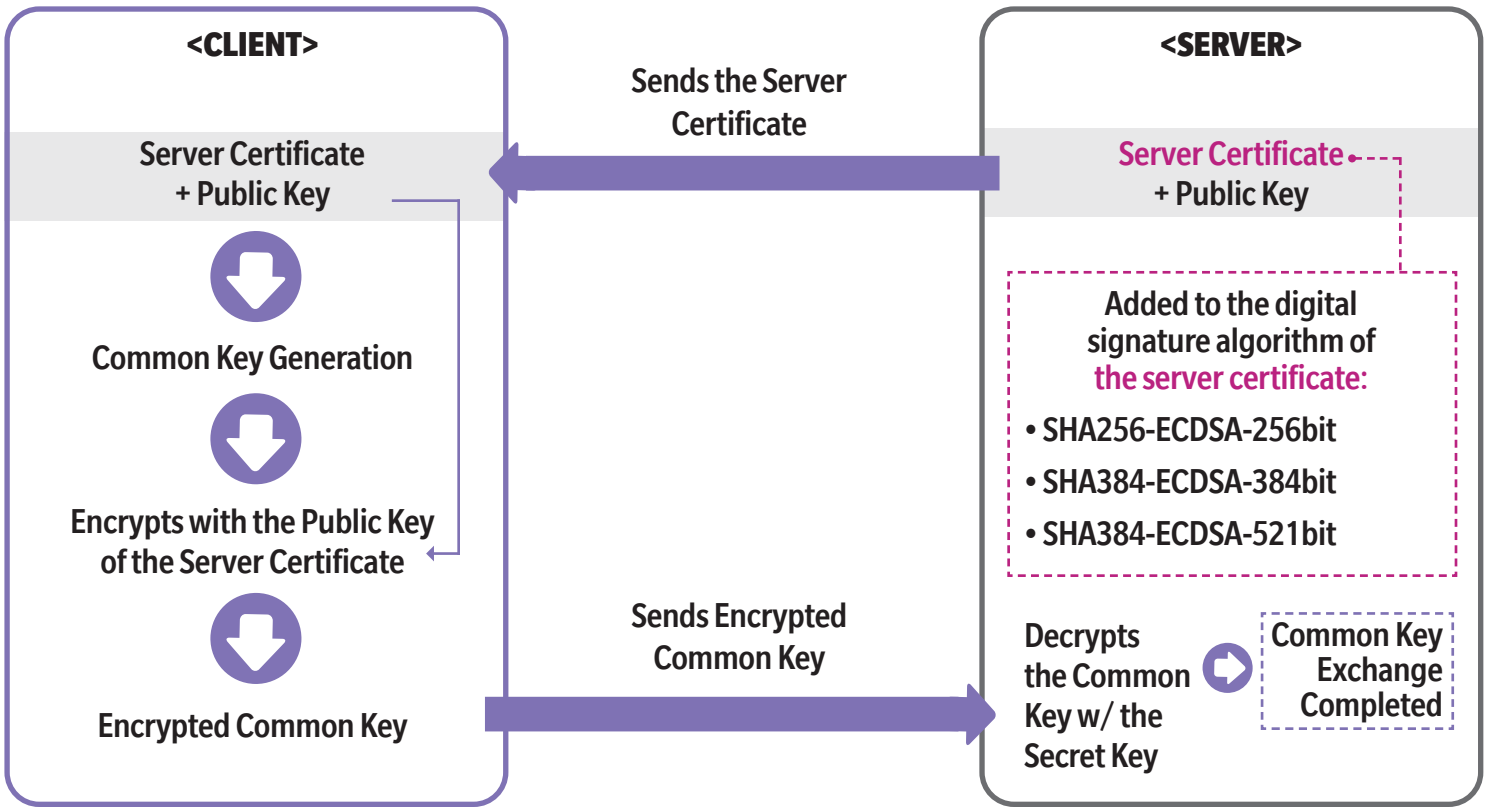
Konica Minolta uses Elliptic curve cryptography in the following cases.

- Elliptic Curve Digital Signature Algorithm (ECDSA) based on elliptic curve cryptography is used as an digital signature algorithm for this server certificate.
- Elliptic curve Diffident–Hellman key exchange (ECDH) is used as a key exchange algorithm.
- When an MFP device acts as client: It can communicate with the server which is using Elliptic Curve Cryptography
- When an MFP device acts as server: It can create server certificates using Elliptic Curve Cryptography
- When creating and issuing a certificate: ECDSA can be selected as an encryption key type
- At the time of import/export of certificate: It supports certificates with ECDSA as an encryption key

In this way, the highest security can be fulfilled.

FLOW OF PUBLIC KEY SHARING

A common key required for the encrypteed communication by SSL is exchanged with the following flow.



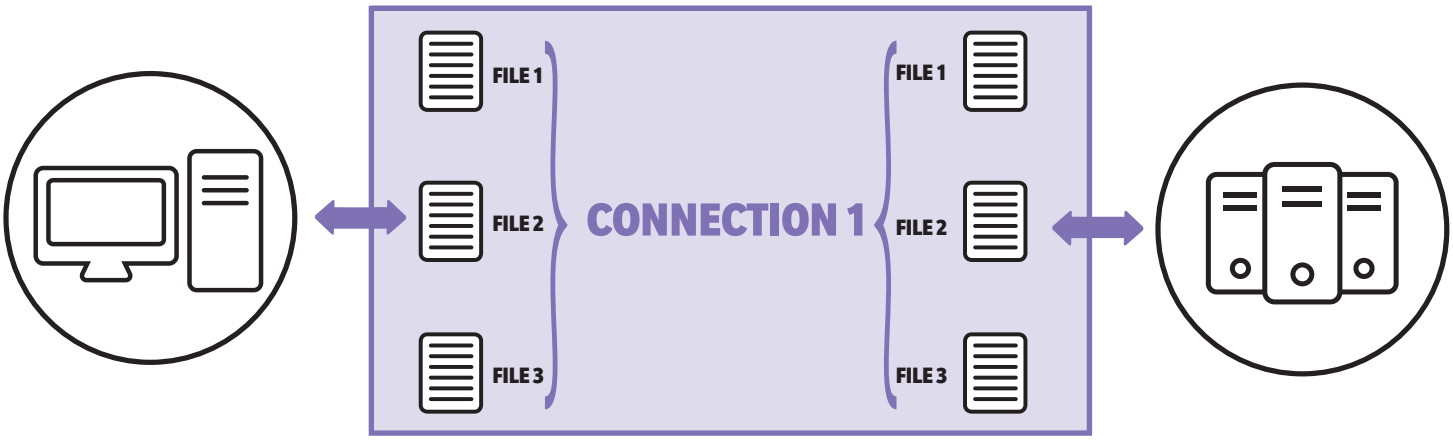
Adoption of HTTP/2 over TLS

"HTTP/2" is a new version of HTTP protocol. Approved as a formal specification on February 17, 2015. It improves the Internet connection and connectivity to the cloud environment with the introduction of the "Stream" concept that can process multiple requests/responses with a single TCP connection, and the "Server push" function capable of request/response processing with priority control and asynchronously. It supports HTTP/2 in major Web browsers (Google Chrome, Microsoft Edge, Safari, etc.), however the MFP device is compatible with only HTTP/2 over TLS. Also, it is necessary to enable communication by SSL/TLS to use HTTP/2 in this device. Since encrypted communication is mandatory, it improves the security when using a Web browser.

DIFFERENCE BETWEEN HTTP 1.1 AND HTTP/2

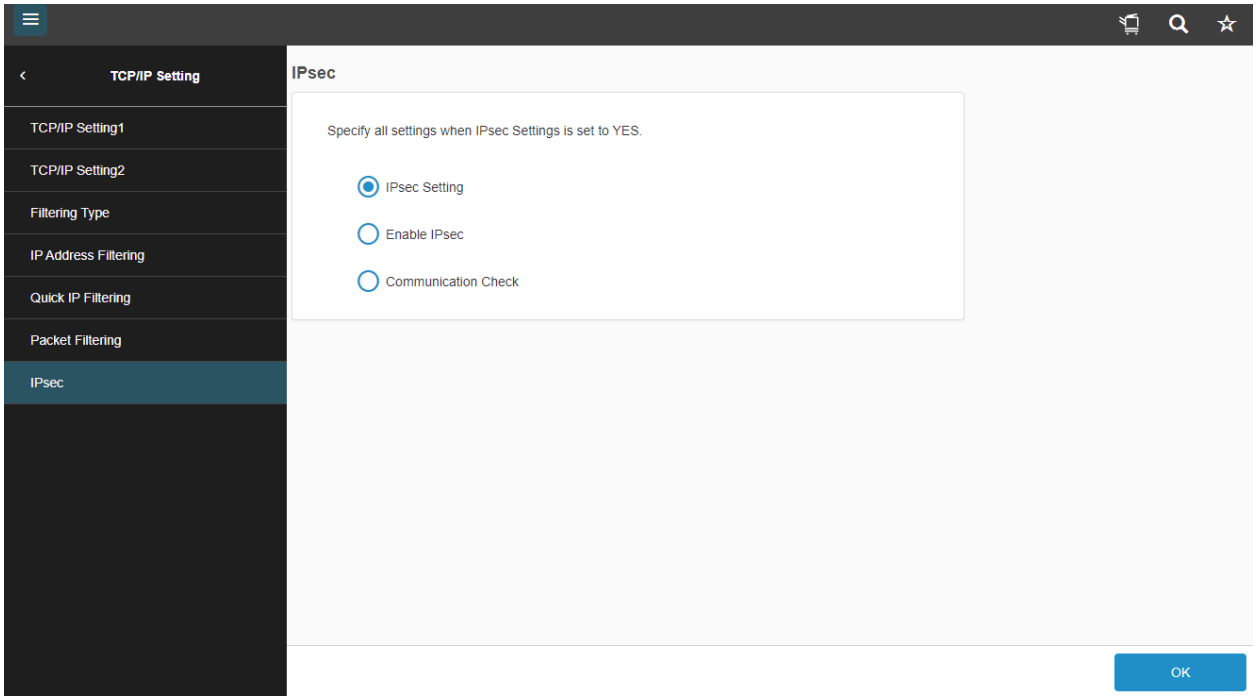
HTTP 1.1: Multiple TCP connections are necessary

HTTP/2: Multiple requests/responses can be included in a single TCP connection



IPsec support

To complete the encryption of any network data transmitted to or from the MFP, the bizhub devices also support IPsec (IP security protocol). This protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself. The IPsec protocol can be programmed via the IKE settings. Up to four groups of IPsec/IKE settings can be stored.



Abolition of Vulnerable Protocols in IPsec Communication Settings

Vulnerable protocols and encryption schemes have been removed from the IPsec communication settings.

By removing these vulnerabilities, IPsec communication can now be used safely and more securely.

The following changes were made in Web Connection's [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting].

Vulnerable Protocols in IPsec Communications Defined

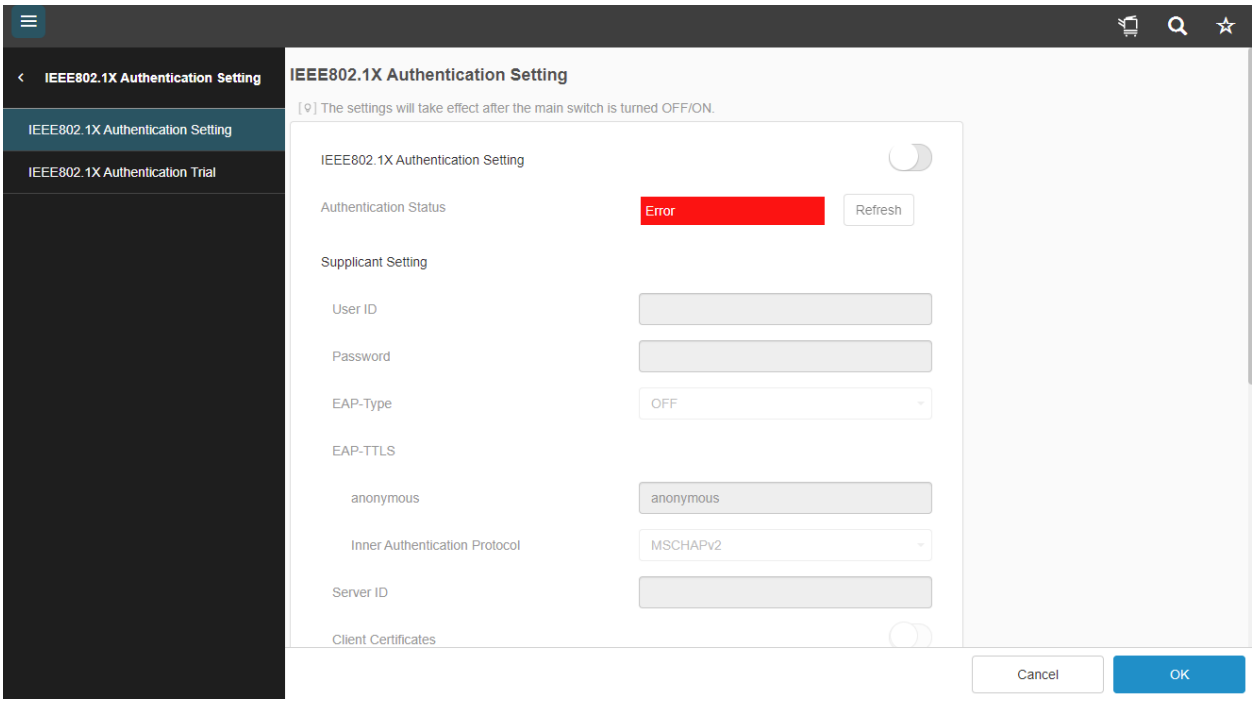
CHANGED POINTS	CORRESPONDING LOCATION (IN THE [IPSEC SETTING] MENU)	IMPACT ON USER
MD5 without support	[IKE], [SA]	When MD5 is used, it is necessary to change the settings in the algorithm such as SHA1.
No support to DES is provided when using ESP	[SA]-[IKE Setting]-[ESP Encryption Algorithm]	When DES is used, it is necessary to change the settings in the algorithm such as AES.
When using ESP, the settings without the authentication algorithm are not supported	[SA]-[IKE Setting]-[ESP Authentication Algorithm]	In the security protocol if ESP is used and if authentication algorithm is not specified, the settings of authentication algorithm such as SHA1 is necessary.
"Manual key" is not supported as key exchange method	[SA]-[Key Exchange Method]	When using the manual key, it is necessary to change the key exchange method to IKE.
The range settings of IPaddress is not supported (Instead, subnet specifications and unicast specifications are supported)	[Peer]-[Set IP Address]	• When a specific host is to be excluded from the subnet: Disable IPsec connection using IP filtering, etc. • When a specific host is to be added to the subnet: Specify IP address individually in unicast specification.
It is not necessary to specify TCP/UDP port or specify it individually	[Protocol Setting]-[Port No.]	• When protecting the entire traffic using only one IPsec session: It is not necessary to specify port number • When TCP/UDP session is to be protected individually: Individually set the port number to be used in the session.
When using AH, authentication algorithm "AES_GMAC" is not supported	[SA]-[IKE Setting]-[AH Authentication Algorithm	When authentication algorithm "AES_GMAC" is used, it is necessary to change the the security protocol settings from AH to ESP.

IEEE 802.1x support

IEEE 802.1x is a port-based authentication standard for network access control to WAN and LAN networks.

The IEEE 802.1x authentication standard generates a secure network by closing any network communication (e.g. DHCP or HTTP) to unauthorized devices except for authentication requests. This prevents devices gaining access to a network by sim- ply acquiring an IP address via DHCP and, for instance, performing a man-in-the-middle attack to sniff data streams on the network.

Only proper authentication, a password or certificate entered by the authenticator will grant access to the secure network



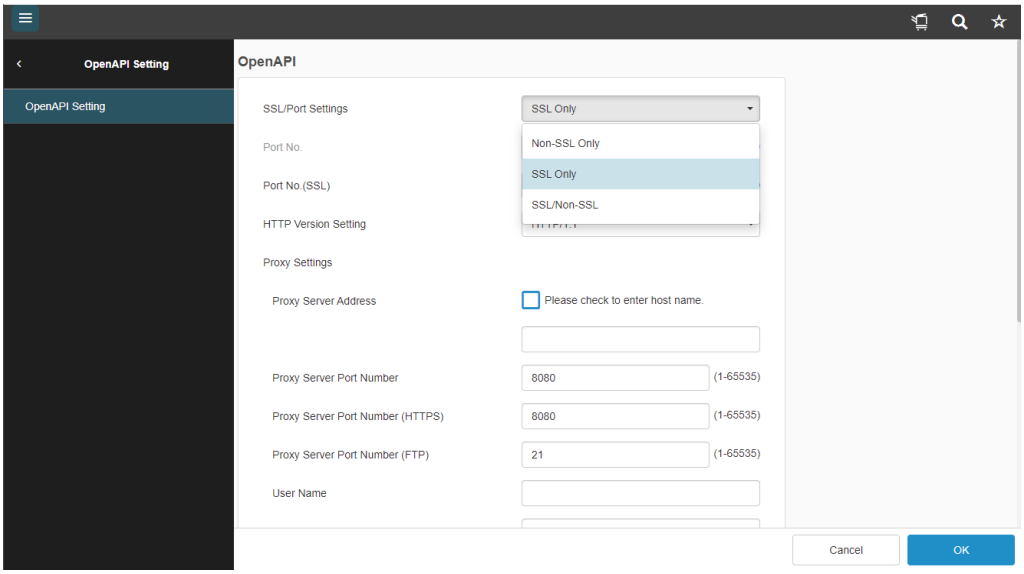
This is an example of the MFP 802.1x authentication settings

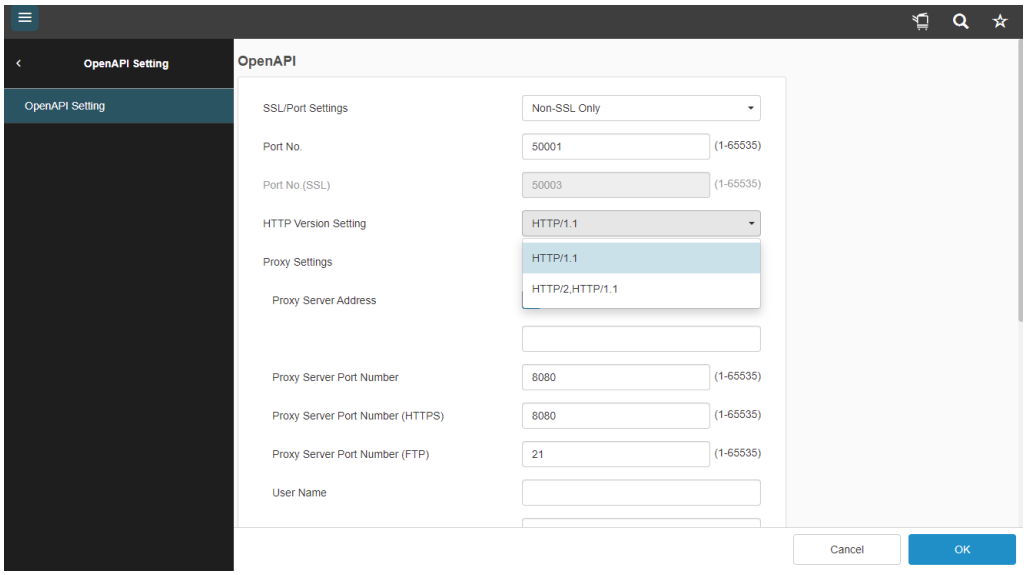
OpenAPI (Application Programming Interface) communication

Most of the Konica Minolta devices are equipped with OpenAPI. OpenAPI is Konica Minolta's own application programming interface. This gives users the option of integrating Konica Minolta devices into application-controlled workflows, such as external authentication, secure pull printing, job and cost accounting as well as scan workflows

bizhub OpenAPI acquires and sets the data received from devices via networks using the SSL/TLS encryption protocol. By using an original password, communication is rendered more secure.

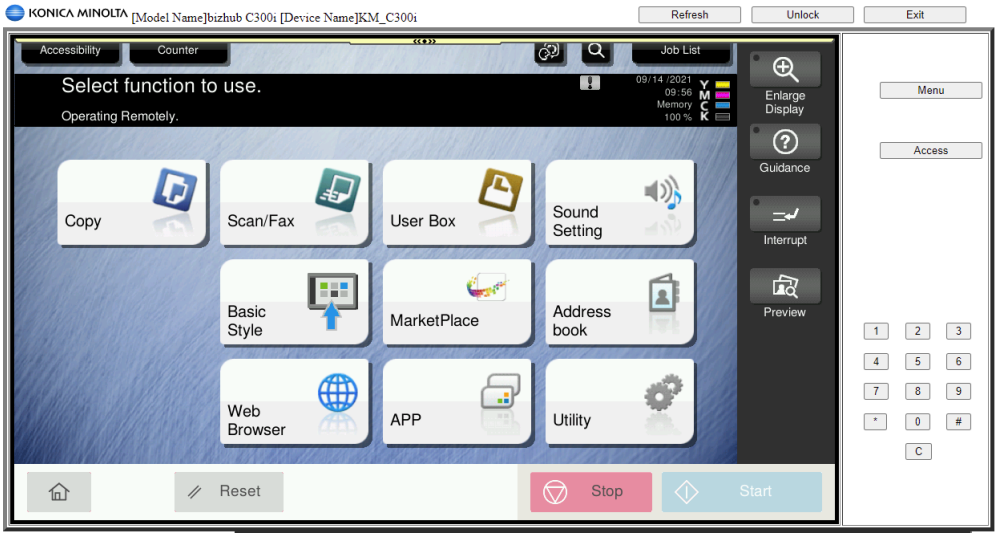
When managing the important data of the device (e.g. setting information on user authentication), the data is safely protected.



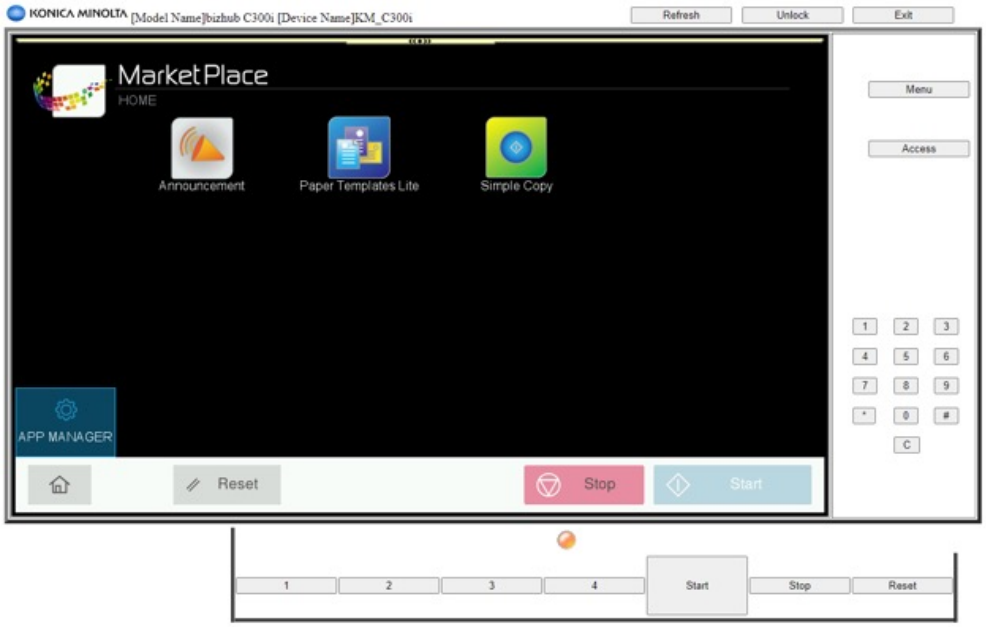


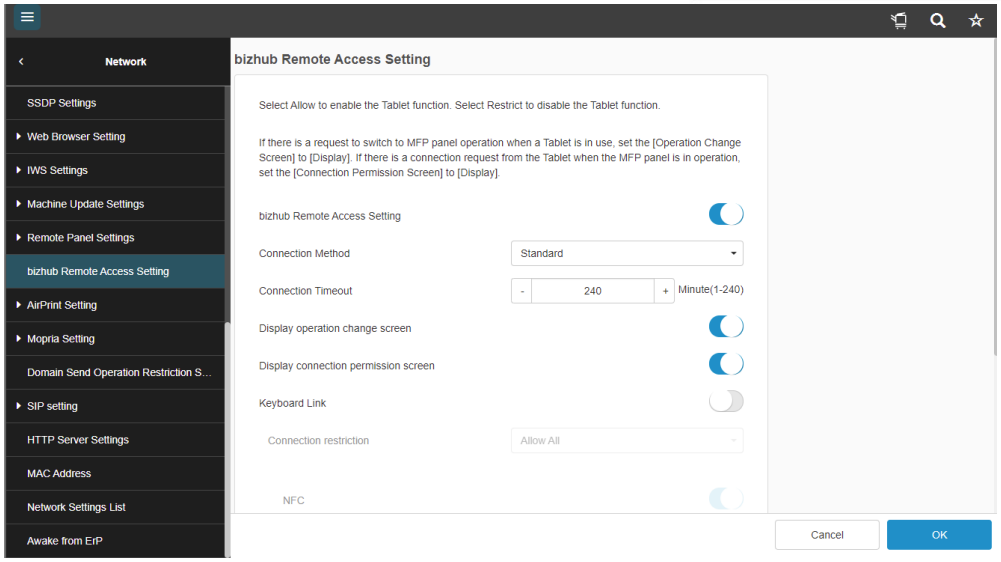
Remote panel

The latest generations of Konica Minolta devices offer the option of a remote panel. This means administrators are able to have real-time access to the MFP panel remotely, e. g. via a Web browser. Every function which is available on the MFP panel can also be executed remotely.



These are examples of the Remote Panel screens





There are various settings with which the remote panel feature can be configured, made secure or disabled.

SCAN SECURITY

POP before SMTP

To secure access to the MFP with the intranet email server, it is possible to authenticate with an email account (POP3 – Post Office Protocol) before an email is sent via the email server. This avoids the possibility of unauthorized email traffic with the intranet email server, and with the domain/email suffix respectively.

In addition to the above email security, APOP (Authentication for Post Office Protocol) can be set. APOP is an authentication method with encrypted passwords which ensures increased safety in comparison to the usual unencrypted password exchange used by POP for the retrieval of email messages.

SMTP authentication (SASL)

SMTP (Simple Mail Transfer Protocol) authentication can be activated on bizhub MFPs. This authorizes a device to send emails. For those customers who do not host their email services, the use of an ISP mail server is possible and supported by the machine. SMTP authentication is required by, for example, AOL and for the prevention of SPAM

S/MIME

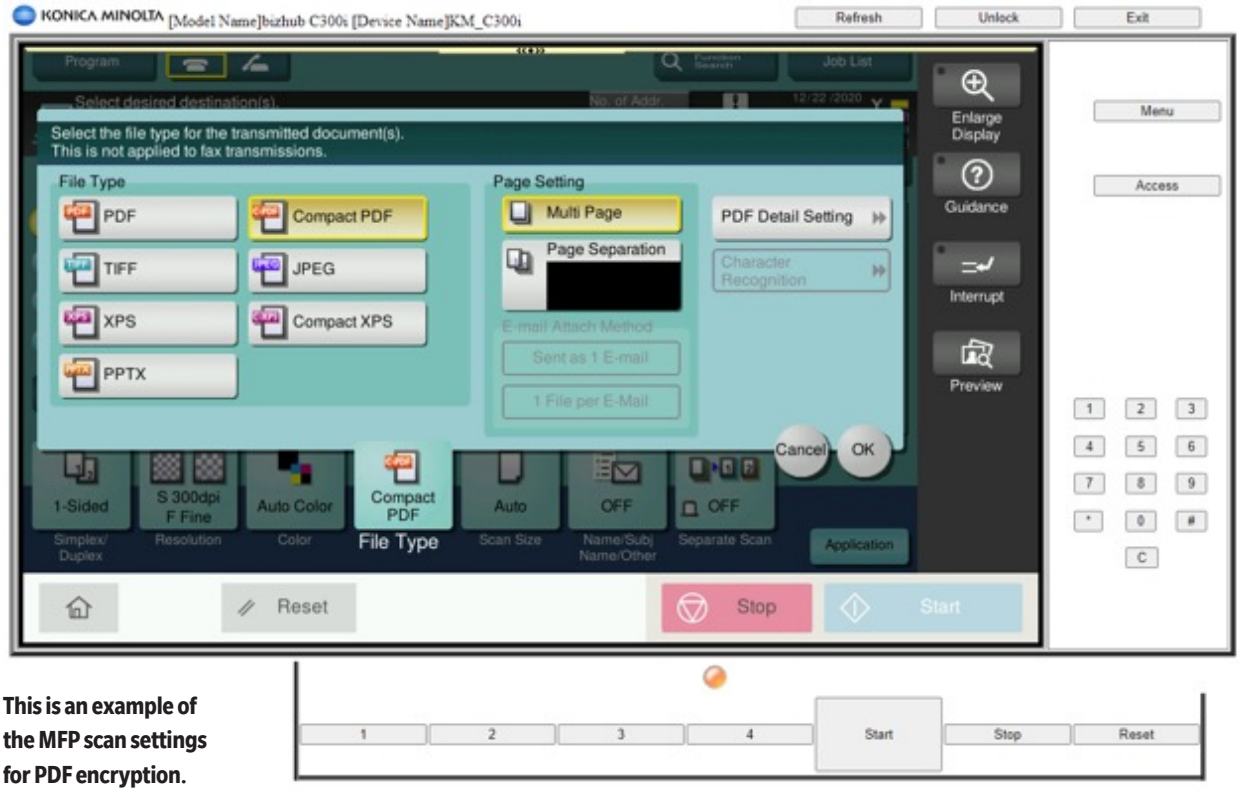
For email transmission, the MFPs support S/MIME (Secure/Multipurpose Internet Mail Extensions) encryption.

S/MIME encryption is based on email certificates that can be registered on the MFP for all stored email addresses. The encryption of the email information by the "public key" (given via the certificate) prevents the sniffing and unauthorized decryption of email information at a high security level. For example, if an email is sent accidentally to a wrong destination, the email information can still only be opened by the intended recipient, who is the only one in possession of the "private key" necessary for decryption.

Encrypted PDF

bizhub OP-based products can encrypt scanned files in PDF format before sending them to a destination across the network. The user has the ability to encrypt a scanned file by selecting the encryption key on the bizhub's control panel. The encryption option supports the PDF file type, and will require the decryption code to open the file from the recipient of the scan.

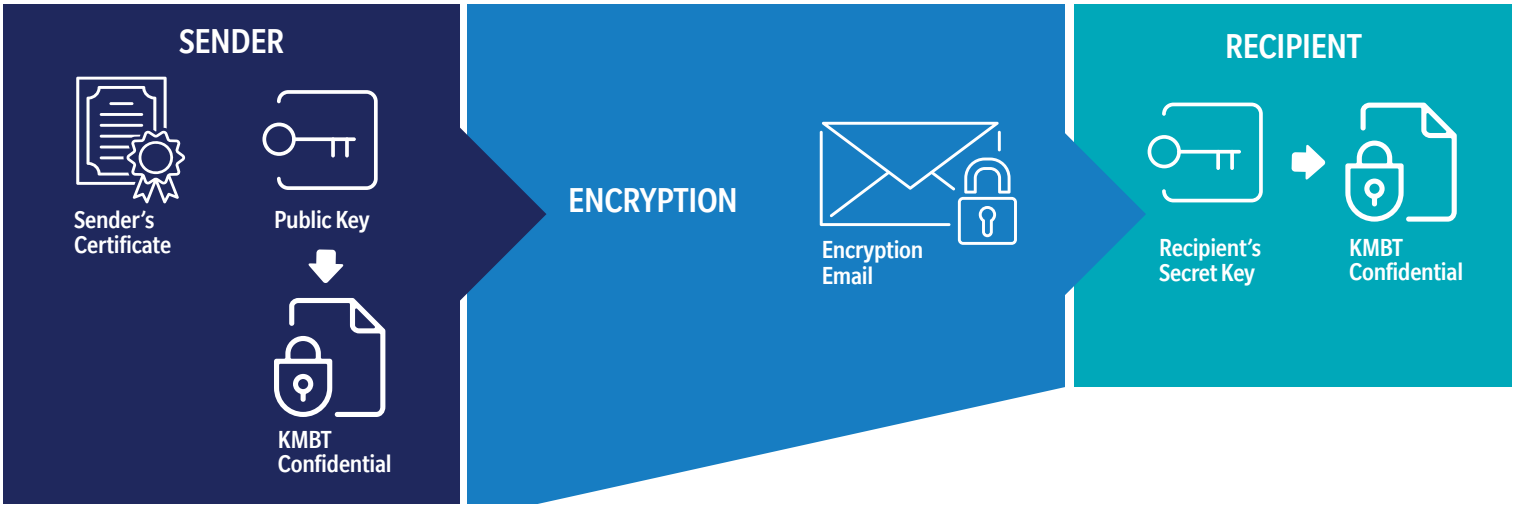
This feature is very similar to the Adobe Acrobat encryption process where a password is utilized for encryption and opening a file, as well as to access the permissions area of the encryption process. This functionality is now included as standard in the i-Series MFP.



This is an example of the MFP scan settings for PDF encryption.

PDF encryption via digital ID

PDF data that is attached to an email or sent to an FTP or SMB folder can be encrypted by a digital ID. Digital ID encryption is based on the S/MIME encryption using a public key for encryption and private key for decryption. Compared to S/MIME, the digital ID will only secure the attachment, which also allows using this transmission process for other transmission types than email. In addition to digital ID stored on the MFP, certificates and/or public keys stored on the LDAP server can be used. This functionality is now included as standard in the i-Series MFP.



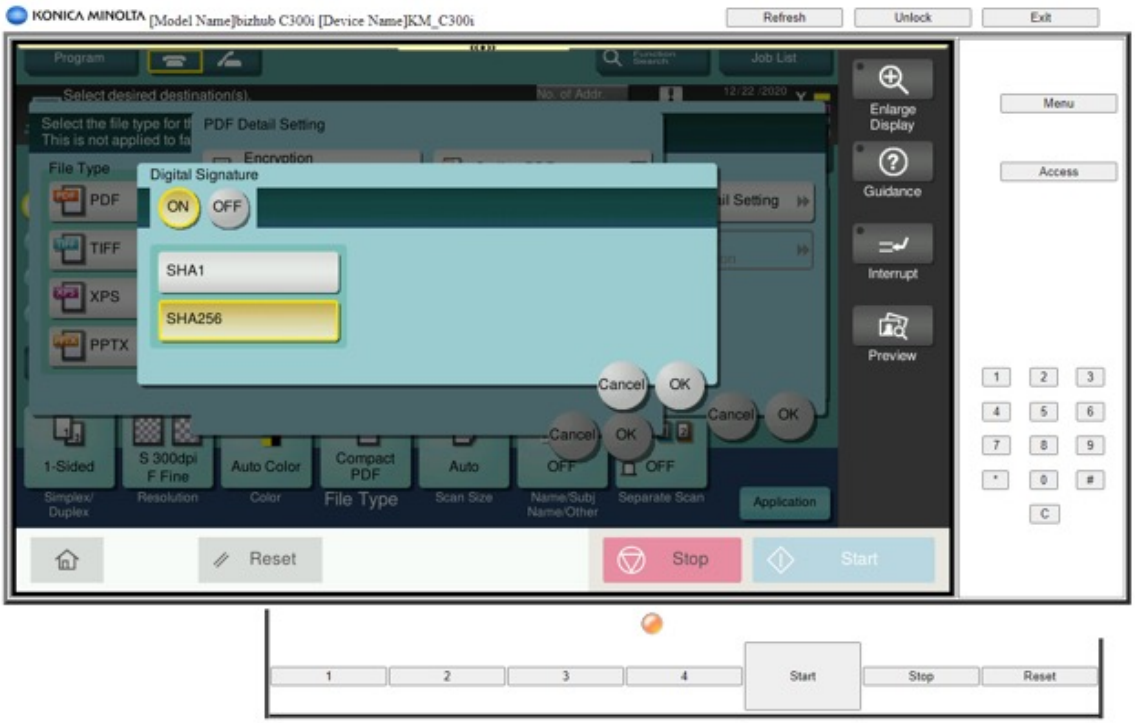
This illustration shows the encryption process via digital ID.

PDF digital signature

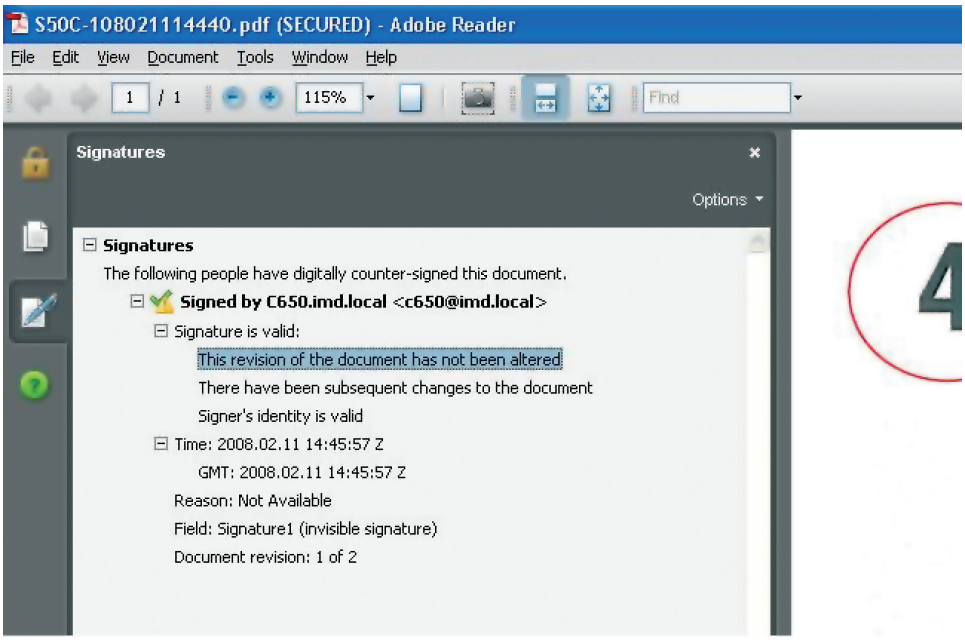
To prevent tampering with MFP-created PDF documents, it is possible to add a digital signature. The digital signature is based on the SSL certificate installed on, or used by, the MFP.

The certificate information will be added to the PDF file without encryption. However, changes to the PDF after creation (e.g. changing text, adding or deleting items) will be recorded in the PDF security information which is available in the PDF reading applications.

In addition to preventing documents from being tampered with, the PDF signature gives information about the source of the document, helping the program to recognize invalid document sources. This functionality is now included as standard in the i-Series MFP.



This is an example of the MFP digital signature settings for PDF files.



This screenshot is an example of a PDF document that has been signed with a digital ID. The signature information shows that this document has been altered since its creation and is no longer valid/trustworthy.

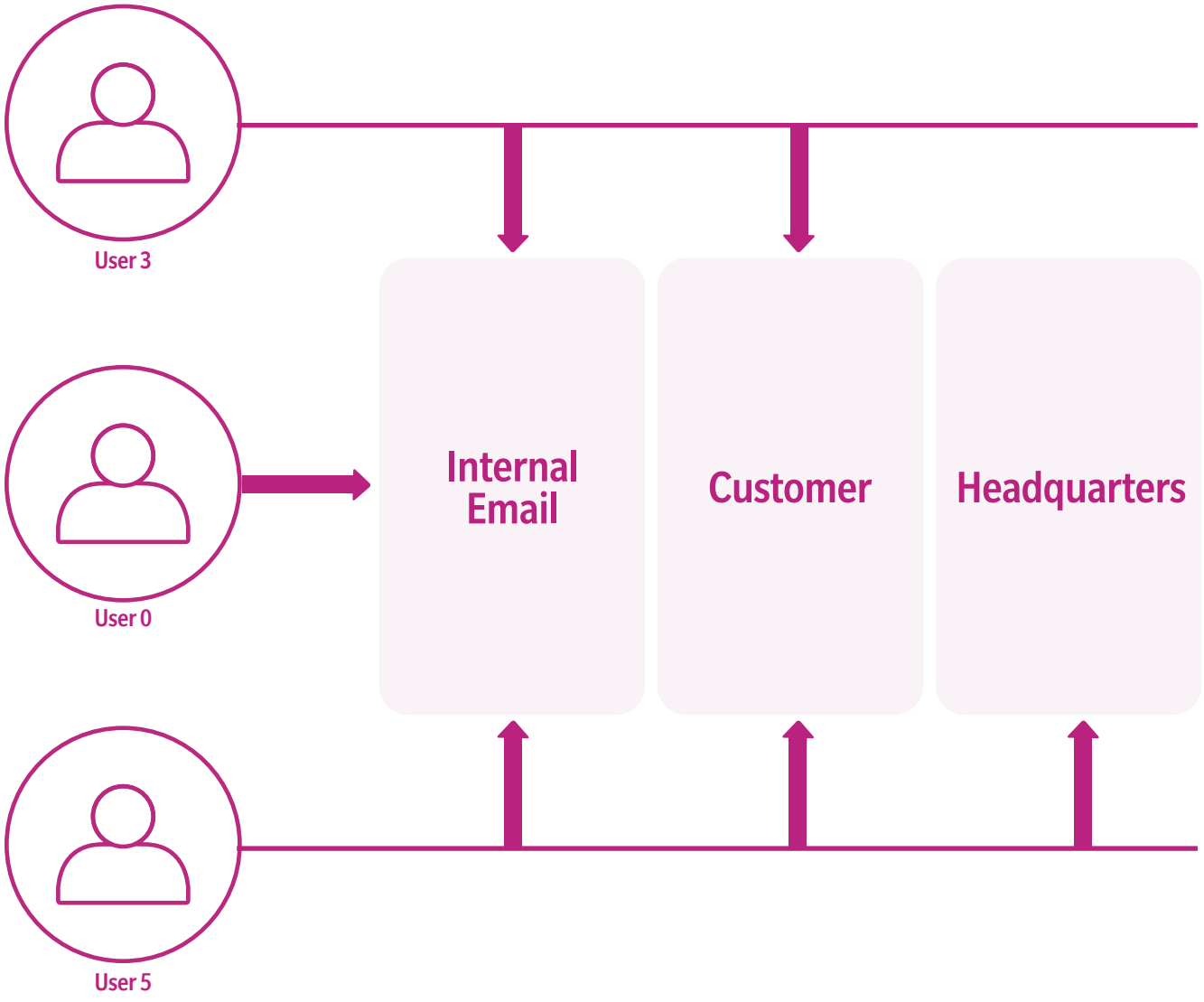
MANUAL DESTINATION BLOCKING

The selection of manual destination blocking will prevent the direct input of, for example, email addresses for transmission of scan files from the MFP. If it is set to "on", the user only has the possibility to use destinations stored on the MFP.

In addition to preventing the direct input of destinations, the user can be blocked from changing the FROM address for an email transmission. If the machine is set to authentication, the user's email address stored in the authentication data or Active Directory will automatically be used.

Address book access control

The destinations (ie. email, SMB, FTP) stored in the MFP or address book can be set with an access level. These levels control the access/visibility of destinations for the user, depending on their security level as given in the authentication data. Possible levels are 0–5.



ADDITIONAL VALUE ADDED SECURITY OFFERINGS

bizhub SECURE Suite of Solutions

The bizhub SECURE Suite of Solutions includes HDD/SSD storage media and data hardening, customized port and protocol restrictions to meet specific industry requirements like HIPAA, FERPA, Sarbanes Oxley, PCI Audits, etc. Konica Minolta offers these solutions as a value added service on behalf of our clients who do not have the infrastructure or bandwidth to enable and configure these critical security functions, settings and protocols. The bizhub SECURE Suite of solutions has been expanded to also include the protection and monitoring of PII at all MFP locations and real-time, on-board anti-virus and malware detection.

bizhub SECURE

In today's business and professional world, our customers' data can be the most valuable – and also the most vulnerable. How can our customers make certain their valuable data is safe from theft – and prevented from being stolen from an MFP by an unauthorized user or extracted if the storage media is removed from the multifunction device? Konica Minolta offers lockdown protection with bizhub® SECURE: a set of enhanced password and data security measures to give your bizhub MFP an extra level of security.

At Konica Minolta we understand that your organization may not have the bandwidth or infrastructure to enable, configure and track the security functions that are required for compliance or internal mandates. That is why we developed the bizhub SECURE Service. To provide you with the resource you need to lockdown and protect any document data that might reside on the bizhub's internal storage media.

Ultimately, a secure document workflow is everyone's responsibility. Konica Minolta has led the industry by providing enhanced security features for the digital era – and with powerful bizhub SECURE functions activated by your authorized Konica Minolta field engineer; you'll have an additional line of defense against data theft and unauthorized access to documents or devices.

- Create a 20-digit secure alphanumeric password to lock down your bizhub storage media
- Encrypt the entire contents of your bizhub storage media for remarkable data security
- Time your bizhub MFP to auto-delete any material located in personal or public User Boxes, System User Boxes, Documents and Folders
- Automatic overwrite of Temporary Image Data (not required on iSeries due to SSD technology)
- Disable non-secured and unwanted services, protocols and ports at the MFP

AccurioPro SECURE

Konica Minolta also offers the same lockdown protection of bizhub® SECURE but specifically for our Production Print devices called AccurioPro SECURE.

Reassuring peace of mind

Hackers can relatively easily access devices if the default password has never been changed. So we make sure each admin password is changed from default mode to a unique and secure password to prevent unauthorized access. We also equip each AccurioPress device with a control mechanism to ensure the admin password is most securely set, i.e. with a sufficiently safe combination of characters and numbers.

Password-protected documents and hard drive – no data can go astray

Business-critical documents can be stored on the AccurioPress device's hard drive. If you want an even higher level of security, the hard drive can be encrypted to prevent data being read, even if the hard drive is removed.

Automatic deletion of print jobs

When documents are printed in your business, potentially confidential data is sent to the printer and temporarily stored. To prevent access to such data, AccurioPro SECURE can be set to automatic deletion mode – yet another way of safe-guarding business-critical data on your AccurioPress device.

Continuous real time status of your security settings

For your peace of mind you can choose an optional application that highlights at a glance if all your security settings are still in place and re-enforced.

bizhub SECURE Platinum

To meet your security needs, our bizhub SECURE Platinum solution and IT Services combine to enhance your security, speed your work and help control your costs. We provide assurance in today's ever-changing workplace environment to help you navigate these questions. And succeed.

Lockdown protection for your MFP means safeguarding information and defending your organization from security breaches. Konica Minolta offers your organization the enhanced confidence and compliance of bizhub SECURE Platinum: powerful password and advanced network and data security measures to protect your valuable data. These enhanced security features will be enabled by your Konica Minolta Field Engineer to ensure that your data is more than secure – it's bizhub SECURE. It's just another way that Konica Minolta gives shape to ideas.

Konica Minolta's bizhub SECURE Platinum provides the following set of features:

- Create a 20-digit secure alphanumeric password to lock down your bizhub storage media
- Encrypt the entire contents of your bizhub storage media for remarkable data security
- Eliminate any trace of data even after it's been deleted with Temporary Data Overwrite (Temporary Data Overwrite conforms to DoD methods)
- Time your bizhub MFP to auto-delete any material located in personal or public User Boxes, System User Boxes, Documents and Folders
- Disable Non-secured and unwanted Services, Protocols and Ports at the MFP
- Enable TLS v1.2* on the MFP (self-signed certificate)
- Enable Network User Authentication
- Enable MFP Audit Logs

* TLS v1.3 available in June 2021 on i-Series MFPs only

bizhub SECURE Healthcare

HIPAA COMPLIANCE RELATED TO PATIENT SECURITY AND CONFIDENTIALITY ARE CRITICAL CONCERNS.
Massive fines have been handed out to organizations that have Patient Confidentiality breaches.

To satisfy these requirements, Konica Minolta provides the industry's most comprehensive suite of standard privacy and security solutions based on bizhub SECURE Platinum technology. Konica Minolta provides all the tools needed for Healthcare officials to protect patient information with secure printing, scanning, copying and faxing functions. Konica Minolta MFPs feature the lock-down protection of bizhub® SECURE Healthcare to help you ensure patient confidentiality and enhance your organization's HIPAA compliance strategy.

Lockdown protection for your MFP means safeguarding information and defending your organization from security breaches. Konica Minolta offers healthcare professionals the enhanced confidence and compliance of bizhub SECURE Healthcare: powerful password, network ports & protocols and data security measures to protect your ePHI (electronic Protected Health Information).

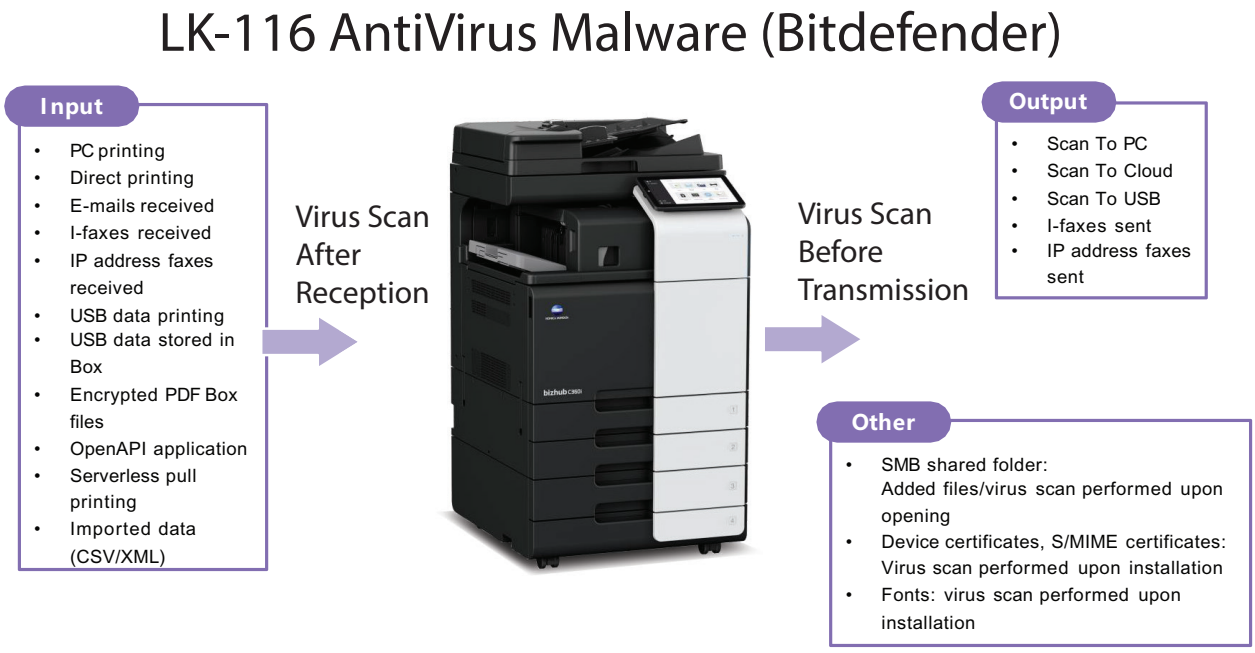
LK-116 AntiVirus and Malware (Bitdefender)

In today's environment, MFPs are essential document distribution devices. They have become a business-critical shared data resource that can be located anywhere — public areas, within a department, in an office, etc. — and may be housed in secure or non-secure areas. They contain sensitive, confidential and private information — exactly what hackers are looking to extract from every possible target they can access.

The infamous worldwide WannaCry ransomware cyber attack was aimed at computers running Microsoft Windows and the DarkHotel spyware targeted business hotel visitors through the hotel's in-house Wi-Fi. These are two very prominent examples of the potential for cyber attacks and must be taken seriously.

The statistical* threats in the office environment are alarming. A hacker attack takes place on an average of every 39 seconds. Every single day sees approximately 230,000 new malware threats, a staggering number that is expected to continue to grow. Worldwide, three quarters of all companies have felt the consequences of such hacker attacks, resulting in the loss of critical business data and applications as well as the inability to access their computer center for days.

Konica Minolta continues to set the bar as a leader in MFP device security by introducing true Antivirus and Malware protection.



FIPS (FEDERAL INFORMATION PROCESSING STANDARD) PUBLICATION 140-2

The Federal Information Processing Standard (FIPS) Publication 140- 2, is a U.S. government computer security standard used to accredit cryptographic modules. It is a benchmark that describes US Federal government requirements that IT products should meet for sensitive, but unclassified use. The criteria was published by the National Institute of Standards and Technology (NIST). It is administered under the umbrella of the Cryptographic Module Validation Program (CMVP).

The certification ensures that the cryptographic modules contained in bizhub MFP's are the highest levels and meet US Government Regulatory compliance. Konica Minolta is one of the only MFP manufacturers who has obtained FIPS 140-2 certification for their products.

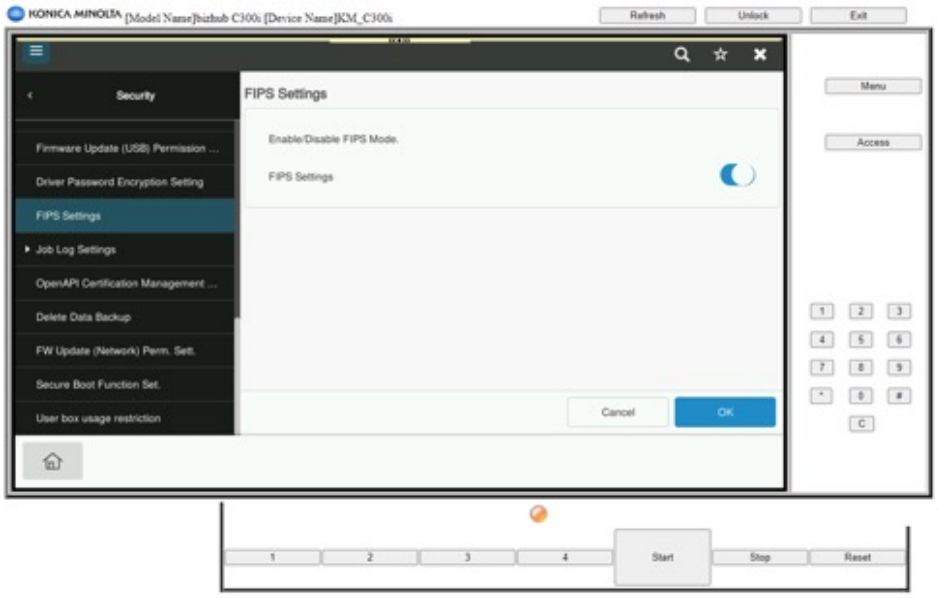
Encryption and the authentication function has been attained by the using the standard embedded Encryption modules, such as OpenSSL/MES.

The following encryption functions are FIPS 140-2 certified on the latest bizhub office models.

1. Encrypted communication at the time of sending scanned data from the bizhub MFP
    - Scan to WebDav over SSL
    - Scan to WebDav function is encrypted by using SSL has FIPS 140-2 certification
    - Scan to email encryption

    At the time of S/MIME transmission of Scan to Email from the MFP

2. PDF encryption file generating function
    - The MFP can encrypt the scanned PDF image prior to transmitting the file as an email attachment or to a shared folder. The PDF encryption is FIPS 140-2 certified.
    - Our certificate is available upon request.



MFP AUDIT LOGS

Many Konica Minolta bizhub systems contain electronic job logs that record all print, copy, scan and fax jobs sent to or from the MFP. For example, the bizhub MFP Audit Log records all print jobs sent by named users. The Audit Log records when the job was printed, how many copies, the time it was printed, etc.

Supported information in the Job Log include:

- User ID
- Time & Date of event
- Job Number
- Job ID
- Job Name
- Scan Destination
- Number of Pages

In addition, Konica Minolta now offers a new audit trail security feature called.

bizhub SECURE Alert

Nearly all multifunction printers (MFPs) have a fundamental security risk – organizations don't know when a data or document breach occurs. Unauthorized MFP use by authorized users is a key source of data breaches: Organizations don't know who used the MFP for what and when. This leaves these organizations potentially liable for the data breaches that occur at their MFPs. In addition, data breaches at the MFP may expose an organization's important trade secrets and intellectual property information as well as customer, patient, and employee data and personally identifiable information (PII).

With the introduction of bizhub SECURE Alert Konica Minolta MFPs don't have this security risk. bizhub SECURE Alert is powered in conjunction with Prism' DocRecord, an application that automatically processes Konica Minolta MFP activity records. This MFP activity record, Image Log Transfer File (ILTF), is an inherent, built-in feature of nearly all of Konica Minolta MFPs – both A3 and A4 models. The ILTF records all user MFP activity information: copies, prints, scans, emails, and faxes. The ILTF provides both a data file and a PDF of the document of this activity. This data set (activity data file and PDF) is then provided to DocRecord which OCRs (optical character recognition) the documents and then automatically analyzes and categorizes the document looking for specific PII information as defined by the customer, Names, addresses, Social Security number patterns, credit card # patterns, any PII information that requires protection. If a potential breach is detected a notification is sent to all designated personnel for investigation and finally the documents are archived.

Bizhub SECURE Alert provides a full-management interface allowing the user to easily manage MFPs, key words and key data, breach alerts, and much more.

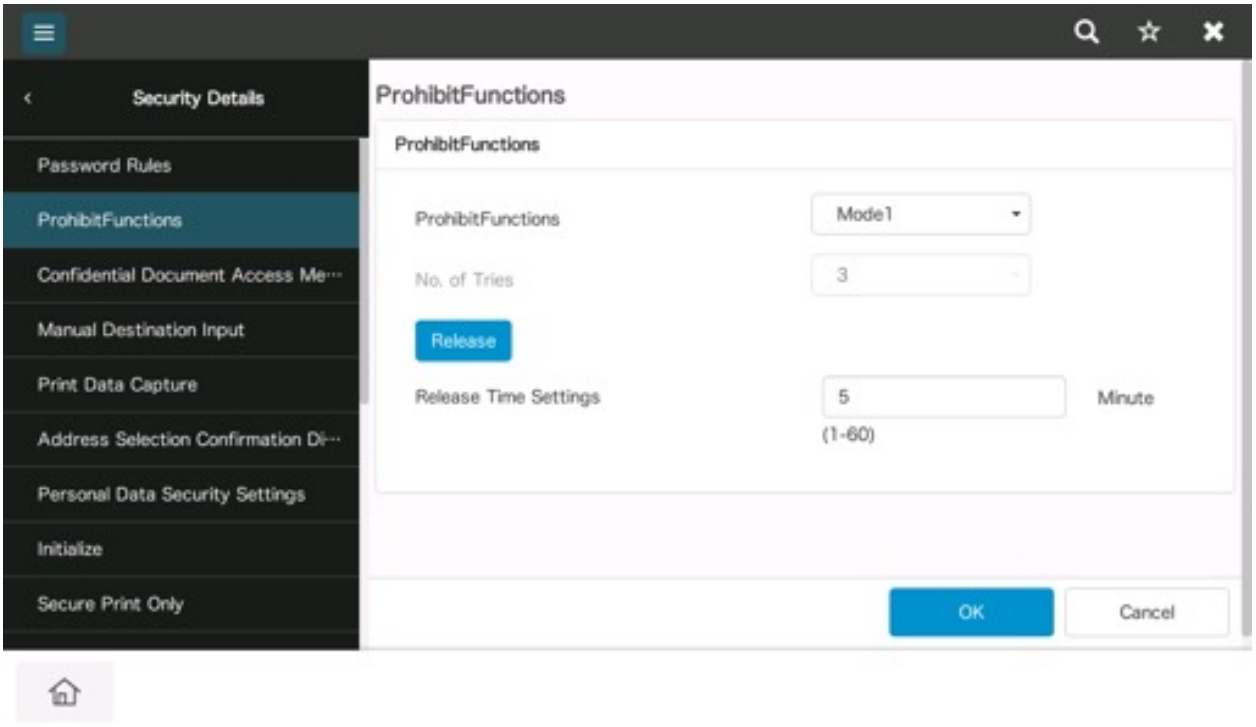
SERVICE MODE/ADMINISTRATOR MODE PROTECTION

The service mode and the administrator mode are protected by passwords or by codes. The service mode is only accessible via a special code that is only known to Konica Minolta certified engineers.

The administrator mode is protected by an eight-digit alphanumeric password. This password can only be changed by the service engineer or in the administration mode itself. This avoids any changes to passwords, destinations or other security- related functions being made by unauthorized users.

UNAUTHORIZED ACCESS LOCK

Like a cash terminal, the MFP can be set to reject a user if they attempt to authenticate with the wrong password. The MFP administrator has the choice of two modes to lock the machine:



Mode 1: The machine lock-out will be released after a certain time (1–60 minutes)

Mode 2: In addition to mode 1, the number of wrong attempts can be specified (1–5)

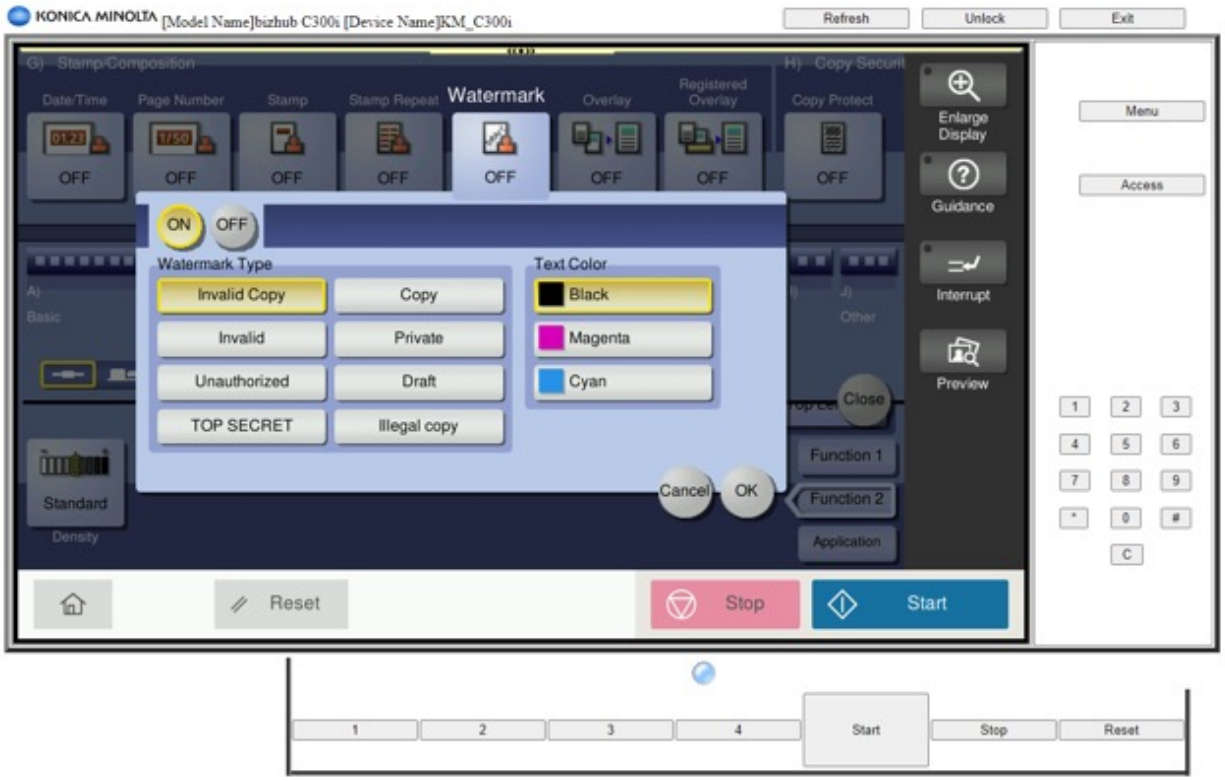
The unauthorized access lock can be extended to the system user box for confidential documents (secure print box). The same modes will be applied in the case of unauthorized access to this document storage location.

DISTRIBUTION NUMBER PRINTING

To index a certain number of printouts, it is possible to print a distribution number on every handout (first page or all pages). This allows the easy identification of illegal copies made of this limited issue of documents.

WATERMARK/OVERLAY

All copies, prints and scans created on the MFP can be marked with a watermark or overlay image. This enables easy and highly visible classification of the document security level. The stamping of the different document types can be set as default by the administrator or individually as required by the user.



COPY PROTECTION VIA WATERMARK

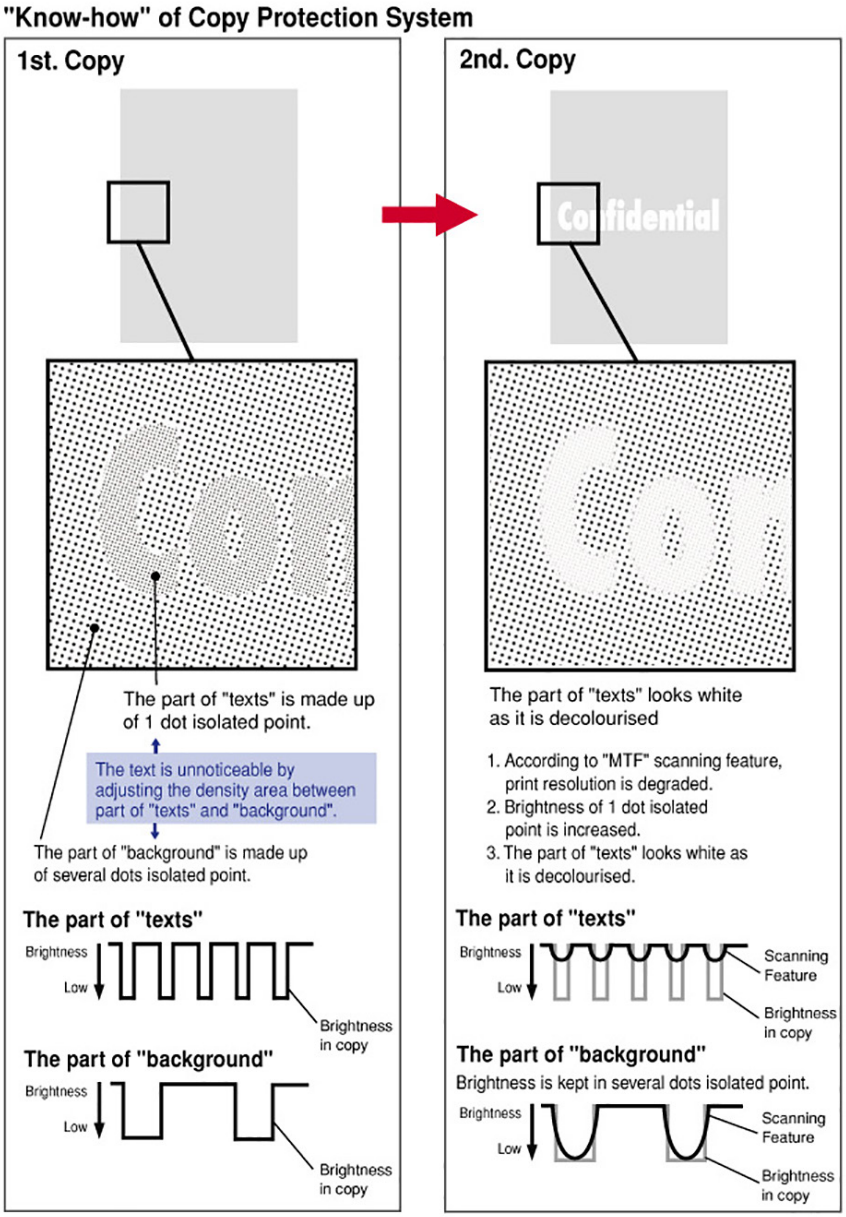
This function adds an invisible pattern to the original printed document. When the original document is copied, the message pattern (e.g. “Copy”) comes up, and clearly distinguishes the copied document from the original one.

In addition to the message, the MFP serial number, as well as the date and time the copy was made, can be set for the pattern. The combination of the information in the pattern and the audit log helps to trace the person who made the illegal copy.

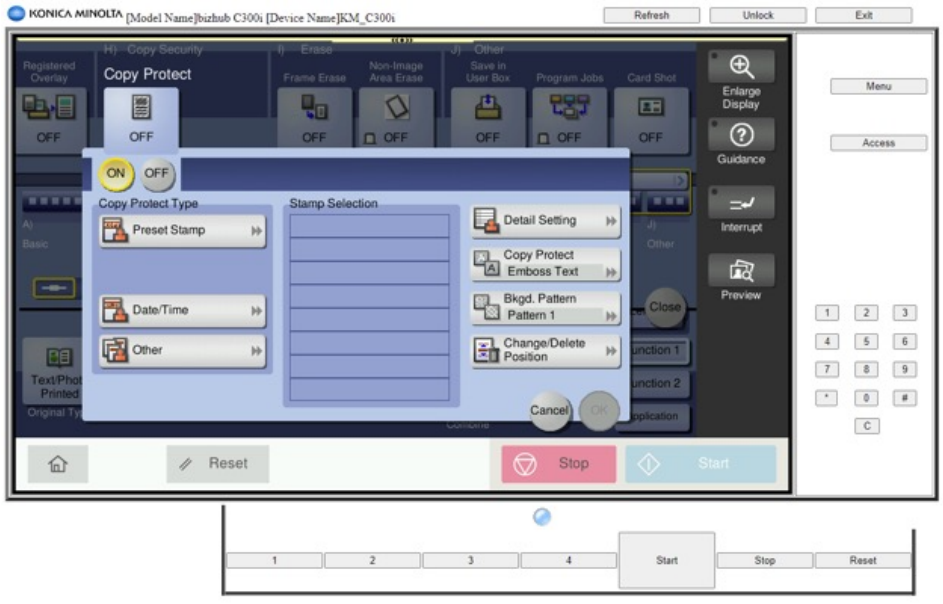
COPY PROTECTION VIA WATERMARK

This function adds an invisible pattern to the original printed document. When the original document is copied, the message pattern (e.g. "Copy") comes up, and clearly distinguishes the copied document from the original one.

In addition to the message, the MFP serial number, as well as the date and time the copy was made, can be set for the pattern. The combination of the information in the pattern and the audit log helps to trace the person who made the illegal copy.



This illustration shows the copy protection functionality.

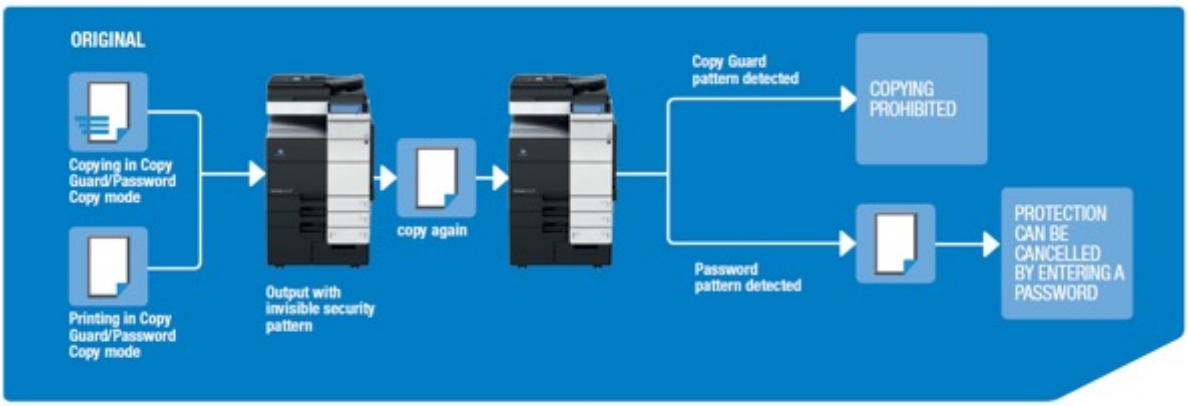


These are examples of the MFP copy security settings.

COPY GUARD FUNCTION / PASSWORD COPY FUNCTION

Many of the Konica Minolta devices could be equipped with a security kit which offers the Copy Guard and Password Copy functions.

These functions allow administrators to embed a security pattern on the output. If a user tries to make a secondary copy of the output, the device will display a message that says "Copying Prohibited" and will prohibit copying. The password copy function allows administrators to set a password so the document can only be copied if the user enters the correct password.



FAX REROUTING

Usually, incoming fax documents are immediately printed by a fax or MFP device. This enables anyone to view the fax document in the output tray. To prevent all unauthorized access to arriving fax documents, it is possible to reroute incoming faxes to a secure location. This could be any destination stored in the MFP address book (email, SMB, FTP or user box). The user box is particularly suited as a destination for confidential fax receipt, and can digitally receive incoming faxes with an F-Code. Besides the fact that digital fax receipt can speed up the fax reception process in general, it completely prevents unauthorized access to fax information, confidential or not.

PKI CARD AUTHENTICATION SYSTEM

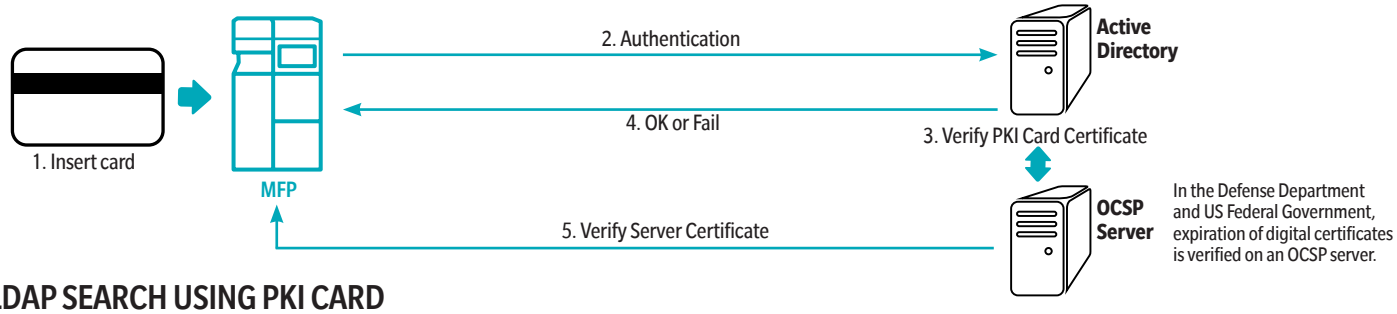
Konica Minolta has incorporated PKI card technology in order to truly harden the MFP or Printer using the two factor authentication requirements of the PKI solution. PKI card technology is a requirement when placing MFP devices in a US Government agency or the DoD but more and more customers outside of the typical government like financial, healthcare, etc. are drawn to the top level security provided by a PKI authentication solution.

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.

Konica Minolta supports PKI Card Technology in the private sector as well as US Government, Government Agencies, Department of Defense, Defense Contractors all utilizing PIV, CAC NIPRNET and SIPRNET networks.

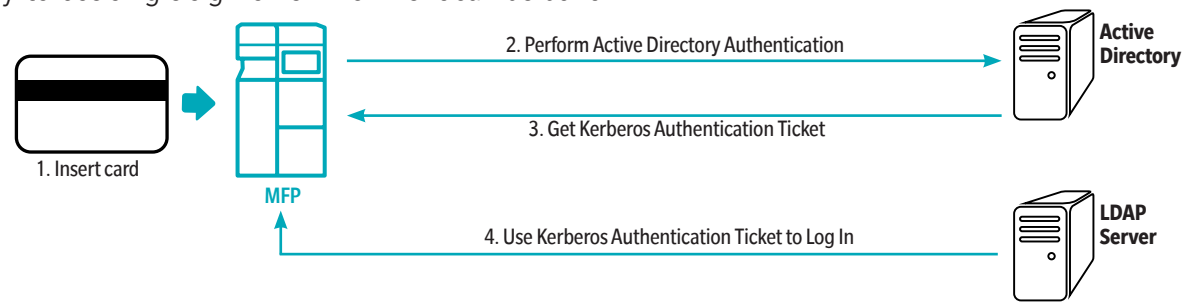
1. LOG-IN USING PKI CARD

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.



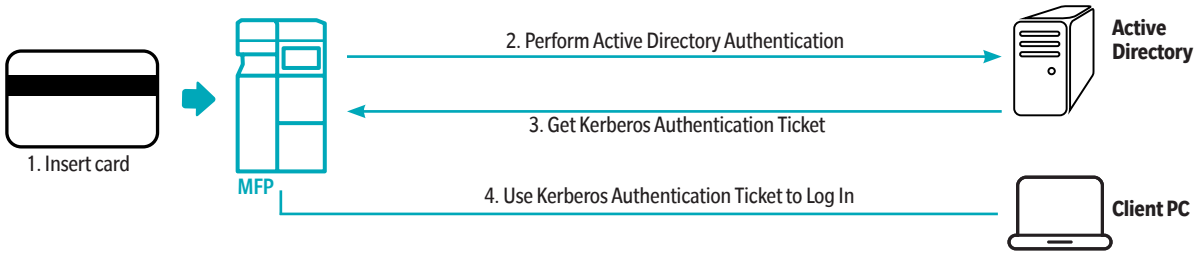
2. LDAP SEARCH USING PKI CARD

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.



3. SMB TRANSMISSION USING PKI CARD

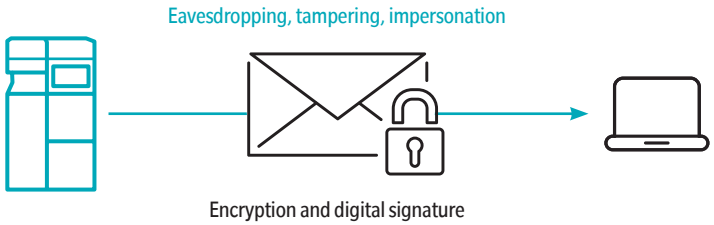
Use the Kerberos authentication ticket acquired from the Active Directory authentication to log into the computer of the address when sending scanned data via SMB. Since it can be accessed with a single authentication, a very easy-to-use single sign-on environment can be built. Moreover, by using the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



4. E-MAIL TRANSMISSION USING PKI CARD (S/MIME)

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

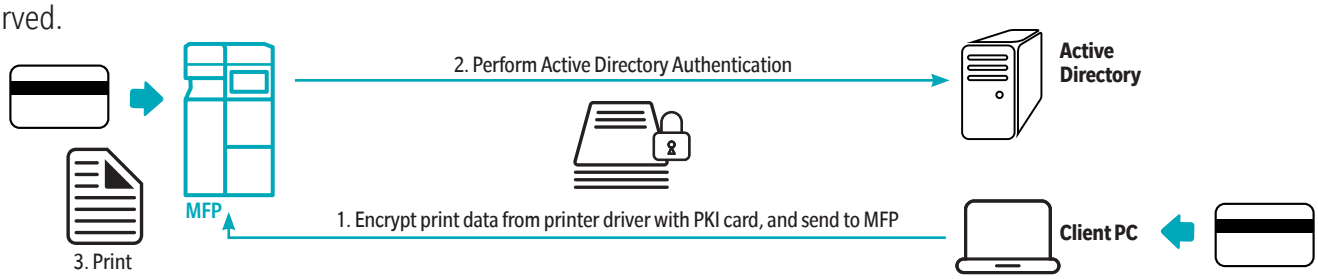
Moreover, if the address certificate is registered, it can be combined with E-mail encryption and sent. By sending the E-mail encrypted, one can prevent information leaking to a third party on the transmission path.



5. PKI CARD PRINT

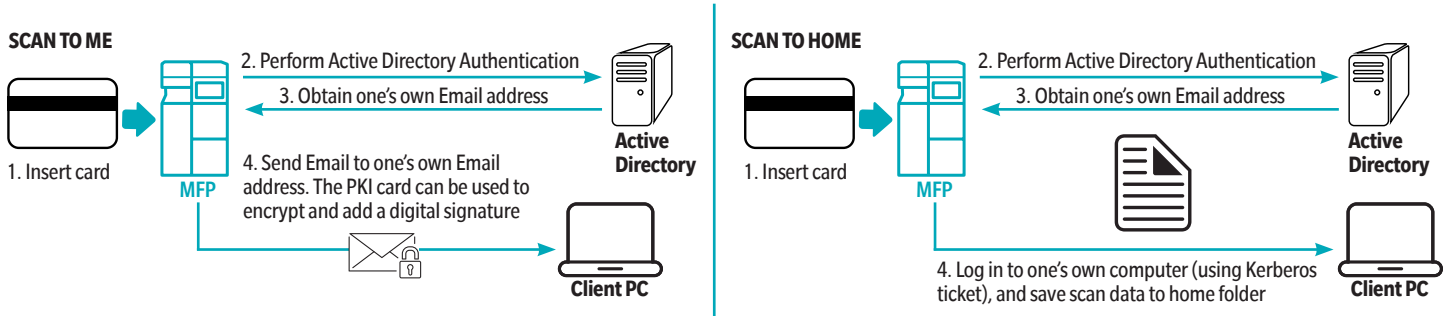
Encrypt print data from the printer driver with a PKI card, and send to MFP. Print data is stored in the PKI encryption box of the MFP, and by the same user performing PKI card authentication with MFP, it can be decrypted and printed.

Since print data can only be printed if authentication by a PKI card on the MFP succeeds, the confidentiality of data is preserved.



6. SCAN TO ME / SCAN TO HOME

This feature allows for sending scanned data to one's own email 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.



KONICA MINOLTA BUSINESS SOLUTIONS U.S.A., INC.
100 Williams Drive, Ramsey, New Jersey 07446

CountOnKonicaMinolta.com

Revision 1.4 10/29/2021

10/21-P