

FUNDAMENTALS OF SECURITY



FUNDAMENTALS OF SECURITY: A GUIDE FOR BUSINESS SOLUTIONS

This fundamentals of security guide is a “living” document – this means it is continually updated. This guide is intended solely for the use and information of Konica Minolta Business Solutions U.S.A., Inc., its subsidiaries and distributors, and their employees. The information herein was obtained from various sources that are deemed reliable by all industry standards. To the best of our knowledge, this information is accurate in all respects. However, neither Konica Minolta nor any of its agents or employees shall be responsible for any inaccuracies contained herein.

Table of Contents

Security without sacrifice02

Konica Minolta security standards02

Cause for concern everywhere – security vulnerability02

Access control/Access security02

Document security/Data security02

Network security02

General system security03

Protection against virus from USB memory.03

Security for fax line.....03

Security of remote diagnostic services03

Security of RAM.....03

Password handling03

Access control04

Copy/print accounting.....04

User authentication – ID and password04

User authentication – Finger vein scanner ..04

User authentication – IC card reader05

Auto log off05

Function restrictions.....05

Secure print (lock job).....06

Touch & Print/ID & Print06

User box password protection.....06

Event log.....07

Driver user data encryption07

Password for non-business hours.....07

Data security07

Hard disk password protection.....07

Data encryption (hard disk).....08

Hard disk data overwrite08

Temporary data deletion.....09

Data auto deletion09

Network security09

IP filtering09

Port and protocol access control.....09

SSL/TLS encryption (https)10

IPsec support10

IEEE 802.1x support.....10

NDS authentication.....11

OpenAPI communication11

Remote panel11

Scan security12

POP before SMTP.....12

SMTP authentication (SASL).....12

S/MIME.....12

Encrypted PDF12

PDF encryption via digital ID13

PDF digital signature.....13

Manual destination blocking13

Address book access control.....13

Additional security functions.....14

bizhub SECURE14

Federal Information Processing

Standard Publication 140-214

MFP Audit Logs14

Service mode/administration

mode protection15

Unauthorized access lock.....15

Distribution number printing.....15

Watermark/Overlay15

Copy protection via watermark15

Copy Guard function/

Password Copy function.....16

Fax rerouting.....16



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 in our multi-functional 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 Europe is ISO 15408, also known as Common Criteria certification. Konica Minolta has newly introduced multi-functional bizhub products validated to Common Criteria EAL3 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 companies look for today. With the CC certification users can rest assured that on Konica Minolta's multi-functional devices their confidential data remains confidential.

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).

ISO 15408 certification and IEEE P2600.1/P2600.2 protection profile for hard copy devices.

It is important to note that the P2600 specification has been dropped by NIAP. A new specification for MFPs is expected by the end of 2014.

Konica Minolta MFPs will continue to achieve ISO 15408 Common Criteria certification at EAL 3+ together with IEEE P2600.1.

ISO 15408 is divided into seven levels of EAL (Evaluation Assurance Level) certification. Standard off-the-shelf products can only achieve up to EAL4 certification. Most IT-related products are certified at EAL3. A certification lab in Japan tests Konica Minolta products. Konica Minolta certifications and related documentation can be found at the following website:
<http://www.commoncriteriaportal.org>

Cause for Concern Everywhere – Security Vulnerability

Generally MFPs offer a huge range of combined and single functions and choices; therefore they represent a similarly wide range of potential security loopholes. 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 hard disk 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 office devices 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

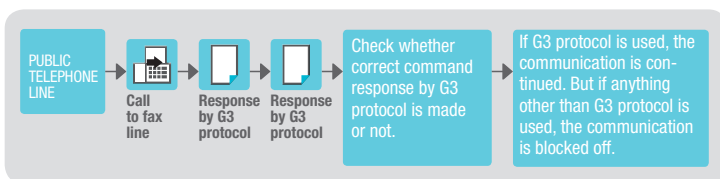
Protection Against Virus from USB Memory

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.

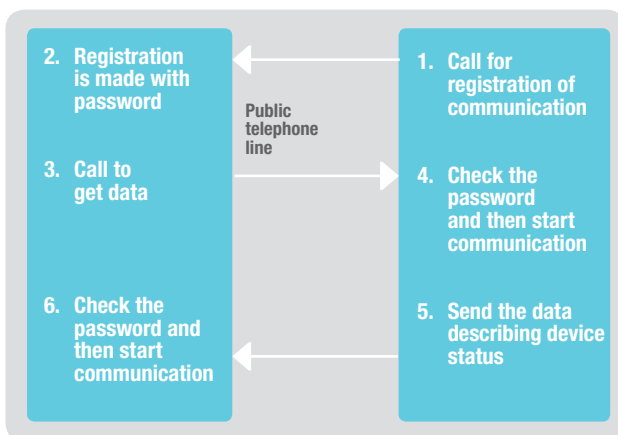
Security for Fax Line

Any communication via fax line uses only fax protocol and does not support any other communication protocol. If someone from outside 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 Remote Diagnostic Services

The remote diagnostic system uses a public telephone line for communication between the Konica Minolta system and the service center. With this system, Konica Minolta devices send main-body data to the service center; and the service center can transmit data to change the main-body settings remotely. An ID preset on every main body and service center ensures that communication is only enabled if the IDs match.



Security of RAM

There are three types of RAM currently used in bizhub products:

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 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 the RAM. Also, as soon as 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 chip will have already been deleted. It is impossible to remove the RAM while the engine power is on. The only other way to possibly extract data would be via an indirect route or a security hole.

These access points are evaluated and tested by independent security consultants before the Konica Minolta products are submitted for ISO 15408 certification. There are no indirect routes or security holes in bizhub MFPs.

Non-volatile RAM (NV-RAM) – typically non-volatile RAM would be:

- counter data
- job settings
- utility settings

The data written to non-volatile RAM is not image or document data, meaning the data is not confidential or private. Unlike volatile RAM this data is not cleared when the power is turned off. It is important to note that when the HDD is formatted, the user/account data in NV-RAM will be deleted and reset to factory default.

Flash memory – typically flash memory is utilized with:

- machine firmware
- control panel data
- printer-resident fonts
- copy-protect watermarks

Flash memory is embedded on an MFP circuit board and cannot be erased. The data stored in flash memory is not critical, confidential or private.

Password Handling

In general, all passwords are handled securely by the MFP following several security rules:

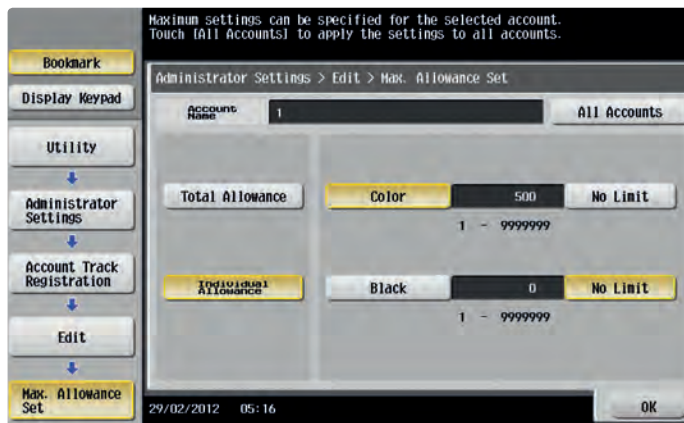
1. Independent of the functionality the setting of a password always has to be verified once.
2. All passwords entered via MFP panel, Web interface or application appear on the screen as “xxx” to prevent illegal copying.

3. All passwords are encrypted for storage.
4. All passwords contain at least 8 to 64 alphanumeric characters. Depending on the MFP functionality, passwords can be even longer.
5. Passwords transferred via a network can always be transmitted encrypted.
6. Passwords for user authentication and user boxes can only be reset by the administrator.
7. Administrator passwords can only be reset by a Konica Minolta certified engineer.

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 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 C654 control panel.

User Authentication - ID and Password

Network

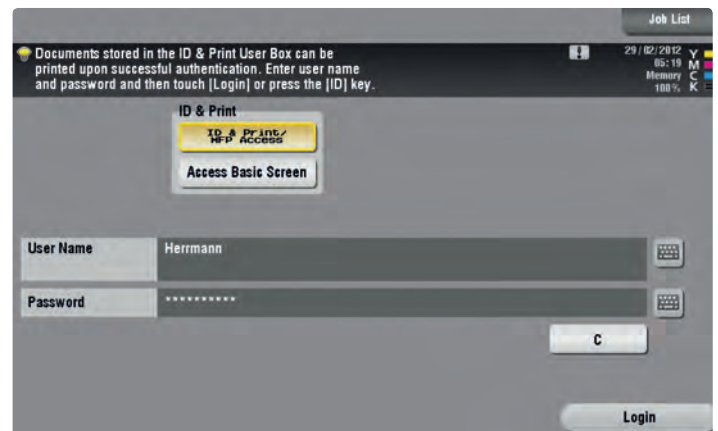
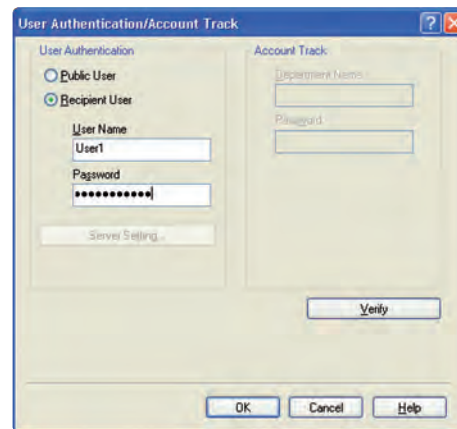
Supported external servers like Active Directory, Novell NDS, NTLM v.1 and NTLMv.2; a maximum of 64 characters can be utilized. Active Directory can support up to 20 domains.

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 C654 control panel and printer driver.

User Authentication – Finger VeinScanner

Besides authentication via user ID and password, use of a biometric device is also possible. The data for the biometric authentication device, is handled securely and cannot be used illegally.

The vein in the finger as biometric data:

The vein is located within the body and, unlike fingerprints, it cannot be scanned/read without the person noticing. This makes it virtually impossible to forge.

The process implemented in this system:

This system implements the security guideline based on the U.S. Government Biometric Verification Mode Protection Profile for Medium

Robustness Environments (BVMPP-MR) version 1.0*; some of the important security/privacy specifications supported by this system are as follows.



Reconstruction of the biometric data:

The only data registered on the HDD are random numbers calculated on the basis of the feature of the scanned data, and it is theoretically impossible to reconstruct the original vein data from the data in the HDD.

Structure of the data on the HDD:

The structure of the data on the HDD is not made public. This makes it impossible to forge.

Erasing of data in the authentication device:

The data left in the device is encrypted when temporarily stored in the RAM, and is erased after transferring to the MFP.

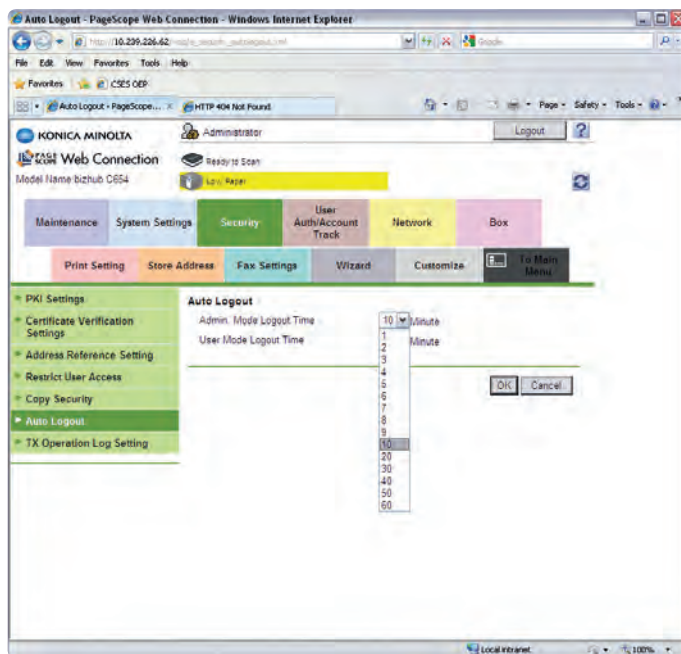
User Authentication – IC Card Reader

As a third authentication solution, Konica Minolta MFPs can be equipped with an IC card reader. The non-contact IC card contains a unique code which is linked in the MFP authentication database to a user ID and password. The biometric data, the IC card code and user information are stored in an encrypted form on the MFP hard disk, and are therefore protected.



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. Some Konica Minolta MFPs can be programmed to reset in as little as 30 seconds. If the machine has the account tracking function enabled the machine 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 (PageScope Web Connection).

Function Restrictions

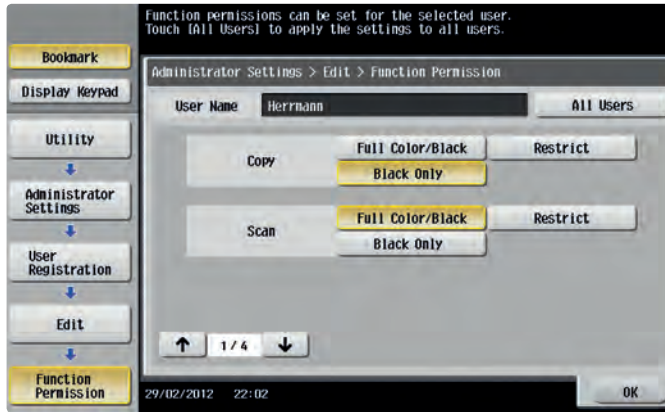
An advanced level of user security allows or prohibits the use and availability of specific machine features. A user and/or administrator can control these features as needed throughout an organization of any size.

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

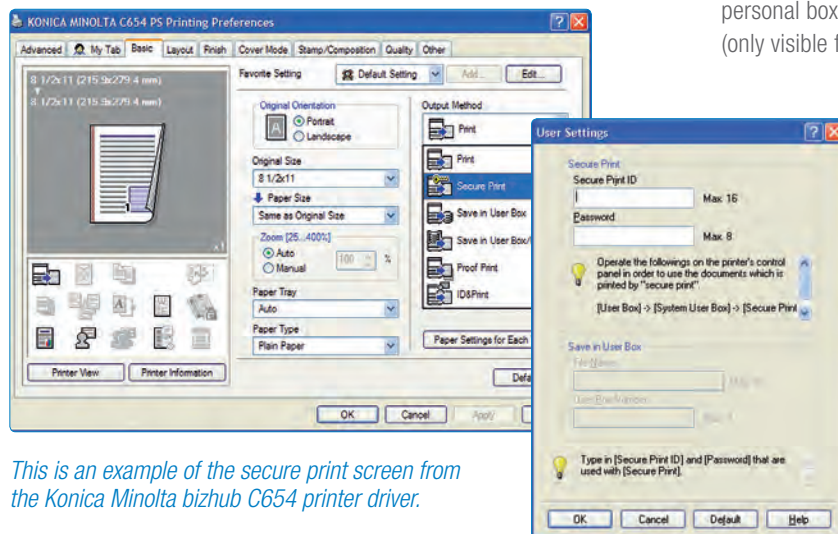
Function restrictions can be set in general either as a walk-up functionality or per user, depending on the user authentication.



This is an example of the function permission screen from the Konica Minolta bizhub C654 control panel.

Secure Print (Lock Job)

Konica Minolta MFPs offer a standard feature called secure printing. This 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 PIN/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 PIN/password is entered on the copier's control panel.



This is an example of the secure print screen from the Konica Minolta bizhub C654 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 authentication data 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 ID and password.

User Box Password Protection

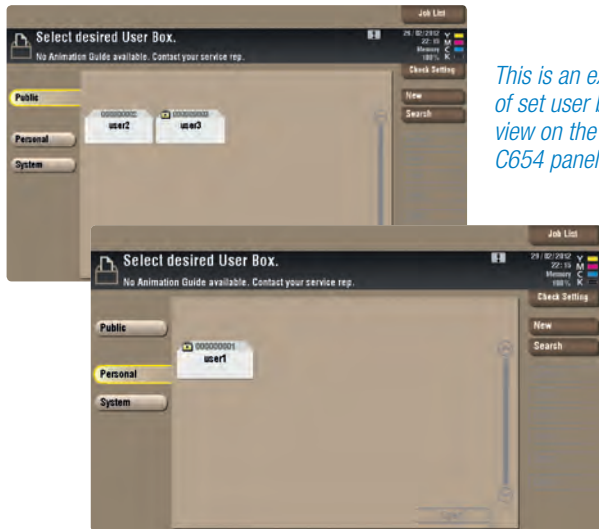
The user box offers the functionality to store commonly used copy, print, scan or fax documents on the hard disk of the MFP. Besides the general security features given to the hard disk, these user boxes can be set with different access levels. On a walk-up MFP the user boxes can be protected by an eight-character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



This is an example of set user box registration on the bizhub C654 panel.

If the MFP is set up with authentication, the user boxes can be set as a personal box (only visible 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 automatically given 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.

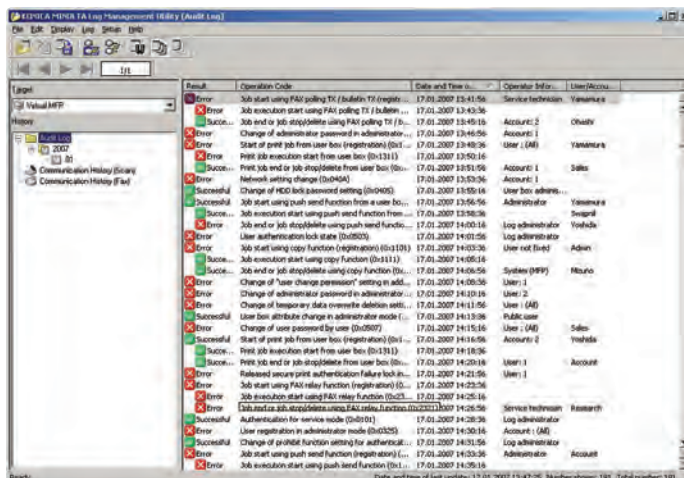


This is an example of set user box view on the bizhub C654 panel.

Event Log

All Konica Minolta MFPs offer the option to record all actions that have happened on the MFP, e.g. 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 PageScope 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.

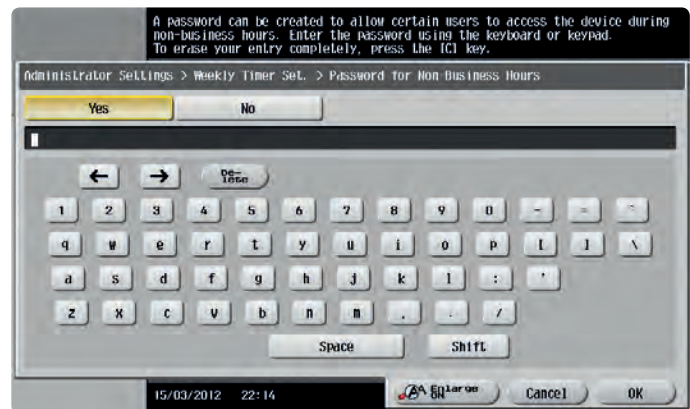
Driver User Data Encryption

For secure printing, print authentication and print accounting it is necessary for the user to input certain information, e.g. 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 time frame", during which the machine can be used as a walk-up device, while outside this period a password is necessary to access the machine.



This is an example of MFP (bizhub C654) password entry during non-business hours.

Data Security

Hard Disk Password Protection

The built-in hard disk of the MFP is automatically protected by a password. This password is stored in the hard disk BIOS and prevents access to the hard disk data, as long as the correct password has not been entered. Therefore, even the removal of the hard disk and installation into a PC,



This is an example of MFP password entry in the administration mode for hard-disk protection (bizhub C654).

laptop or other MFP would not give access to the hard disk. The password is allocated automatically but can be changed by the machine administrator.

Data Encryption (Hard Disk)

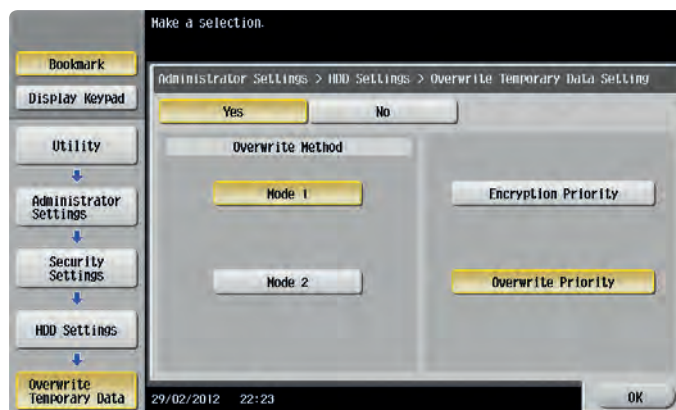
Konica Minolta offers either a standard hard drive encryption kit or an advanced version as an optional extra. If desired, electronic documents can be stored in a password-protected box on the hard drive. If an organization is concerned about the security of such data, this can be protected by encrypting it with the HD encryption kit available. The stored data is encrypted using the advanced encryption standard AES 256 key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.



This is an example of the HDD encryption settings of the MFP (bizhub C654).

Hard Disk Data Overwrite

When equipped with a hard disk drive (HDD), 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 HDD in password-protected boxes. For added safety, a key operator, administrator or technician can physically format (erase) the HDD if the MFP needs to be relocated. The hard drives can be overwritten (sanitized) using a number of different methods conforming to various (e.g. military) specifications, as listed in the table below.



This is an example of the HDD overwrite settings of the MFP (bizhub C654).

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 (NAVSOP-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

Different modes of HDD overwriting.

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

The example shows an MFP panel for hard-disk formatting in administration mode (bizhub C654).

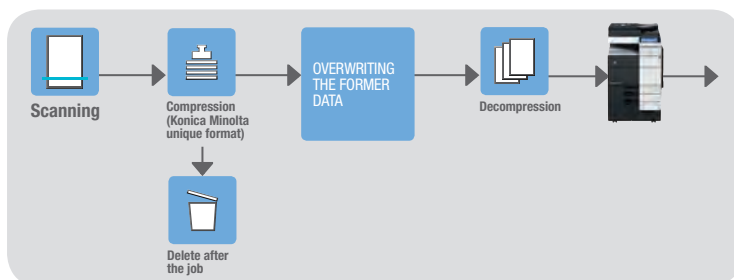


Temporary Data Deletion

Depending on the file size for certain jobs, the MFP might use the hard disk to swap data for copy, scan, print and fax information. As additional security to protect the information stored on the hard disk, 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.

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

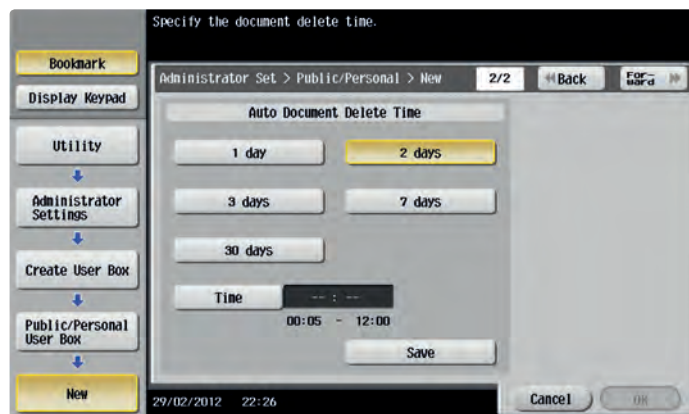
For the temporary data deletion two modes are available.



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

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 time frame selected for deletion.

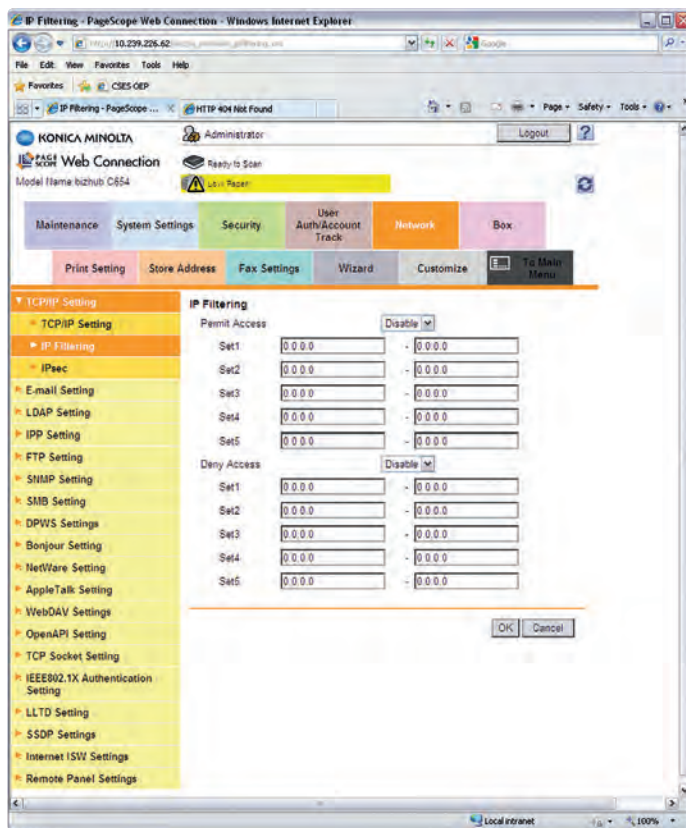


This is an example of the MFP setting for user box document auto deletion (bizhub C654).

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 screen shot illustrates the PageScope Web Connection administrator access to a bizhub C654. 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 123 – NTP	Port 110 – POP3
Port 21 – FTP	Port 161 – SNMP	Port 636 – LDAP
Port 25 – SMTP	Port 389 – LDAP	for TLS/SSL
Port 80 – HTTP	Port 631 – IPP	Port 9100 – PDL

The following protocols can be enabled or disabled:

SNMP, SMB, POP, FTP, SMTP, IPP, Telnet, LDAP, HTTP

SSL/TLS Encryption (https)

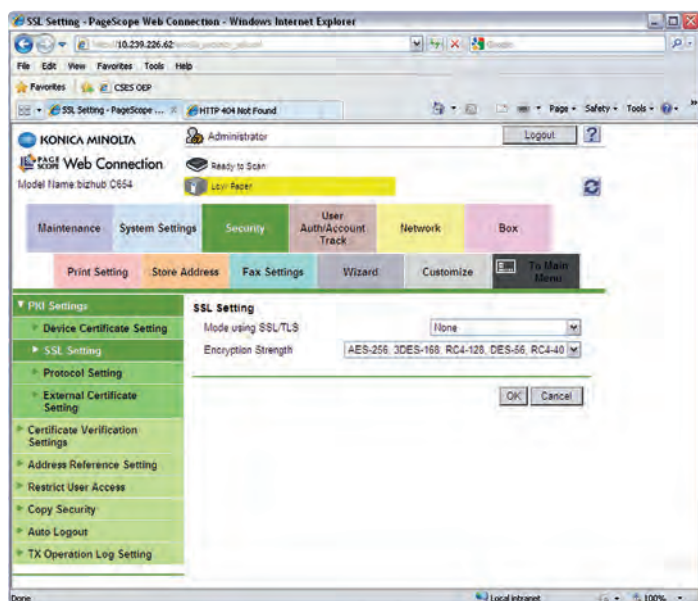
The data communication via network to specific databases or applications can be encrypted by SSL (Secure Sockets Layer) or TLS (Transport Layer Security). Supported versions of encryption are SSL 2.0, SSL 3.0 and TLS 1.0.

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

The MFP allows the programming of an SSL certificate via the administrator mode of PageScope Web Connection.



The screen shot illustrates the PageScope Web Connection administrator access to the security settings for SSL certificates.

IPsec Support

To complete the encryption of any network data transmitted to or from the MFP, the bizhub devices also support IPsec

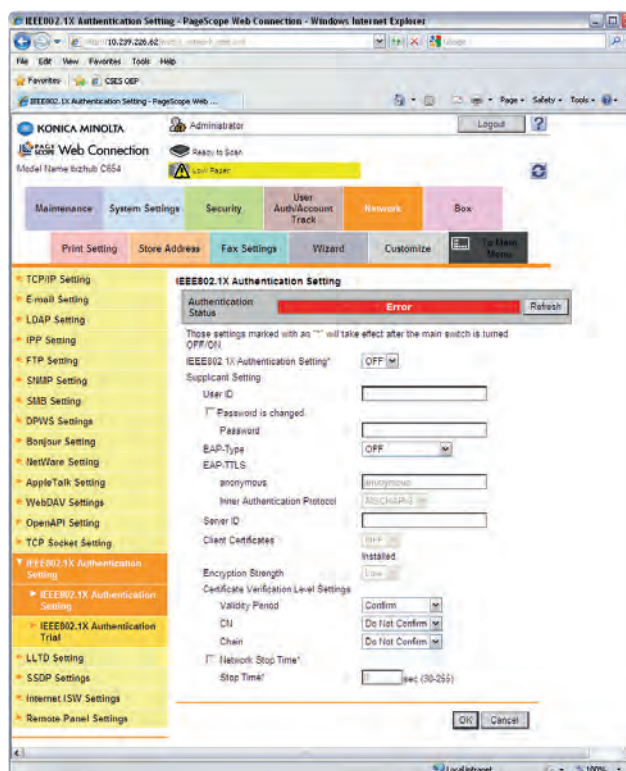
(IP security protocol). This protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself. The IPsec protocol can be programmed via the IKE settings. Up to four groups of IPsec/IKE settings can be stored.



This is an example of MFP IPsec/IKE settings via the MFP panel (bizhub C654).

IEEE 802.1x Support

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



This is an example of the MFP 802.1x authentication settings.

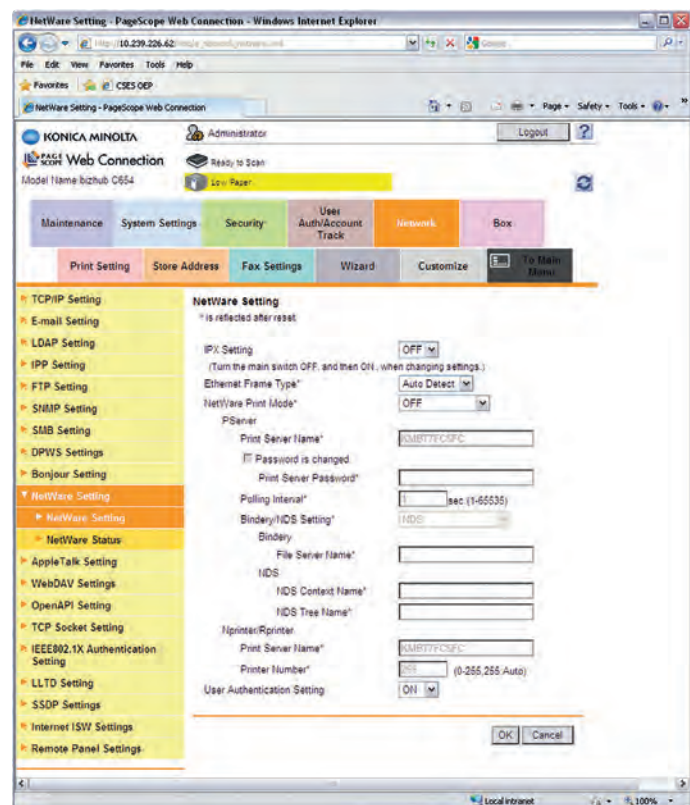
The IEEE 802.1x authentication standard generates a secure network by closing any network communication (e.g. DHCP or HTTP) to unauthorized devices except for authentication requests. This prevents devices gaining access to a network by simply acquiring an IP address via DHCP and, for instance, performing 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.

NDS Authentication

NDS authentication is a method of user identification that performs authentication based on a specified server, an entered user name and password for NDS (Novell Directory Services) running on NetWare 5.1 or later.

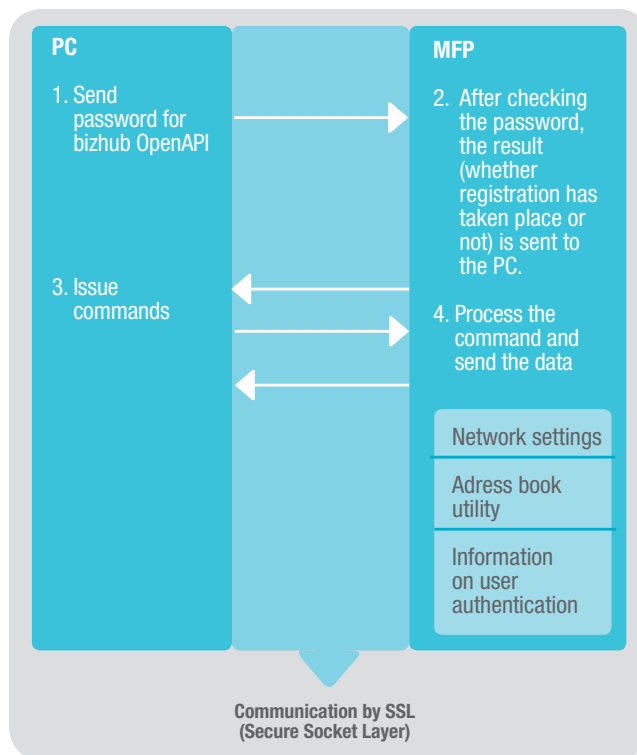
Conventionally, NDS authentication only supported IPX/SPX communication protocols. However, the most recent MFPs also support NDS authentication via TCP/IP. NDS authentication can be performed by specifying either IPX/SPX or TCP/IP protocols. NDS authentication via TCP/IP obtains the IP address of the NDS authentication server by requesting the DNS server for a specified tree and context.



This is an example of the MFP NDS authentication settings.

OpenAPI 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.

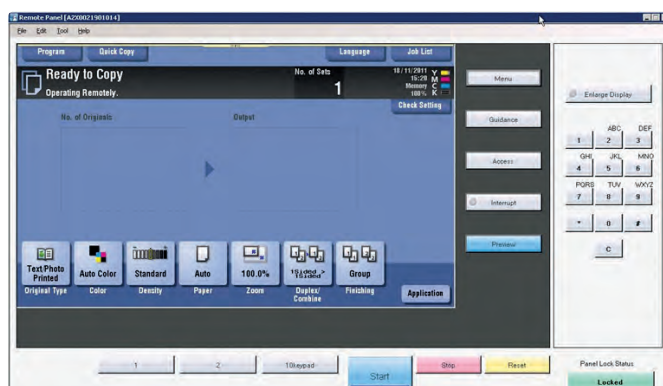


bizhub OpenAPI acquires and sets the data received from devices via networks using the SSL encryption protocol. By using an original password, communication is rendered more secure.

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

Remote Panel

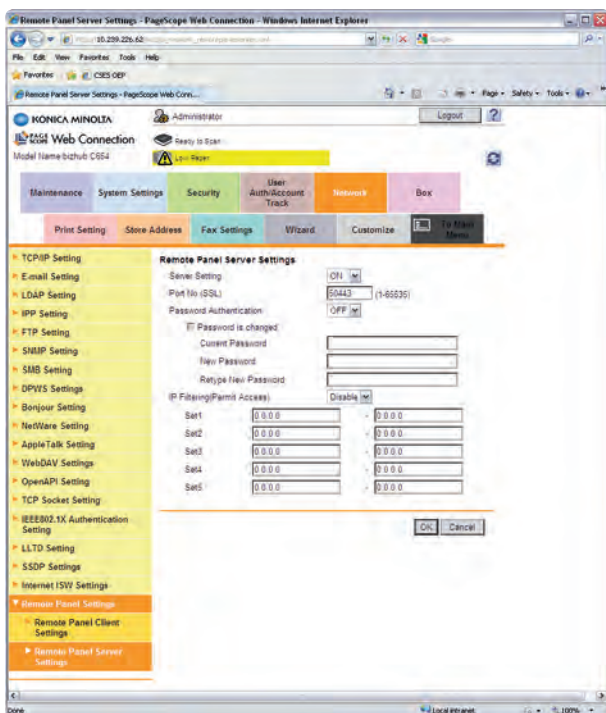
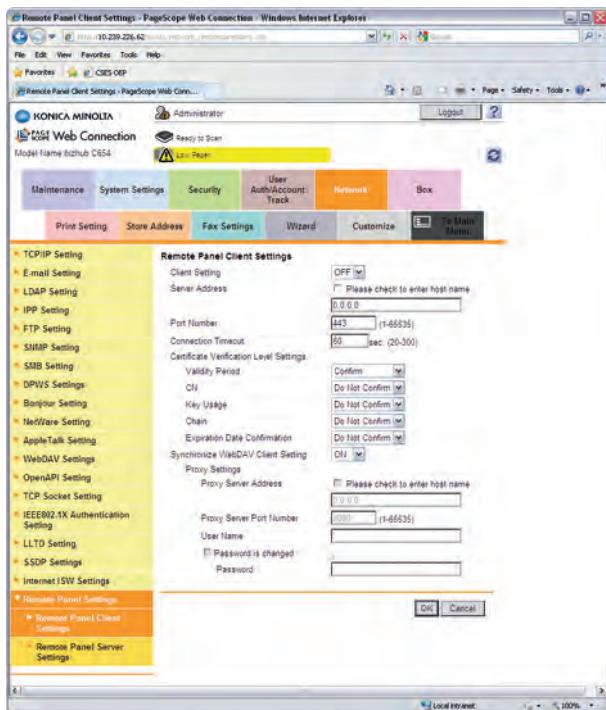
The latest generations of Konica Minolta devices offer the option of a remote panel. This means administrators are able to have real time access to



This is an example of the remote panel on a Web browser (bizhub C654).

the MFP panel remotely, e.g. via a Web browser. Every function which is available on the MFP panel can also be executed remotely.

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



These are examples of the remote panel settings in PageScope Web Connection.

Scan Security

POP Before SMTP

To secure access of 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.

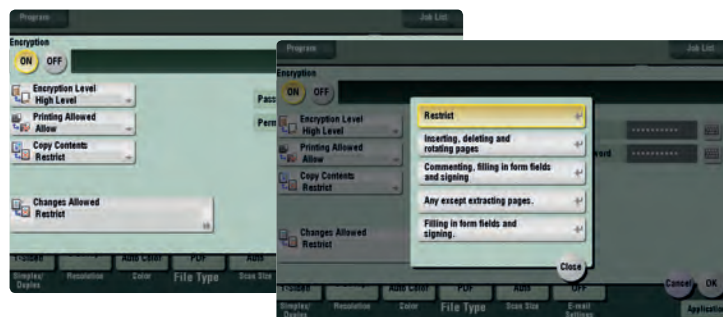
S/MIME

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

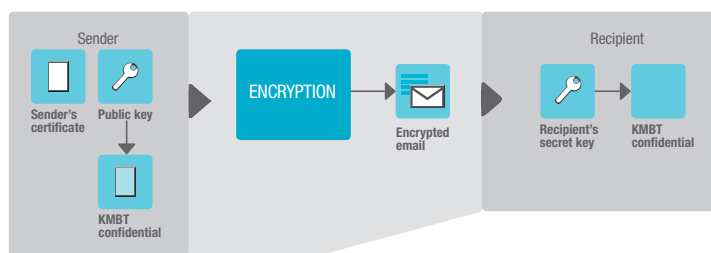


This is an example of the MFP scan settings for PDF encryption (bizhub C654).

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.

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.



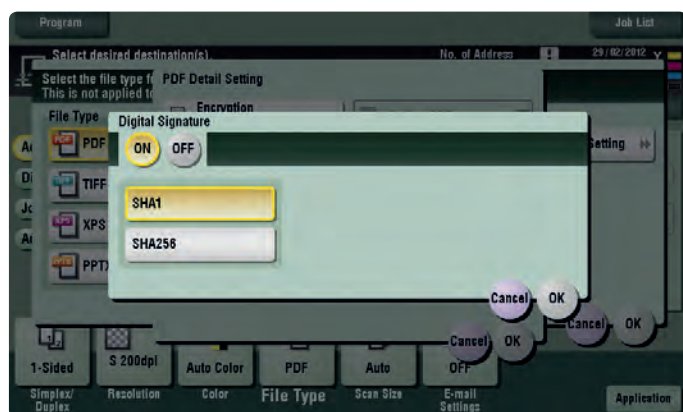
This illustration shows the encryption process via digital ID.

PDF Digital Signature

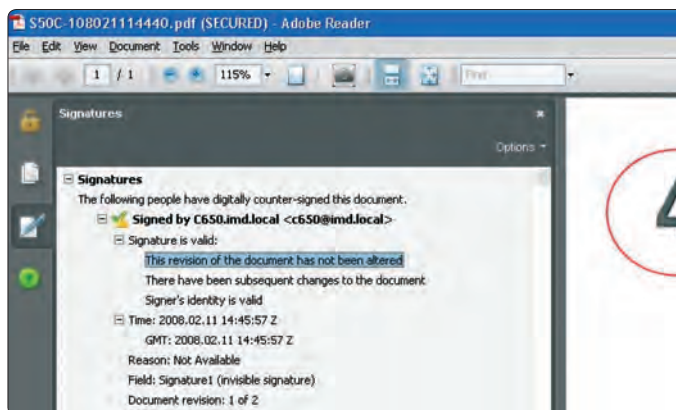
To prevent tampering with MFP-created PDF documents, it is possible to add a digital signature. The digital signature is based on the SSL certificate installed on, or used by, the MFP.

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 is an example of the MFP digital signature settings for PDF files (bizhub C654).



This screen shot 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.

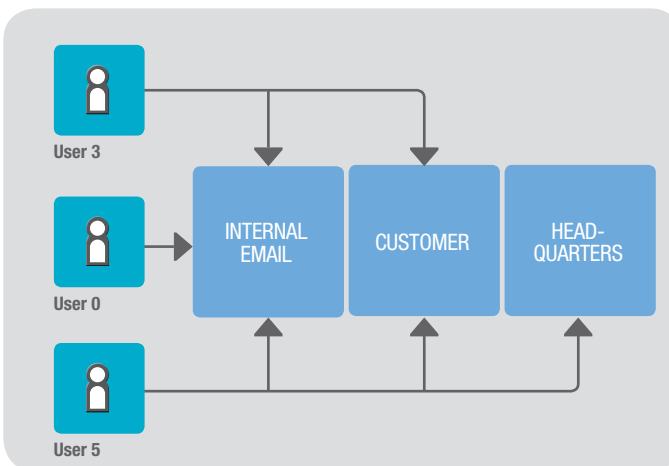
Manual Destination Blocking

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, on the PageScope Enterprise Server or a local email database available via LDAP search.

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 (e.g. email, SMB, FTP) stored in the MFP or PageScope Enterprise Suite 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.



This illustration shows the access levels of different users.

Additional Security Functions

bizhub SECURE

bizhub SECURE is a value added service that Konica Minolta provides on behalf of our clients who do not have the infrastructure or bandwidth to enable and configure the hard drive protection functions detailed in this white paper.



For a nominal charge, we offer this professional security service at the request of our valued customers. Please consult with your Konica Minolta Sales Professional for additional information.

Federal Information Processing Standard (FIPS) 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 Programme (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 (RSA BSAFE Micro Edition Suite).

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 FIP 140-2 certified.
 - Our certificate is available upon request.



MFP Audit Logs

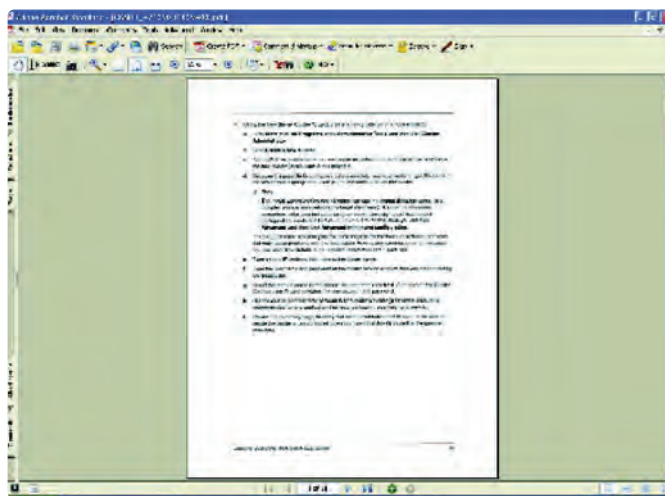
Many Konica Minolta bizhub systems contain electronic job logs that record all print, copy, scan and fax jobs sent to or from the MFP. For example, the bizhub MFP Audit Log records all print jobs sent by named users. The Audit Log records when the job was printed, how many copies, the time it was printed,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

Supported information in the Job Log include:

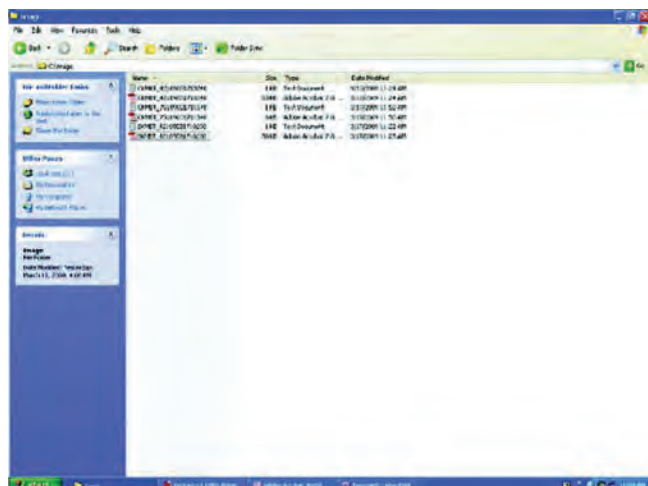
- User ID
- Time & Date of event
- Job Number
- Job ID
- Job Name
- Scan Destination
- Number of Pages

In addition, Konica Minolta now includes a new built-in audit trail security feature in bizhub OP devices called the Image Log Transfer function. With the Image Log Transfer function, you can transfer the image using the Scan-to-FTP or WebDAV process to a registered server at the same time that the device is reading an image in copy mode, reading an image in scan mode, processing a print or image input for FAX RX (reception).

With this setting enabled all documents, whether electronic originals or paper originals are converted to PDF and sent automatically to a registered external server. Here is an example of a scanned job captured and sent to the external log server:



On the next page is an example of the registered location and the two files that are automatically routed to the external server. The text document is the log file, which is associated with the individual pdf image file of the scanned document.



```
Authenticated by External Server
<DeviceInformation>
<PrinterSerialNumber>A0R6011901002</PrinterSerialNumber>
</DeviceInformation>
<JobInformation>
<JobID>923</JobID>
<UserName>david</UserName>
<ExtendedSeverName>Servername</ExtendedSeverName>
</JobInformation>
<ImageInformation>
<SendTime>090323082540</SendTime>
<FileName>CKMBT_42109031809400.pdf</FileName>
</ImageInformation>
```

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.



This image shows the administrator login screen on the MFP panel (bizhub C654).

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:

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.

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)

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

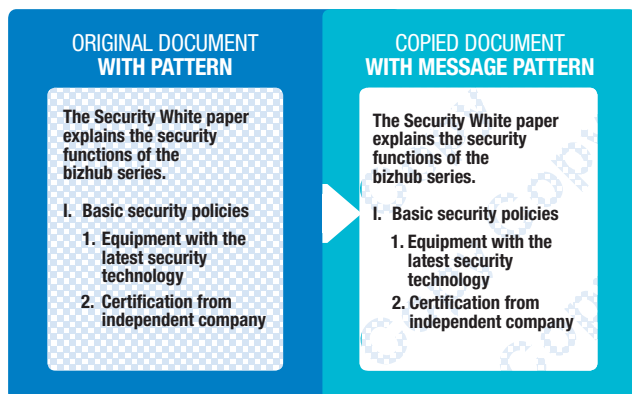
All copies, prints and scans created on the MFP can be marked with a watermark or overlay image. This enables easy and highly visible classification of the document security level. The stamping of the different document types can be set as default by the administrator or individually as required by the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



This is an example of the MFP watermark settings (bizhub C654).

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.



This illustration shows the copy protection functionality.

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.



These are examples of the MFP copy security settings (bizhub C654).

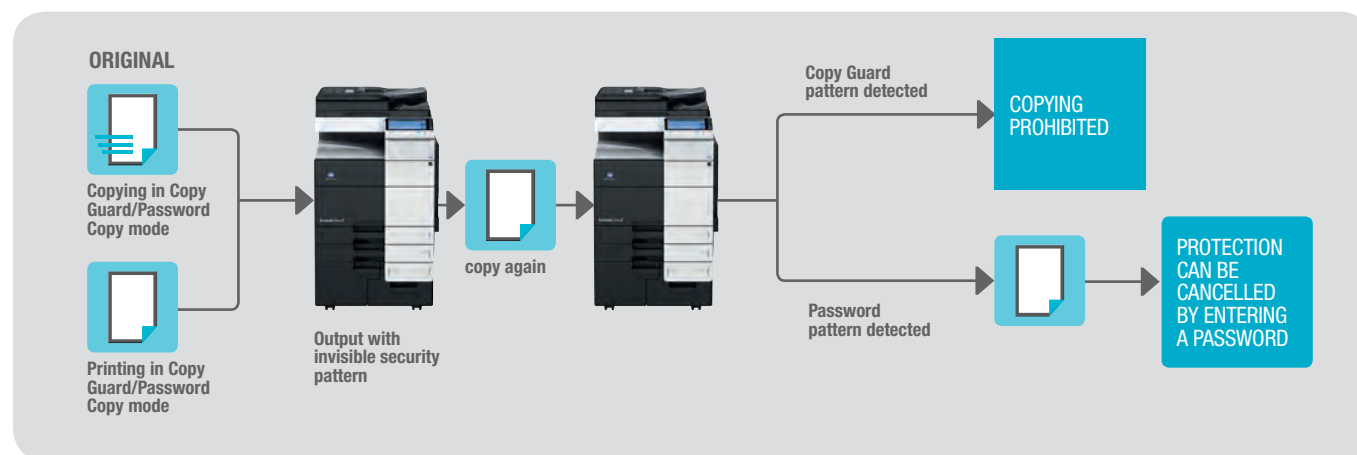
Copy Guard Function/Password Copy Function

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.





Common Criteria Validated

Your Konica Minolta Business Solutions Partner



KONICA MINOLTA

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

CountOnKonicaMinolta.com

