KONICA MINOLTA

The essentials of imaging


# Fundamentals of security

## Whitepaper

Common Criteria Validated

**Information** Security Whitepaper

# Fundamentals of security

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 Europe GmbH, the European Konica Minolta 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.



Some functions may require options, which may or may not be available at the time of launch.

**Konica Minolta**
**Business Solutions Europe GmbH**
Europaallee 17
30855 Langenhagen • Germany
Tel.: +49 (0) 511 74 04-0
Fax: +49 (0) 511 74 10 50
www.konicaminolta.eu

## Contents



**Note:** Some of the security features and options described in this guide may only apply to specific Konica Minolta bizhub models. It is best to refer to the documentation that is provided with every Konica Minolta bizhub MFP to verify exactly which security features are included with a specific product. It is also important to note that a specific machine may require an upgrade to achieve and/or enable some of the features discussed in this document. Please refer to your service representative for further information.

# Introduction

## Security without sacrifice: Konica Minolta security standards

Konica Minolta realised 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 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 Europe is ISO 15408, also known as Common Criteria certification. Konica Minolta has newly introduced multifunctional bizhub products validated to Common Criteria EAL3 security standards. Common Criteria (CC) is the only internationally recognised standard for IT security testing. Printers, copiers and software with the 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 multifunctional devices their confidential data remain confidential.

The Konica Minolta security standards provide protection in more than one respect, securing the network and network access, ensuring secure, authorised 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 the ISO 15408 (Common Criteria).

# What is ISO 15408 **or Common Criteria?**

**To date, the only official security-based certification standard for digital office products is the international standard generally known as Common Criteria. The official international designation for this security standard is ISO 15408.**

**Please refer to the security specification table (back cover) for all Konica Minolta bizhub models that have achieved the ISO 15048 EAL 3 certification, or are currently being evaluated.**

## Common Criteria background

The International Common Criteria for Information Technology Security Evaluation is a relatively new programme, which seeks to establish an internationally agreed-upon language for specifying security functionality, as well as an evaluation methodology to assess the strength of security implementations embedded in various types of technologies located on the network.

In June 1993, the sponsoring organisations of the existing US, Canadian and European criteria started the CC project to align their separate regulations into a single set of IT security criteria. Version 1.0 of the CC was completed in January 1996. Based on a number of trial evaluations and an extensive public review, version 1.0 was extensively revised and version 2.0 was produced in April 1998. This became the ISO International Standard 15408 in 1999. The CC project subsequently incorporated the minor changes that had resulted in the ISO process, producing version 2.1 in August 1999. Today, the international community has embraced CC through the Common Criteria Recognition Arrangement (CCRA) whereby the signers have agreed to accept the results of CC evaluations performed by other CCRA members.

There are seven levels of EAL (Evaluation Assurance Level) certification. Standard off-the-shelf products can only achieve up to EAL 4 certification. Most IT related products are certified at EAL 3.

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/public/consumer/index.php**

Here is the definition of the Konica Minolta data security evaluation for the bizhub C550 that is posted on the Common Criteria portal site mentioned above:

Product description

“This product is the embedded software that is installed on the Konica Minolta Business Technologies, Inc. digital MFP (bizhub C550 / bizhub C451 / ineo+ 550 / ineo+ 451) (hereinafter referred to as ‘MFP’).”

# Security, **General Common Criteria**

This product offers protection from exposure of highly confidential documents stored in the MFP, and aims at protecting the data which may be exposed against a user's intention. In order to realise it, this offers functions such as the function that limits the operation to the specific document only to the authorised user, the function that performs the overwrite deletion of the data domain which became unnecessary, and the function that deletes the confidential information including a setting value. Moreover, this has the mechanism using the unauthorised access protection function (HDD lock function) with which the HDD, which is a medium for storing image data in the MFP, is equipped against the risk of being removed from the MFP unjustly. If the encryption board, an option product, is installed in the MFP controller, this provides the function of generating the encryption key that encrypts all data, including image data written to the HDD."

As you can see, by its nature Common Criteria certification is ambiguous. Hardware and software developers submit their test parameters to a certification lab for testing. The testing lab or the certifying body does not tell the manufacturer what tests need to be performed to achieve EAL 3 certification. For example, EAL 3 does not require any specific security-based function. It is up to the company submitting the product to define the parameters of the evaluation. So, when a vendor submits a product (TOE – target of evaluation and an ST security target) the manufacturer asks the testing lab to verify the accuracy and integrity of the specific security-related functions in the product. As you will see later in this document, Konica Minolta is one of very few vendors to certify the entire system, and not just a kit or specific hard drive erase functionality.

**The security target (ST) and target of evaluation (TOE) have the following definitions:**

- security target (ST): a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE
- target of evaluation (TOE): an IT product or system and its associated administrator, and user guidance documentation that is the subject of an evaluation
- for more information on the subject, please refer to the Common Criteria website: **www.commoncriteriaportal.org/**

# General system security

## System security

Unlike conventional PCs, the controllers built into Konica Minolta products use the operating system VxWorks. It is, therefore, considered extremely unlikely that these controllers might be affected by a virus via the LAN.

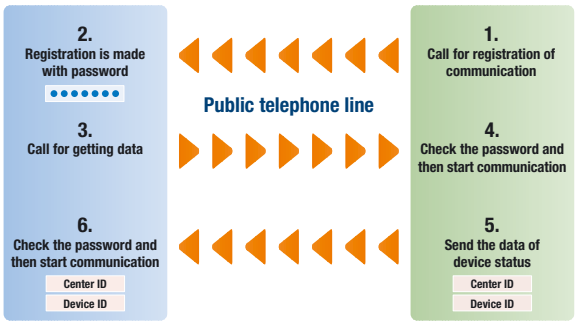
## Security of fax line

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 that kind of 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 centre. With this system, Konica Minolta devices send main-body data to the service centre; and the service centre can transmit data to change the main-body settings remotely. An ID preset on every main body and service centre 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 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 an indirect route or a security hole. These access points are evaluated and tested by third-party security consultants before the Konica Minolta products are submitted for ISO 15408 certification. There are no indirect routes or security holes present 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 set back to factory default.

**Flash memory – typically flash memory is utilised 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 are written with “xxx” to prevent illegal copying.
3. All passwords are encrypted for storage.
4. All passwords contain at least 8 to 64 alphanumeric digits. Depending on the MFP functionality, passwords can be even longer.
5. Passwords transferred via 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 standard with the ability to enable account tracking. 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 authorised PIN (from the print driver), the print job submitted will not be printed. If a user does not enter an authorised PIN at the copier control panel, he 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.

**This is an example of the accounting screen from the Konica Minolta bizhub C550 control panel:**


## User authentication (ID and password)

**User authentication is a function that will prevent unauthorised users from accessing the network or machine. This feature requires a user ID and a password, and can be configured to authenticate to the network or locally at the machine.**

**Network**

- Supported external servers like Active Directory, Novell NDS, NTML v.1 and NTLMv.2; a maximum of 64 characters can be utilised. Active Directory can support up to 20 domains. In addition, the authentication can be centrally managed via PageScope Enterprise Suite Authentication Manager.

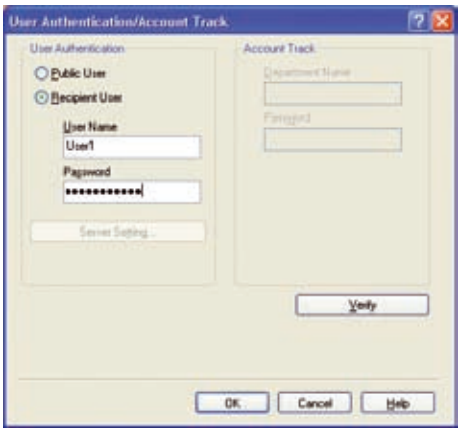
**Machine**

- Internal authentication at the machine can support up to 1,000 user accounts. Passwords can have up to eight alpha-numeric 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.

**This is an example of the authentication screen from the Konica Minolta bizhub C550 control panel and printer driver:**

## Finger vein scanner

**Besides the authentication via user ID and password, the user can authenticate via a biometric or IC-card-based device (see below for IC card). The data for the biometric authentication device, AU-101 and AU-102, is handled securely and cannot be used illegally.**

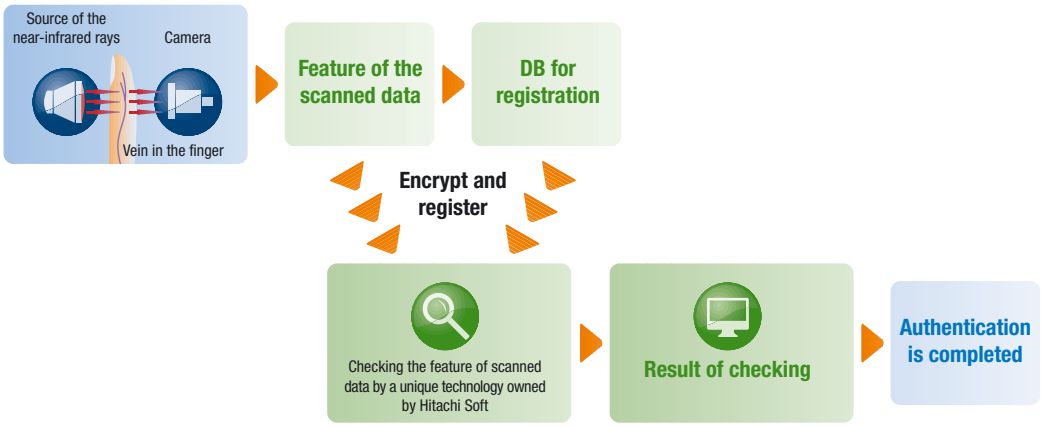
- **The vein on the finger as biometric data:**
  The vein is located in the body and, unlike fingerprints it can not be scanned/read without the person noticing. This makes it virtually impossible to forge.

- **The process implemented in this system:**
  This system implements the security guideline based on 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 based on 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.



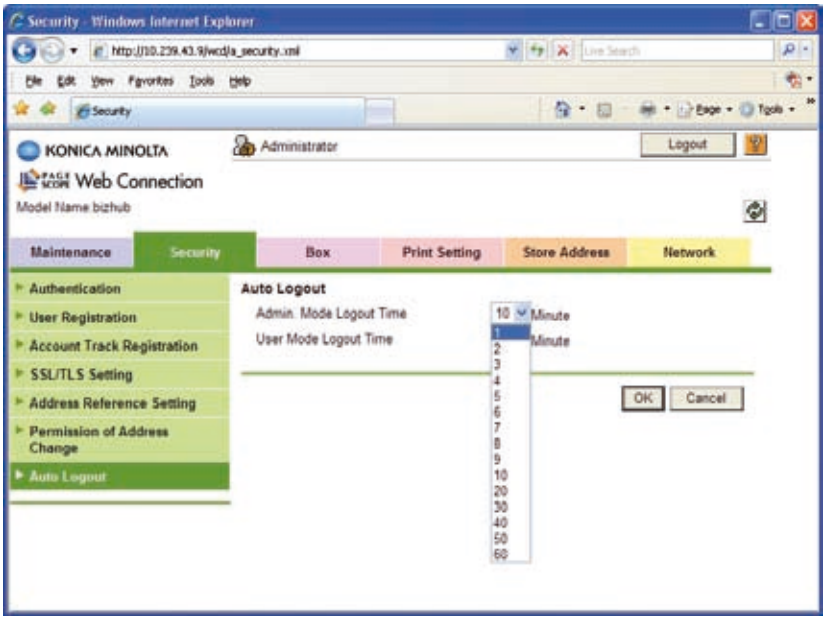

## IC card reader

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

As an alternative to storing authentication data on the MFP hard disk, authentication data can be centrally provided via the PageScope Enterprise Suite Authentication Manager.

## 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 preprogrammed 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

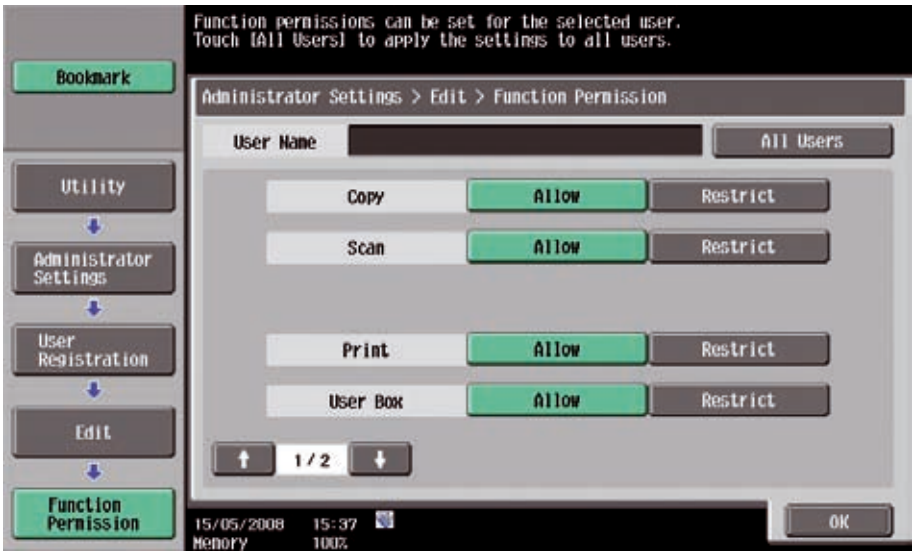
An advanced level of user security allows or prohibits the use and availability of specific machine features.
A user and/or administrator can control these features as needed throughout an organisation of any size.

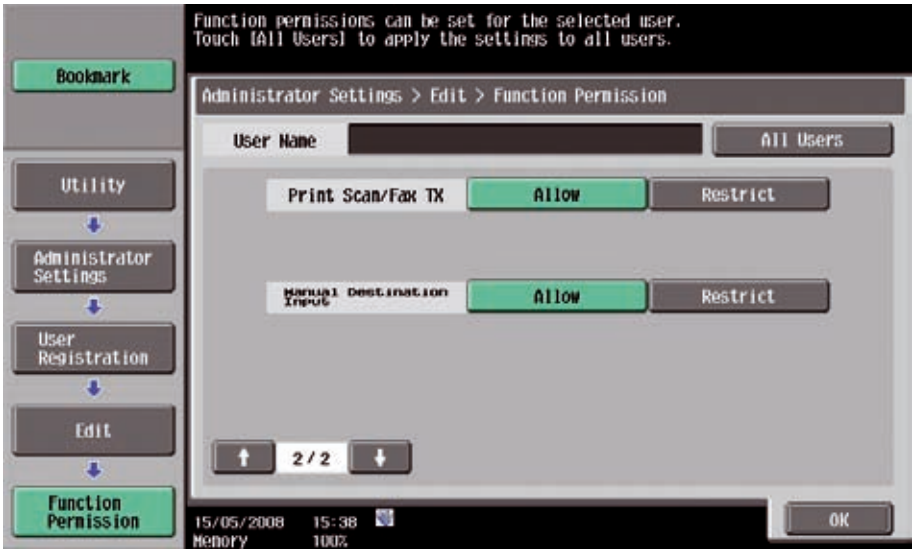
**The specific features are:**

- 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 colour copying or neither b/w nor colour 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 colour printing or neither b/w nor colour printing

Function restrictions can be set in general as 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 C550 control panel:**

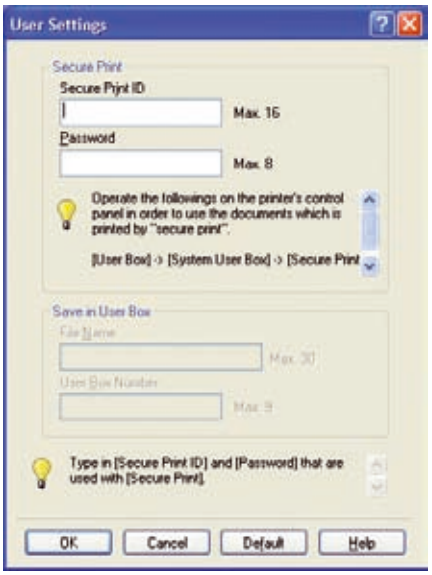


## Secure print (lock job)

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 authorised 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 C451 printer driver:**


## Touch & print / ID & print

In case 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.

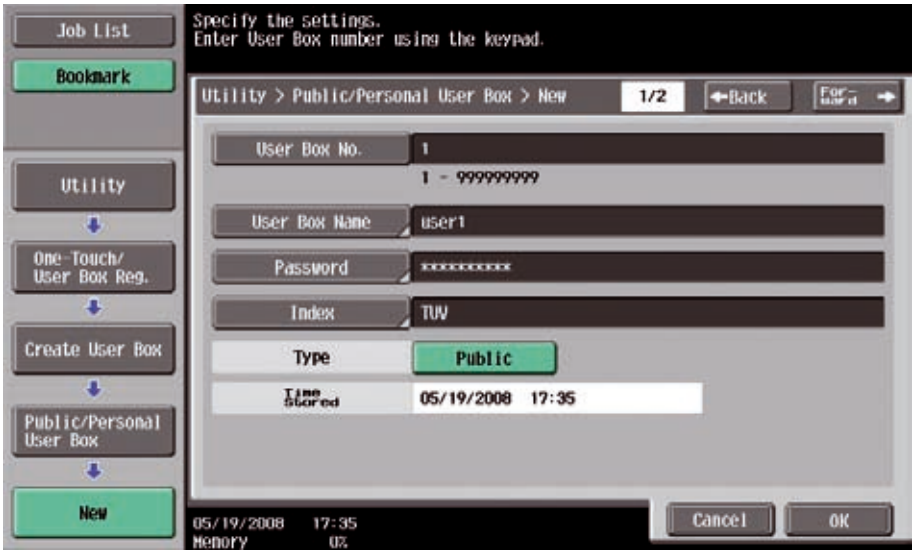
Touch & print is based on an authentication via finger vein scanner or IC card reader.
ID & print is based on the user authentication via ID and password.

## 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-digit alphanumeric password.

In case the MFP is set up with authentication, the user boxes can be set as 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 boxes. 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 chance to hack into it by trying out passwords.

**This is an example of set user box registration and user box view on the C550 panel. For this example, the machine is not set up with authentication but as a walk-up MFP:**

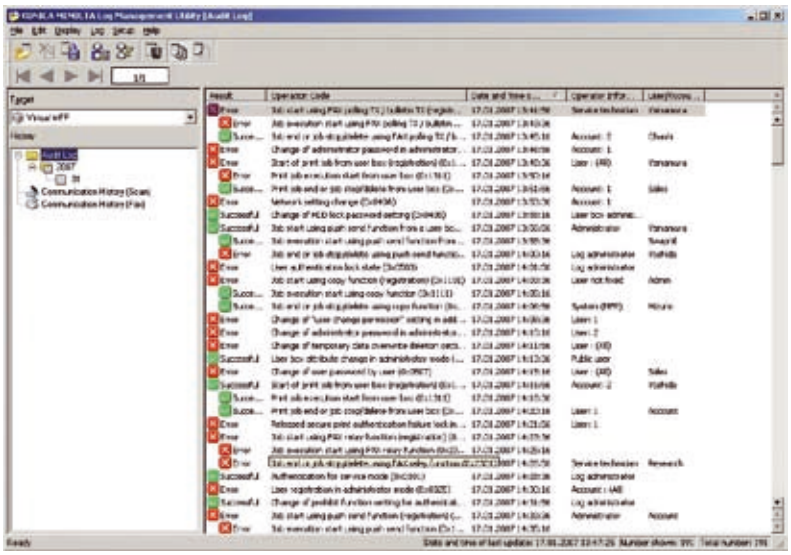



## Event log

All Konica Minolta MFPs offer the possibility 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 view:**



## 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. In case 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

In case an MFP is not set up with user authentication but used as walk up device, basically everybody has the possibility to access the machine and print/send data that is not safe. To prevent this happening, the administrator can program a so-called business timeframe, during which the machine can be used as walk up device, while outside this period a password is necessary to access the machine.

**This is an example of MFP 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, 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.

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


## Data encryption (hard disk)

Konica Minolta offers an optional or standard hard drive encryption kit. If desired, electronic documents can be stored in a password-protected box on the hard drive. If an organisation is concerned about the security of such data, this can be protected by encrypting it with the HD encryption kit available. The stored data are encrypted using the advanced encryption standard (AES) supporting 128-bit key size. Once a HDD is encrypted its data cannot be read, even if the HDD is removed from the MFP.

## 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 (sanitised) using a number of different methods conforming to various (e.g. military) specifications, as listed in the table below.

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

| Mode | Overwrite method compliance |
|---|---|
| Mode 1 | Overwrite with 0x00Japan Electronic & Information Technology Association<br>Russian Standard (GOST) |
| Mode 2 | Overwrite with random 1 byte numbers Current National Security Agency (NSA) standard<br>Overwrite with random 1 byte numbers<br>Overwrite with 0x00 |
| Mode 3 | Overwrite with 0x00National Computer Security Center (NCSC-TG-025)<br>Overwrite with 0xff US Navy (NAVSO P-5239-26)<br>Overwrite with random 1 byte numbers Department of Defense (DoD 5220.22M) |
| Mode 4 | Overwrite with random 1 byte numbers Army Regulations (AR380-19)<br>Overwrite with 0x00<br>Overwrite with 0xff |
| Mode 5 | Overwrite with 0x00Former NSA Standard<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff |
| Mode 6 | Overwrite with 0x00North Atlantic Treaty Organization – NATO Standard<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 512 bytes of specified data |
| Mode 7 | Overwrite with 0x00German Standard (VISTR)<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 0xaa |
| Mode 8 | Overwrite with 0x00US Air Force (AFSSI5020)<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 0x00<br>Overwrite with 0xff<br>Overwrite with 0xaa<br>Verified |

**The example shows an MFP panel for hard-disk formatting in the administration mode:**

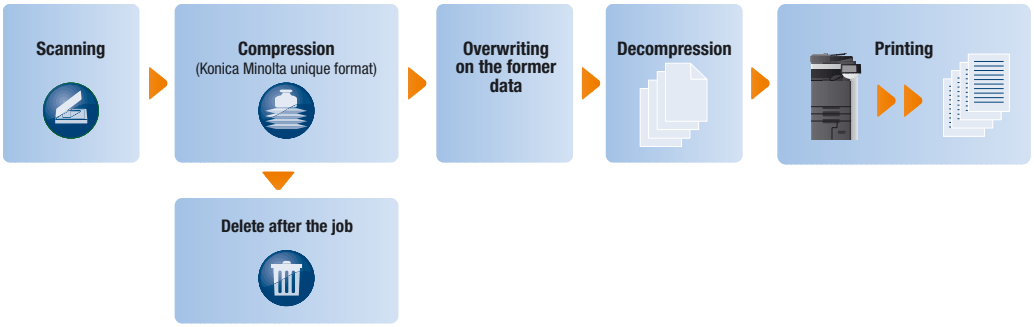
## Temporary data deletion

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.

**For the temporary data deletion two modes are available:**

| Setting | Description |
|---|---|
| Mode 1 | Overwritten with 0x00 |
| Mode 2 | Overwritten with 0x00 → Overwritten with 0xff → Overwritten with the letter “A” (0x61) → Verified |

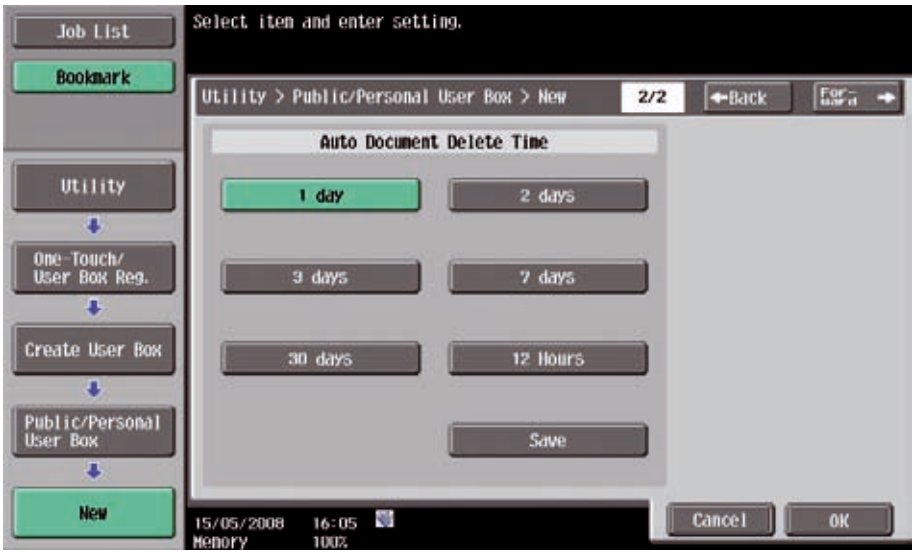
**This is an illustration of the MFP copy process with temporary data deletion selected:**




## 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 timeframe selected for deletion.

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

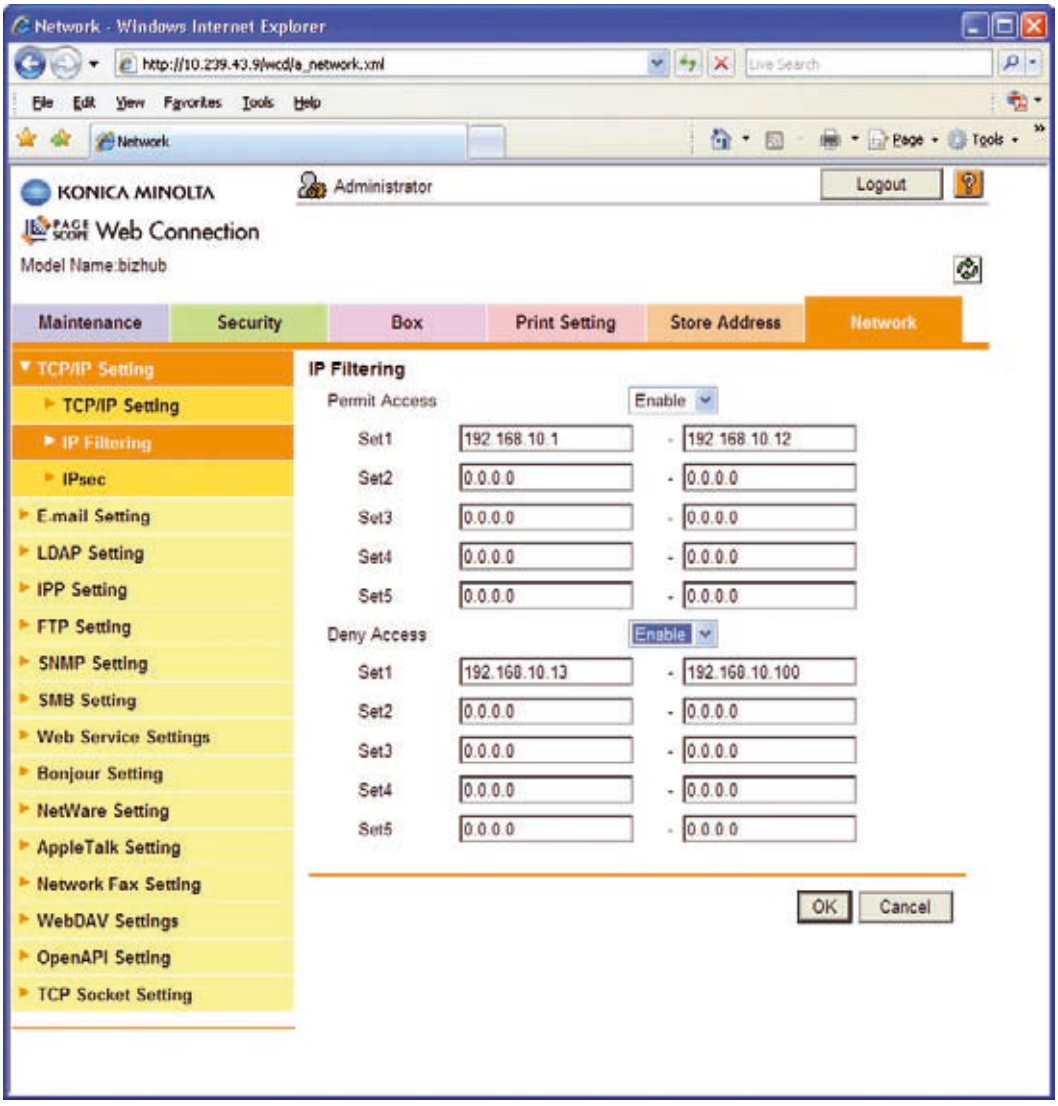



# Network security

## 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 specific IP address ranges of client PCs.

**The screenshot illustrates the PageScope Web Connection administrator access into a bizhub C451. 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.

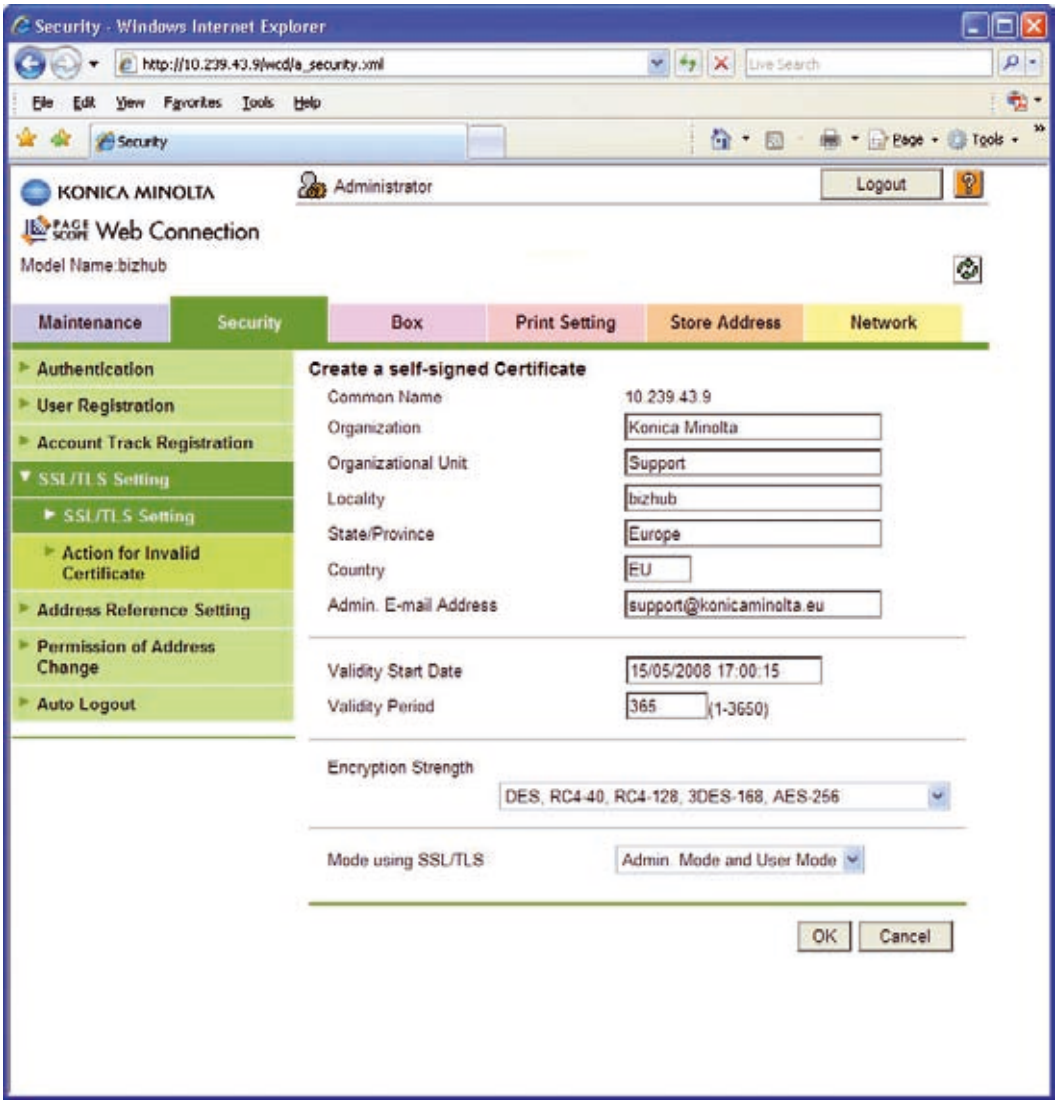
**The following ports can be opened or closed:**

- 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

**The screenshot illustrates the PageScope Web Connection administrator access to the security settings for SSL certificates:**



## 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:**

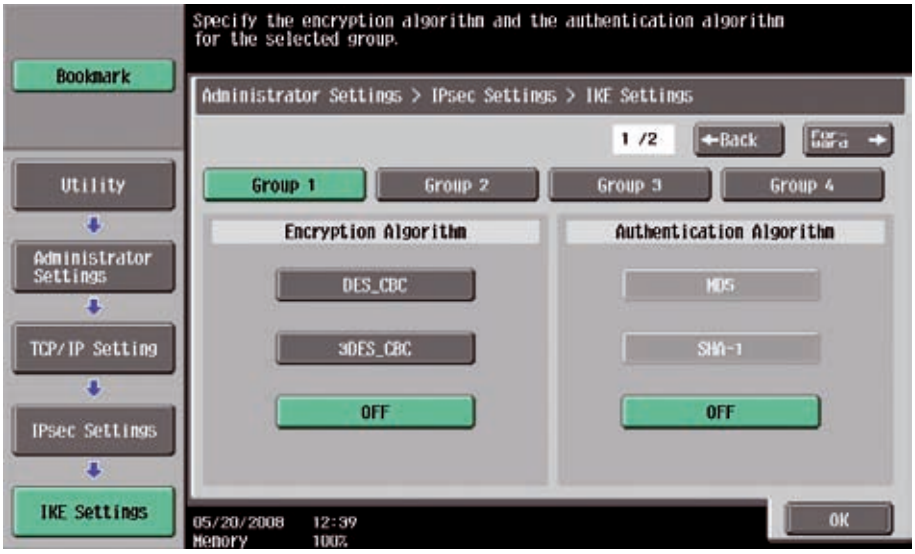
- LDAP protocol
- SMTP protocol
- POP protocol
- IPP (IPPS) protocol
- Windows Active Directory
- PageScope Enterprise Server
- PageScope Data Administrator
- PageScope Addressbook Utility
- PageScope WebConnection (https)

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

## 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:**

## 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 unauthorised devices accept for authentication requests. This prevents that devices can get access to a network by simply acquiring an IP address via DHCP and e.g. performs a Man-in-the-middle attack to sniff data streams on the network.
Only by a proper authentication, password or certificate, at the authenticator, access to the secure network is granted.

**This is an example of the MFP 802.1x authentication settings:**

## NDS Authentication

NDS authentication is a method of user identification that performs authentication based on a specified server, and 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, latest MFPs also support NDS authentication over TCP/IP. NDS authentication can be performed by specifying either IPX/SPX or TCP/IP protocols. NDS authentication over 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:**


# Scanning security

## POP before SMTP

To secure the 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 unauthorised email traffic with the intranet email server, and with the domain/email suffix respectively.

In addition to the above email sending 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 authorises 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 unauthorised decryption of email information on 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 from the recipient of the scan the decryption code to open the file. This feature is very similar to the Adobe Acrobat encryption process where a password is utilised for encryption and opening a file, as well as to access the permissions area of the encryption process.

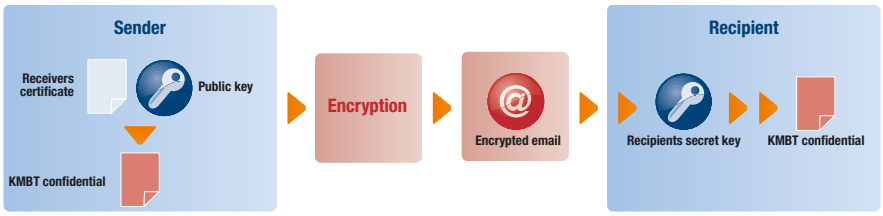
**This is an example of the MFP scan settings for PDF encryption:**



## PDF encryption via digital ID

PDF data that is attached to an email or sent to an FTP or SMB folder, can by 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 allows using this encryption process also 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:**



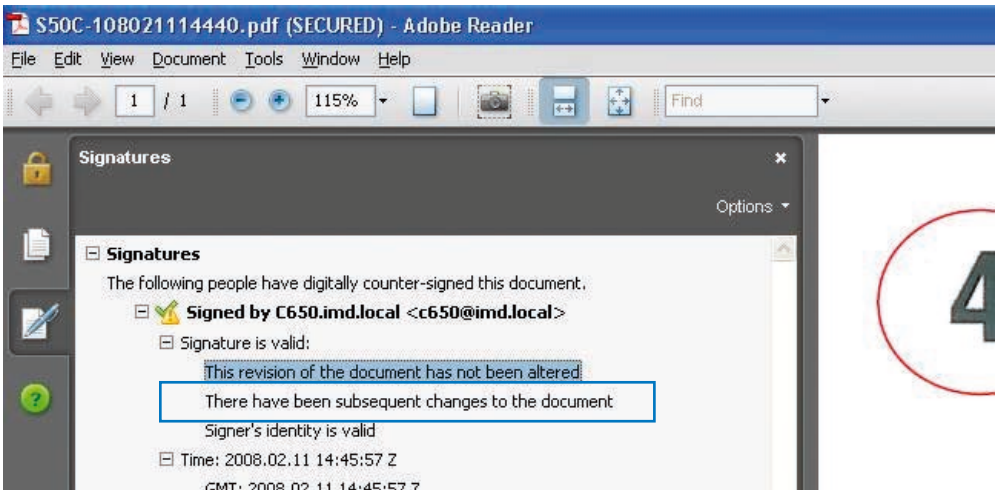

## PDF digital signature

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 encrypting it. 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 to recognise invalid document sources.

**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

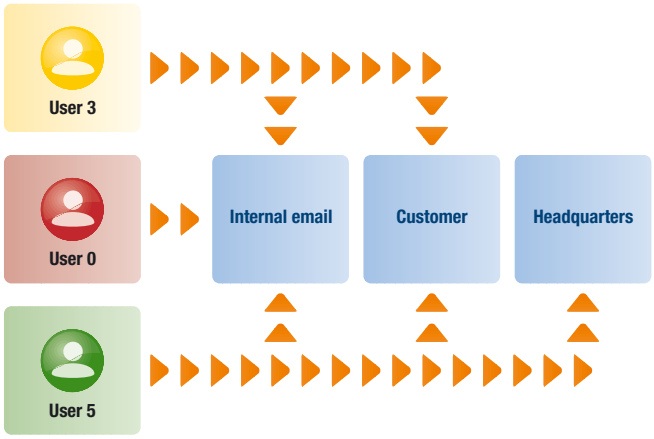
The selection of manual destination blocking will prevent the direct input of, for example, email addresses for transmission of scan files from the MFP. If it is set on, the user has only the possibility to use destinations stored on the MFP, on the PageScope Enterprise Server or a local email database available via LDAP search.

In addition to the prevention of direct input of destinations, the user can be blocked to change the FROM address for an email transmission. In case 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 given in the authentication data. Possible levels are 0–5.

**This illustration shows the access levels of different users:**



# Additional security functions

## Service mode/admin mode protection

The service mode and the admin mode are protected by passwords, respectively 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 unauthorised users.

**This image shows the administrator login screen on the MFP panel:**

## Unauthorised access lock

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

**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 unauthorised access lock can be extended to the system user box for confidential documents (secure print box). The same modes will be applied in case of unauthorised 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 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.

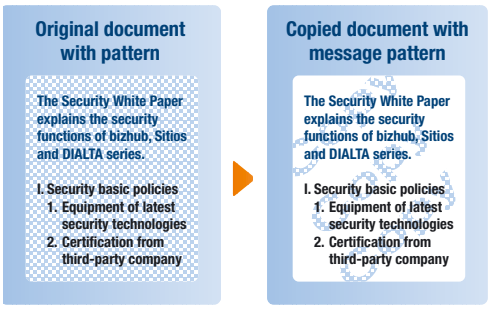


## Copy protection via watermark

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.

**This illustration shows the copy protection functionality:**




## 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 unauthorised 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 F-Code. Besides the fact that digital fax receipt can speed up the fax reception process in general, it completely prevents unauthorised access to fax information, confidential or not.

## Security features & availability

| | Multifunctional systems | | | | | | | | Printers | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Features** | **bizhub C20** | **bizhub C200** | **bizhub C203<br>bizhub C253<br>bizhub C353** | **bizhub C451** | **bizhub C552<br>bizhub C652** | **bizhub 222<br>bizhub 282<br>bizhub 362** | **bizhub 361<br>bizhub 421<br>bizhub 501** | **bizhub 601<br>bizhub 751** | **bizhub C20P** | **bizhub C31P** | **bizhub C353P** | **bizhub 40P** |
| **Access Control** | | | | | | | | | | | | |
| Copy/print accounting | o* | x | x | x | x | x | x | x | o | o | x | o |
| Function restriction (copy/print/scan/fax/box/colour) | x | x | x | x | x | / | x | x | x | x | x | / |
| Secure printing (lock job) | o | o | x | x | x | x | x | x | o | o | x | o |
| User box password protection | / | / | x | x | x | x | x | x | / | / | x | / |
| User authentication (ID + password) | o* | x | x | x | x | x | x | x | o | o | x | o |
| Finger vein scanner | / | / | o | o | o | / | o | o | / | / | o | / |
| IC card reader | / | / | o | o | o | / | o | o | / | / | o | / |
| Event log | / | / | x | x | x | / | x | x | / | / | x | / |
| **Data Security** | | | | | | | | | | | | |
| Data encryption (hard disc) | / | / | o | o | x | o | o | o | / | / | o | / |
| Hard disk data overwrite | / | / | x | x | x | x | x | x | / | / | x | / |
| Hard disk password protection | / | / | x | x | x | x | x | x | / | / | x | / |
| Data auto-deletion | / | / | x | x | x | / | x | x | / | / | x | / |
| **Network Security** | | | | | | | | | | | | |
| IP filtering | x | / | x | x | x | x | x | x | x | x | x | x |
| Port and protocol access control | x | / | x | x | x | x | x | x | x | x | x | x |
| SSL/TLS encryption (https) | x | / | x | x | x | x | x | x | x | x | x | x |
| IP sec support | x | / | x | x | x | / | x | x | x | x | x | x |
| S/MIME | / | / | x | x | x | / | x | x | / | / | / | / |
| 802.1x support | x | / | / | / | x | / | x | / | x | x | / | x |

**x** = standard **o** = option **/** = not available * = for print only



## Security features & availability

| | Multifunctional systems | | | | | | | | Printers | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Features** | **bizhub C20** | **bizhub C200** | **bizhub C203<br>bizhub C253<br>bizhub C353** | **bizhub C451** | **bizhub C552<br>bizhub C652** | **bizhub 222<br>bizhub 282<br>bizhub 362** | **bizhub 361<br>bizhub 421<br>bizhub 501** | **bizhub 601<br>bizhub 751** | **bizhub C20P** | **bizhub C31P** | **bizhub C353P** | **bizhub 40P** |
| **Scanning** | | | | | | | | | | | | |
| User authentication | / | x | x | x | x | x | x | x | / | / | / | / |
| POP before SMTP | x | x | x | x | x | x | x | x | / | / | / | / |
| SMTP authentication (SASL) | x | x | x | x | x | x | x | x | / | / | / | / |
| Manual destination blocking | / | / | x | x | x | / | x | x | / | / | / | / |
| **Others** | | | | | | | | | | | | |
| Service mode protection | x | x | x | x | x | x | x | x | x | x | x | x |
| Admin mode protection | x | x | x | x | x | x | x | x | x | x | x | x |
| Data capturing | / | / | x | x | x | / | x | x | / | / | x | / |
| Unauthorised access lock | / | / | x | x | x | x | x | x | / | / | x | / |
| Copy protection via watermark | / | / | x | x | x | / | x | / | / | / | x | / |
| Encrypted PDF | / | / | x | x | x | / | x | x | / | / | / | / |
| PDF signature | / | / | o | o | o | / | o | / | / | / | / | / |
| PDF encryption via digital ID | / | / | o | o | o | / | o | / | / | / | / | / |
| **ISO 15408** | | | | | | | | | | | | |
| EAL 3 certified | / | / | x | x | x | x | x | x | / | / | x | / |

**x** = standard **o** = option **/** = not available * = for print only

KONICA MINOLTA

**Konica Minolta**
**Business Solutions Europe GmbH**
Europaallee 17
30855 Langenhagen • Germany
Tel.: +49 (0) 511 74 04-0
Fax: +49 (0) 511 74 10 50
www.konicaminolta.eu