CDT GROUP

KONICA MINOLTA

FUNDAMENTALS OF SECURITY WHITEPAPER

WHITEPAPER
SECURITY

Giving Shape to Ideas

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 optional extras to be purchased. Please refer to the function availability table for the various devices on page 37.

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 multifunctional device (MFD), 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 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 remains confidential.

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

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

Common Criteria Validated

CAUSE FOR CONCERN EVERYWHERE – **SECURITY VULNERABILITY**

Generally MFDs 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 MFD 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, MFDs 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 MFDs 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 MFDs 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 unauthorised persons being able to operate an MFD. Preventive measures are needed, firstly to control access to MFDs, 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 MFDs 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 MFD hard disk over a period of time, or simply confidential documents lying in the MFD 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 devices (MFDs) 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

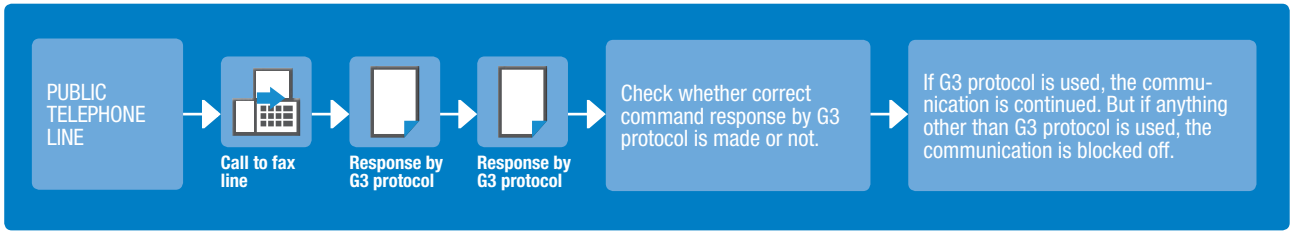
Protection against virus from USB memory

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.

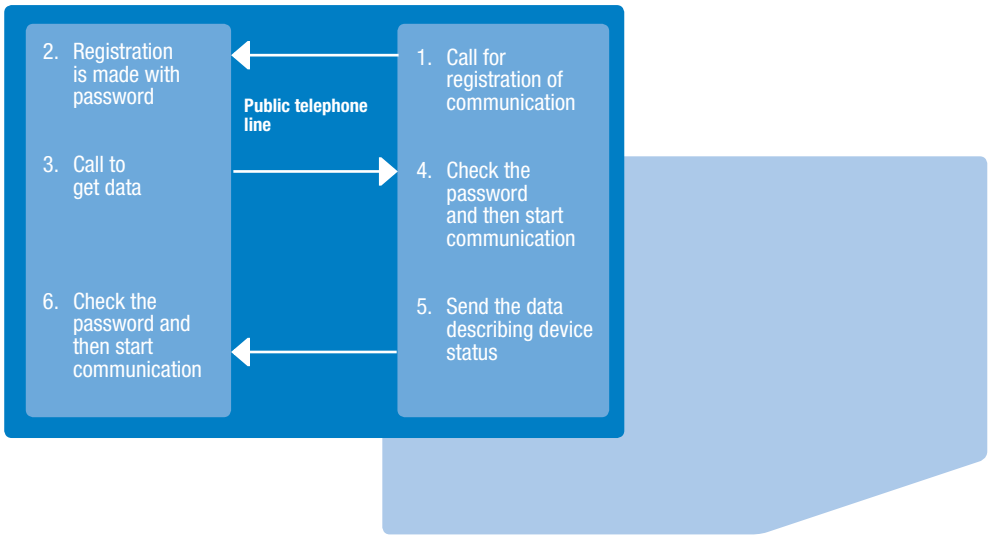
Security for fax line

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

With remote diagnostic services, 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 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 MFDs.

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

Flash memory is embedded on an MFD 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 MFD 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 MFD 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 MFD 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 MFDs 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 MFD. 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, 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.

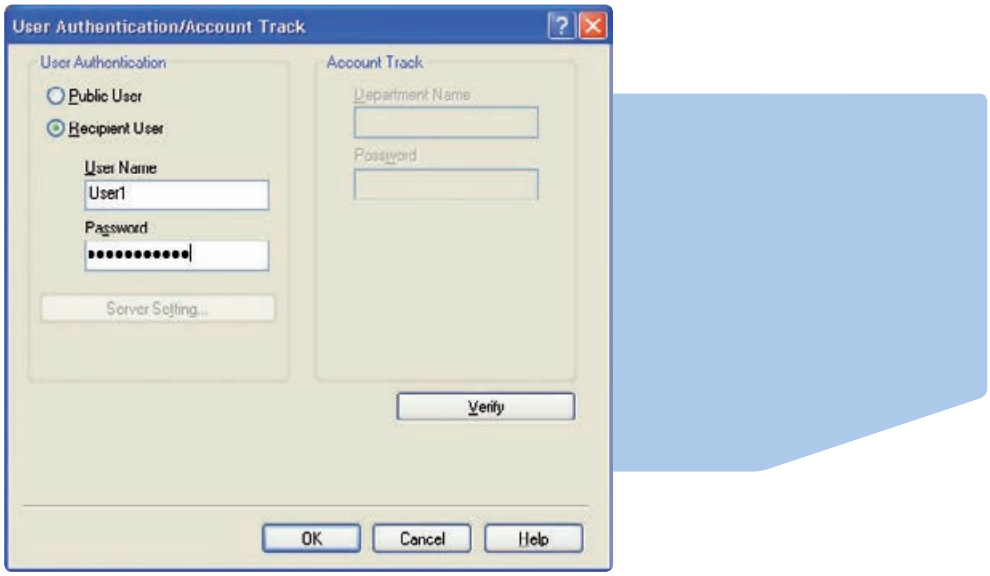
This is an example of the accounting screen from the Konica Minolta bizhub C654 control panel.

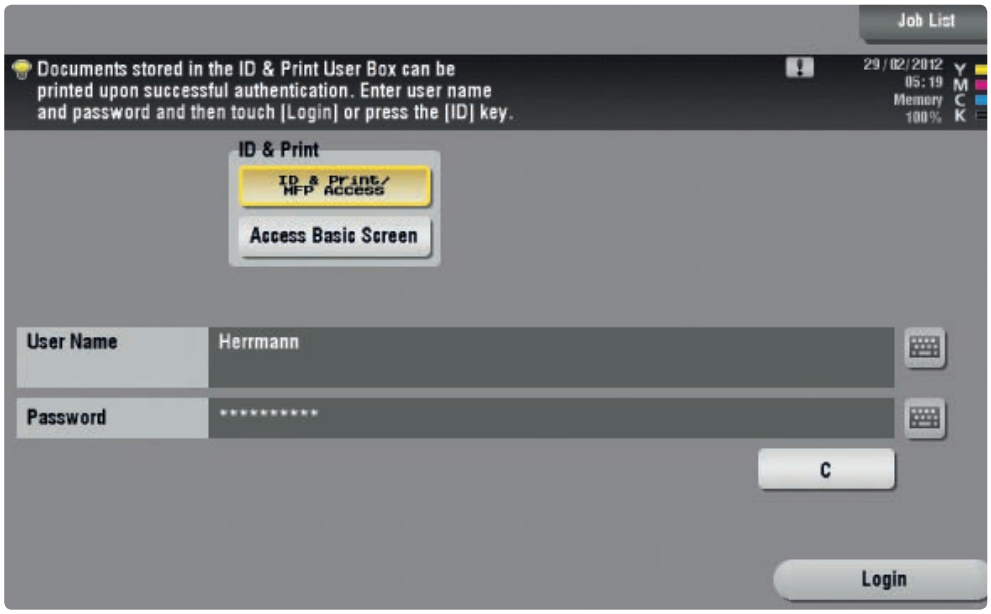
User authentication - ID and password

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

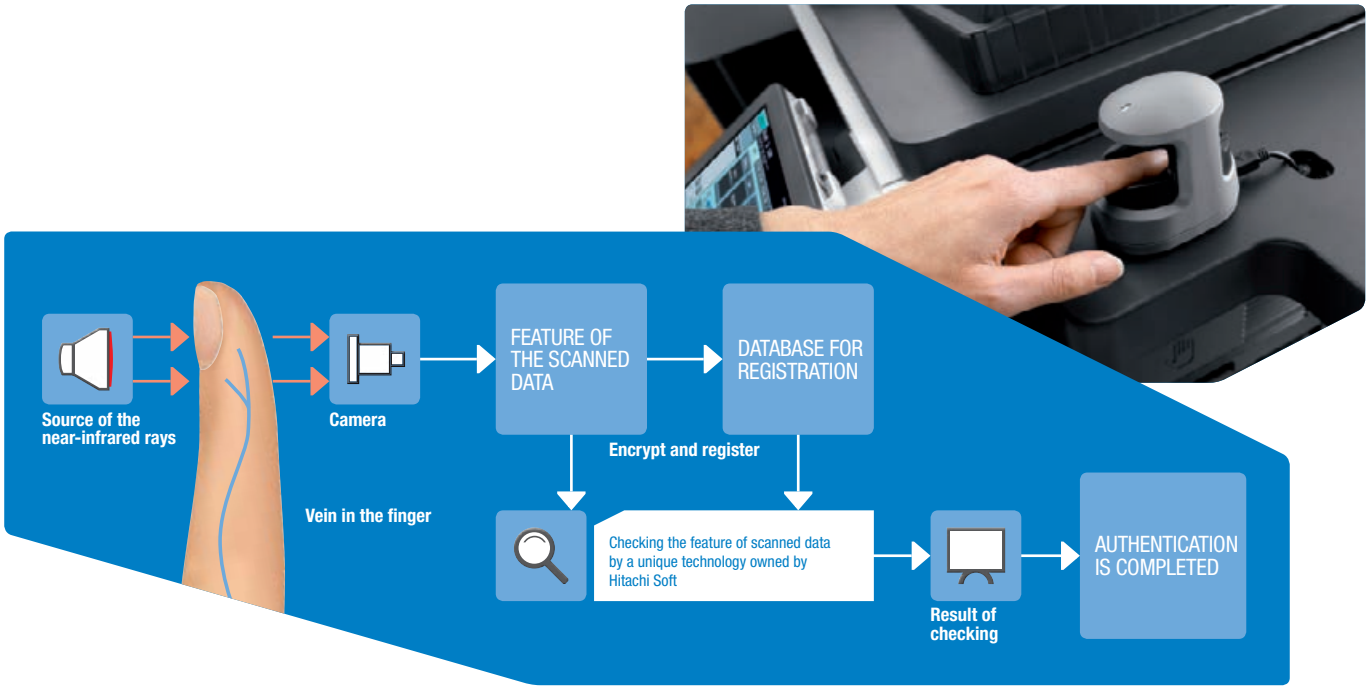
Machine
Internal authentication at the machine can support up to 1,000 user accounts.
Passwords can have up to eight alphanumeric characters.

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 vein scanner

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 MFD.

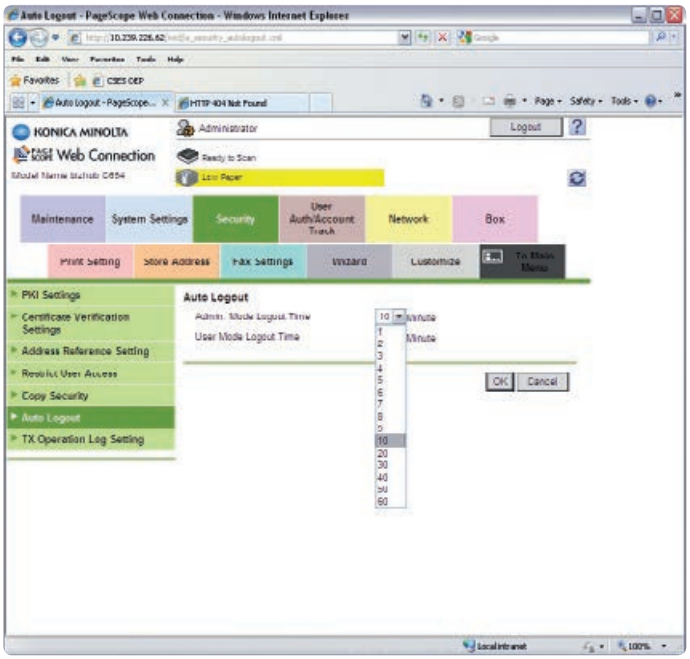
User authentication – IC card reader

As a third authentication solution, Konica Minolta MFDs can be equipped with an IC card reader. The non-contact IC card contains a unique code which is linked in the MFD 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 MFD hard disk, and are therefore protected.

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

Auto log off

Konica Minolta MFDs can be programmed to automatically reset to a state that requires password input after a predetermined time of inactivity. This ensures that the MFD will reset to a secure state if a user forgets to log off from an MFD when finished. Note that the reset timer can be set from 1 to 60 minutes. Some Konica Minolta MFDs 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 MFD.



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

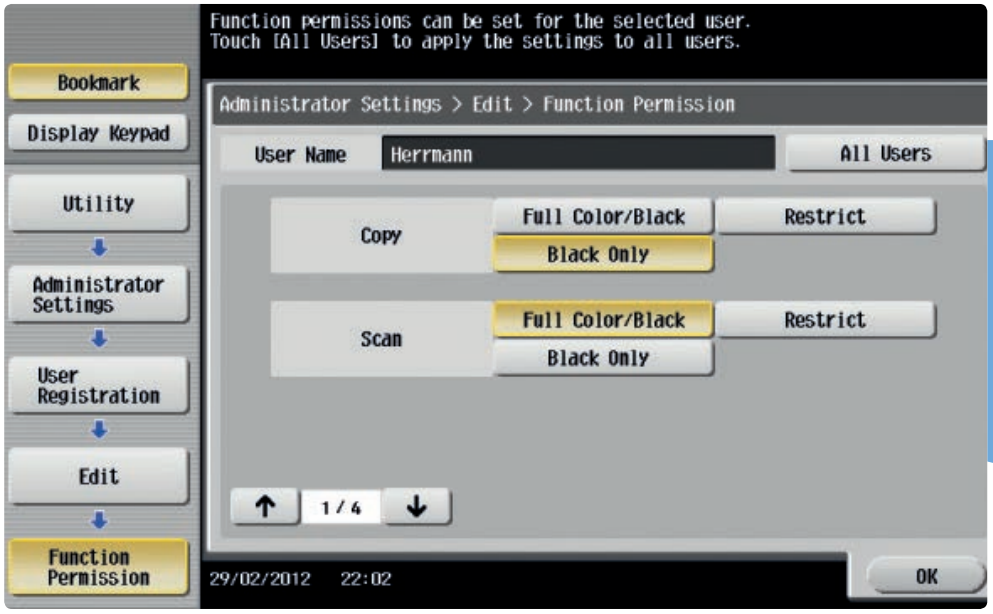
Function restrictions

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

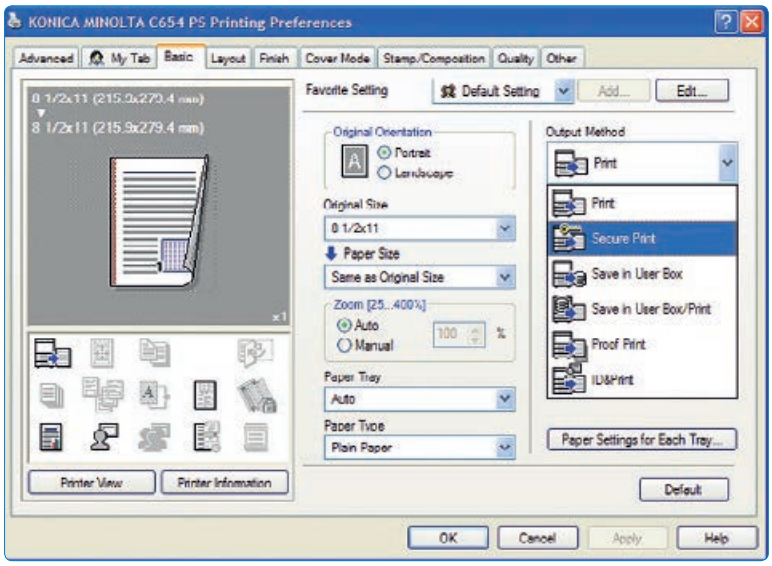
Function restrictions can be set in general either as a walk-up functionality or per user, depending on the user authentication.

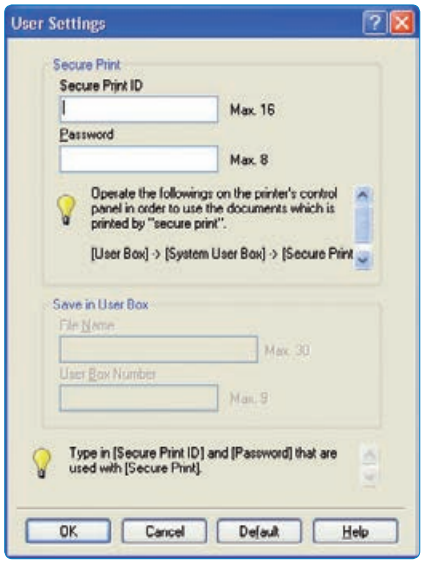


This is an example of the function permission screen from the Konica Minolta bizhub C654 control panel.

Secure print (lock job)

Konica Minolta MFDs 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 MFD. 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 MFDs 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 MFD-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.

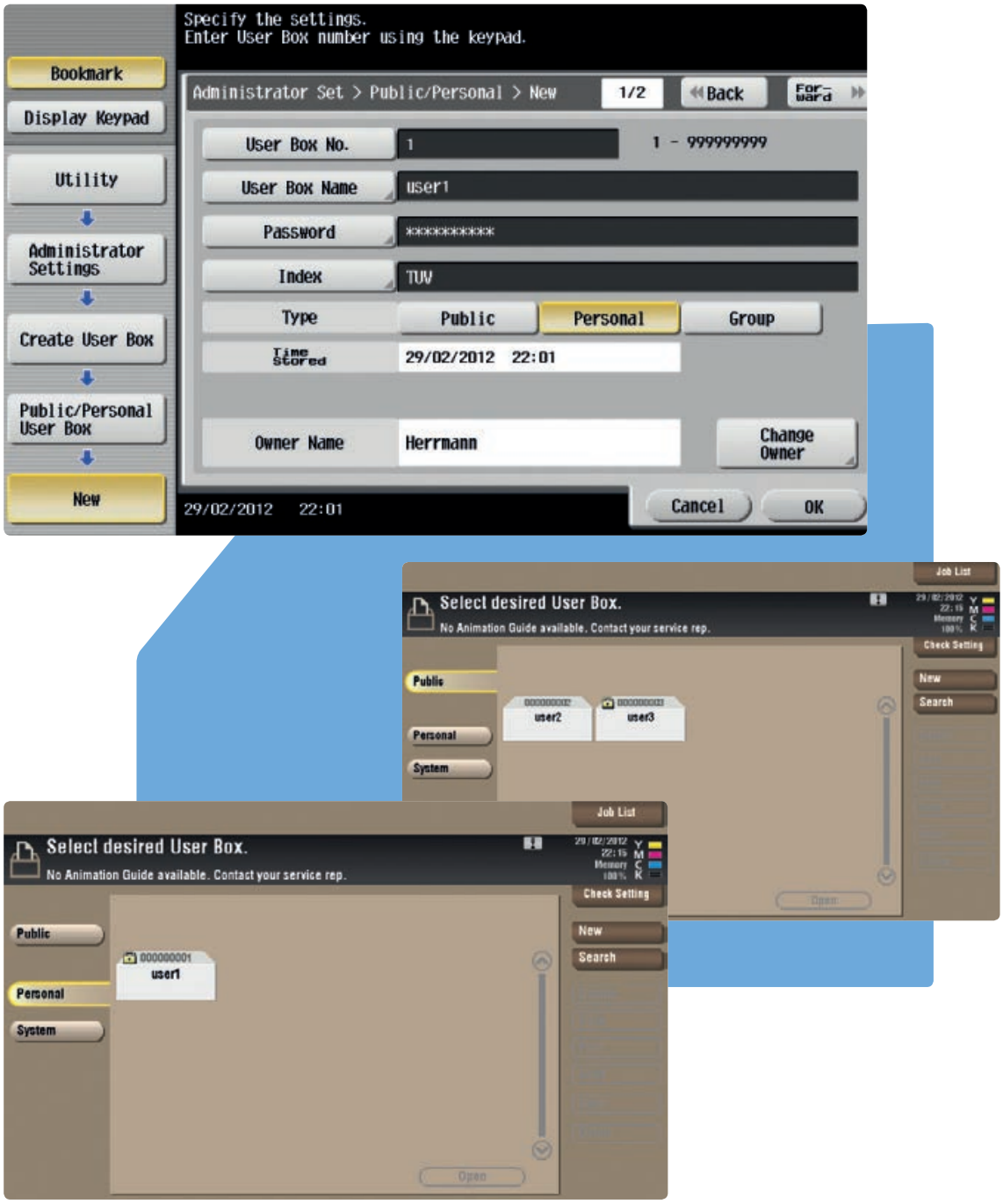
Touch & Print is based on authentication via finger vein scanner or IC card reader.
ID & Print is based on user authentication via ID and password.

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 MFD. Besides the general security features given to the hard disk, these user boxes can be set with different access levels. On a walk-up MFD the user boxes can be protected by an eight-character alphanumeric password.

If the MFD 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.

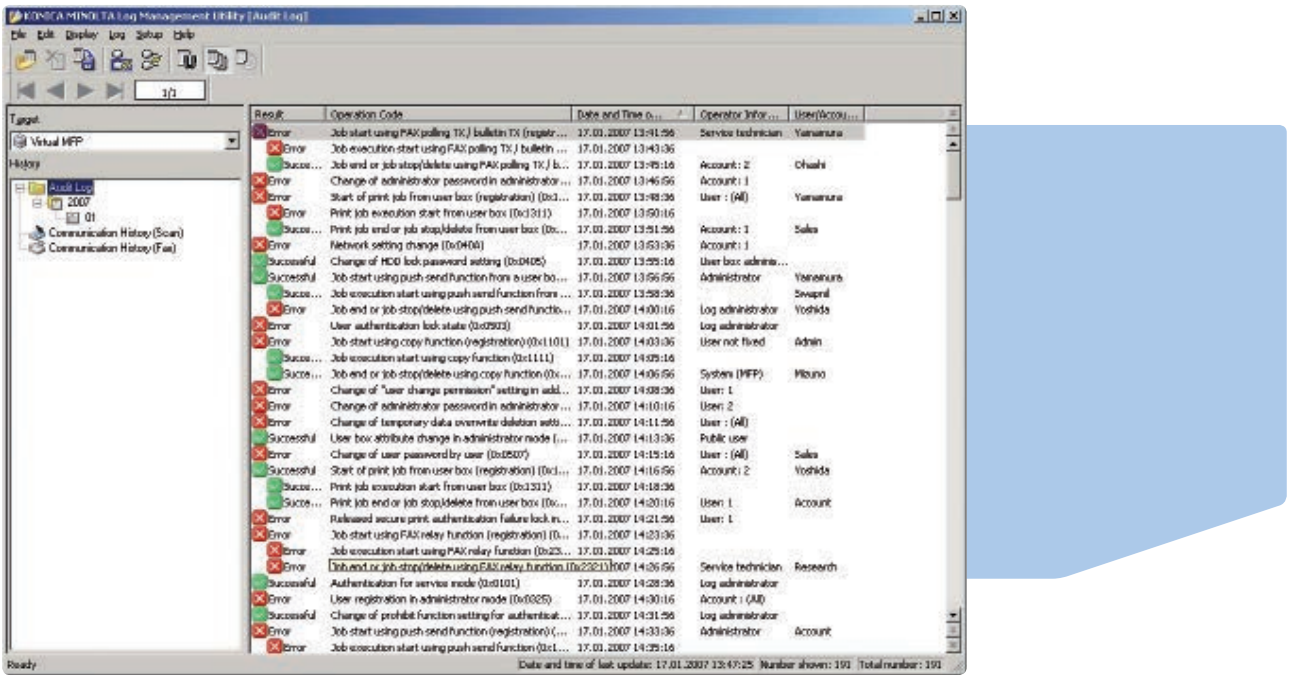


This is an example of set user box registration and user box view on the bizhub C654 panel.

Event log

All Konica Minolta MFDs offer the option to record all actions that have happened on the MFD, 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 MFDs 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 MFD. To avoid network information from being sniffed, such user data can be encrypted by the printer driver and decrypted on the MFD.

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

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

DATA SECURITY

Hard disk password protection

The built-in hard disk of the MFD 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 MFD 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 MFD password entry in the administration mode for hard-disk protection (bizhub C654).

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 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 is 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 MFD.

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

Hard disk data overwrite

When equipped with a hard disk drive (HDD), Konica Minolta MFDs can store sensitive electronic information. The data can be deleted by those users who own the documents that reside inside the MFD's HDD in password protected boxes. For added safety, a key operator, administrator or technician can physically format (erase) the HDD if the MFD 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 example of the HDD overwrite settings of the MFD (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 (NAVSO P-5239-26) Overwrite with random 1 byte numbers Department of Defense (DoD 5220.22M)
Mode 4	Overwrite with random 1 byte numbers Army Regulations (AR380-19) Overwrite with 0x00 Overwrite with 0xff
Mode 5	Overwrite with 0x00 Former NSA Standard Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff
Mode 6	Overwrite with 0x00 North Atlantic Treaty Organization – NATO Standard Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 512 bytes of specified data
Mode 7	Overwrite with 0x00 US Air Force (AFSSI5020) Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa Verified
Mode 8	Overwrite with 0x00 US Air Force (AFSSI5020) Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0x00 Overwrite with 0xff Overwrite with 0xaa Verified

Different modes of HDD overwriting

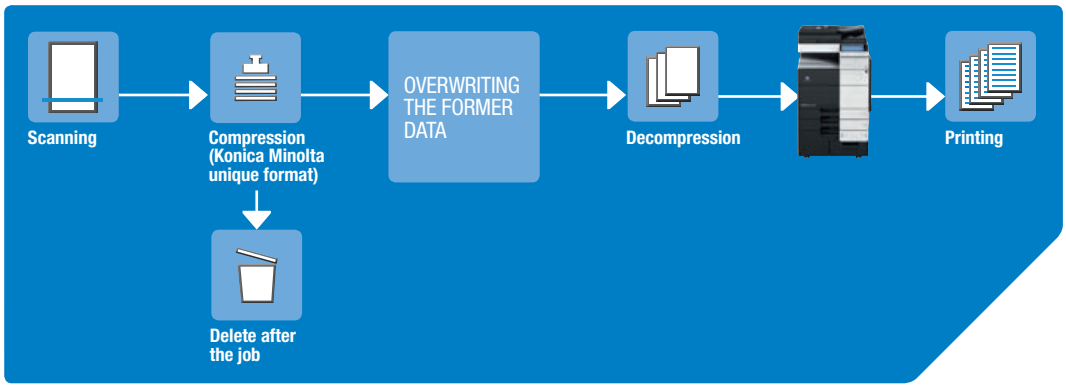
The example shows an MFD panel for hard-disk formatting in administration mode (bizhub C654).

Temporary data deletion

Depending on the file size for certain jobs, the MFD 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

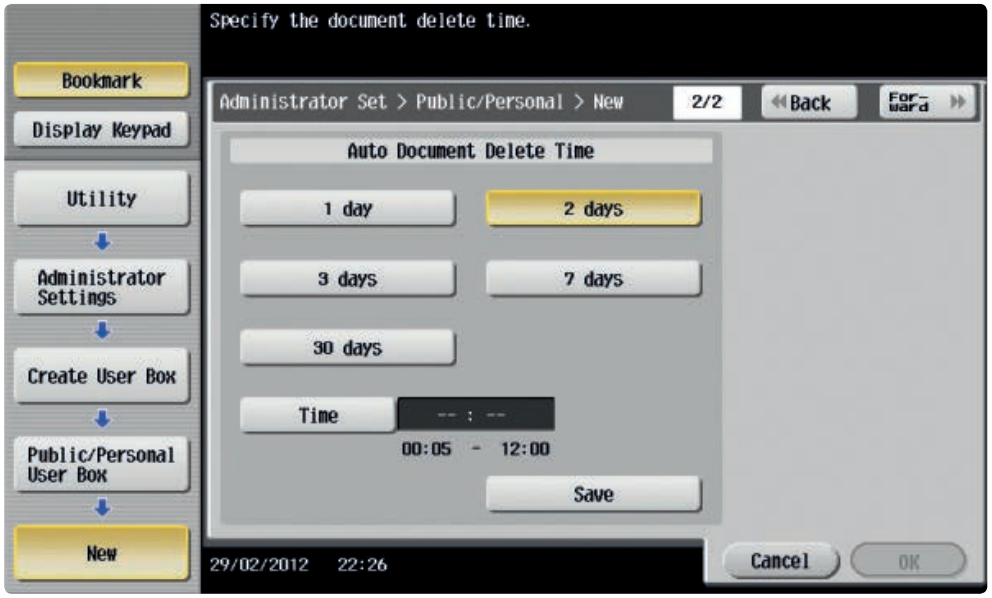
For the temporary data deletion two modes are available.



This is an illustration of the MFD 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.

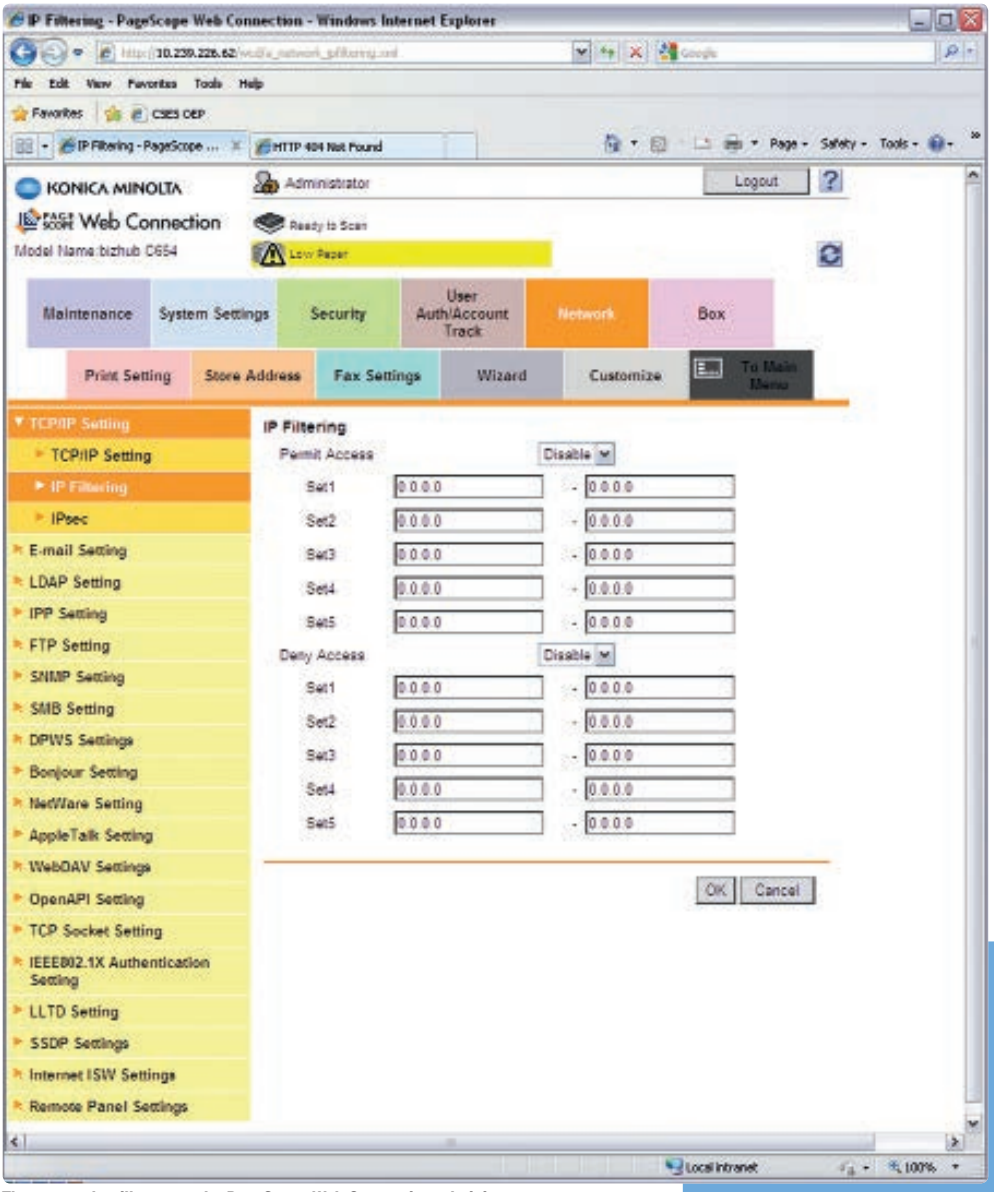


This is an example of the MFD setting for user box document auto deletion (bizhub C654).

NETWORK SECURITY

IP filtering

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



The screenshot illustrates the 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 MFD, 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)

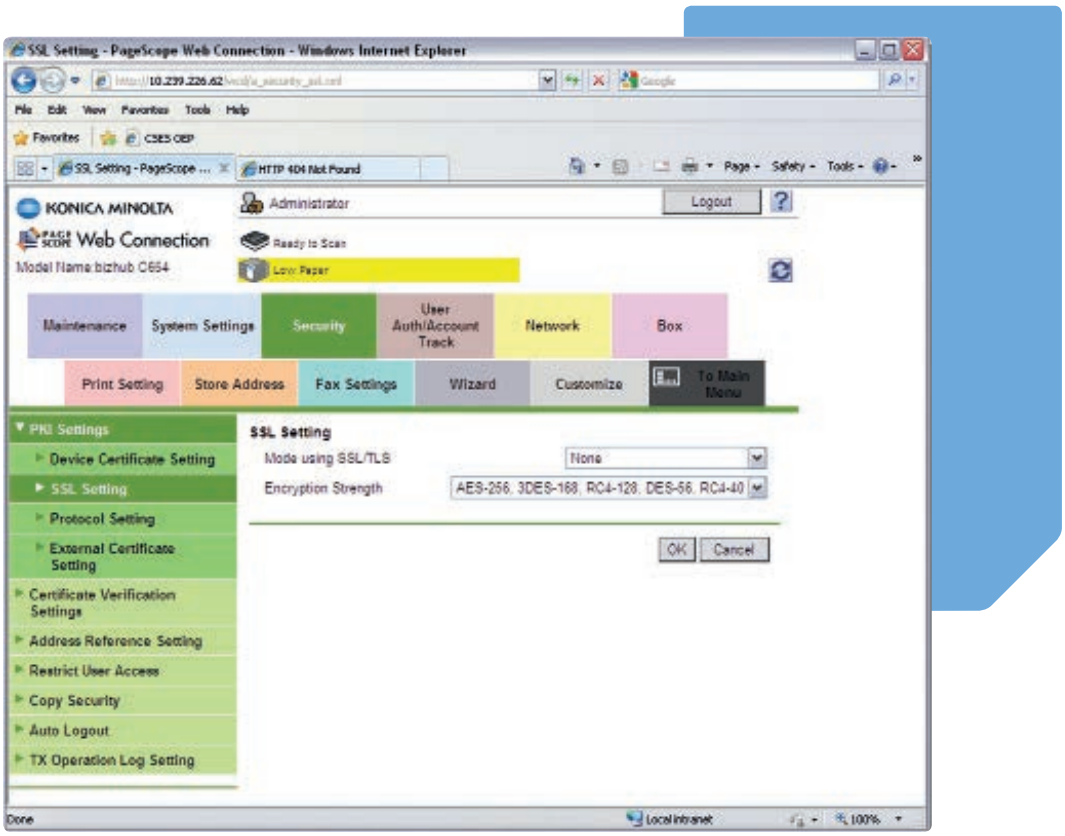
The data communication via network to specific databases or applications can be encrypted by SSL (Secure Sockets Layer) or TLS (Transport Layer Security). Supported versions of encryption are SSL 2.0, SSL 3.0 and TLS 1.0.

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 Addressbook Utility
- PageScope Web Connection (https)

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



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

IPsec support

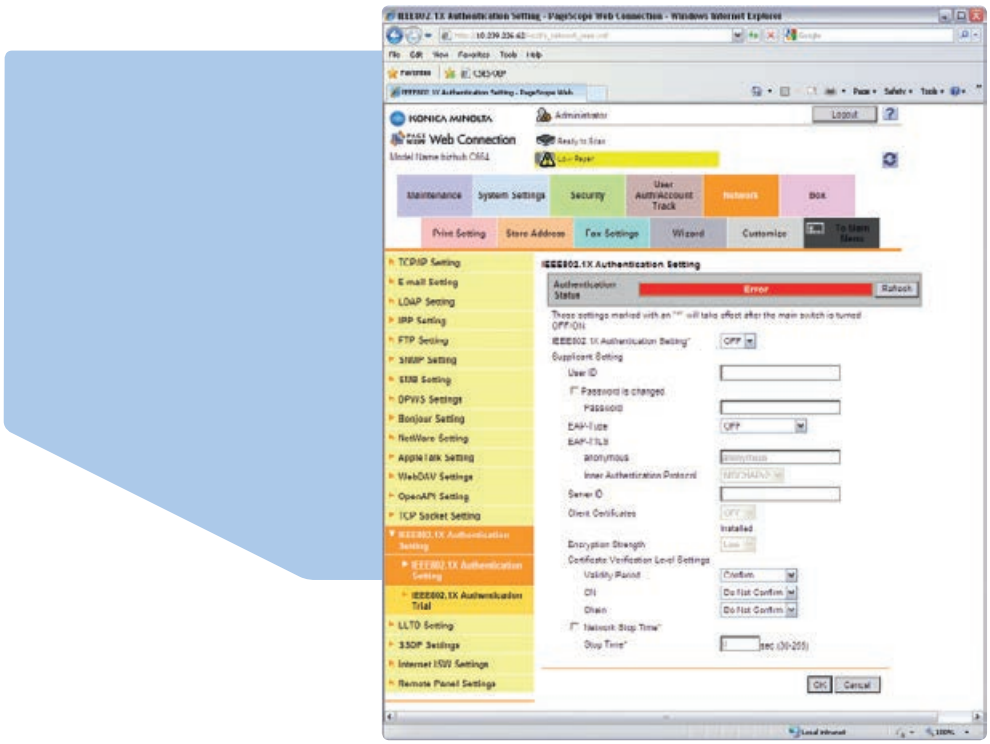
To complete the encryption of any network data transmitted to or from the MFD, the bizhub devices also support IPsec (IP security protocol). This protocol encrypts the whole network communication between the local intranet (server, client PC) and the device itself. The IPsec protocol can be programmed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

This is an example of MFD IPsec/IKE settings via the MFD 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.
The IEEE 802.1x authentication standard generates a secure network by closing any network communication (e.g. DHCP or HTTP) to unauthorised 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.

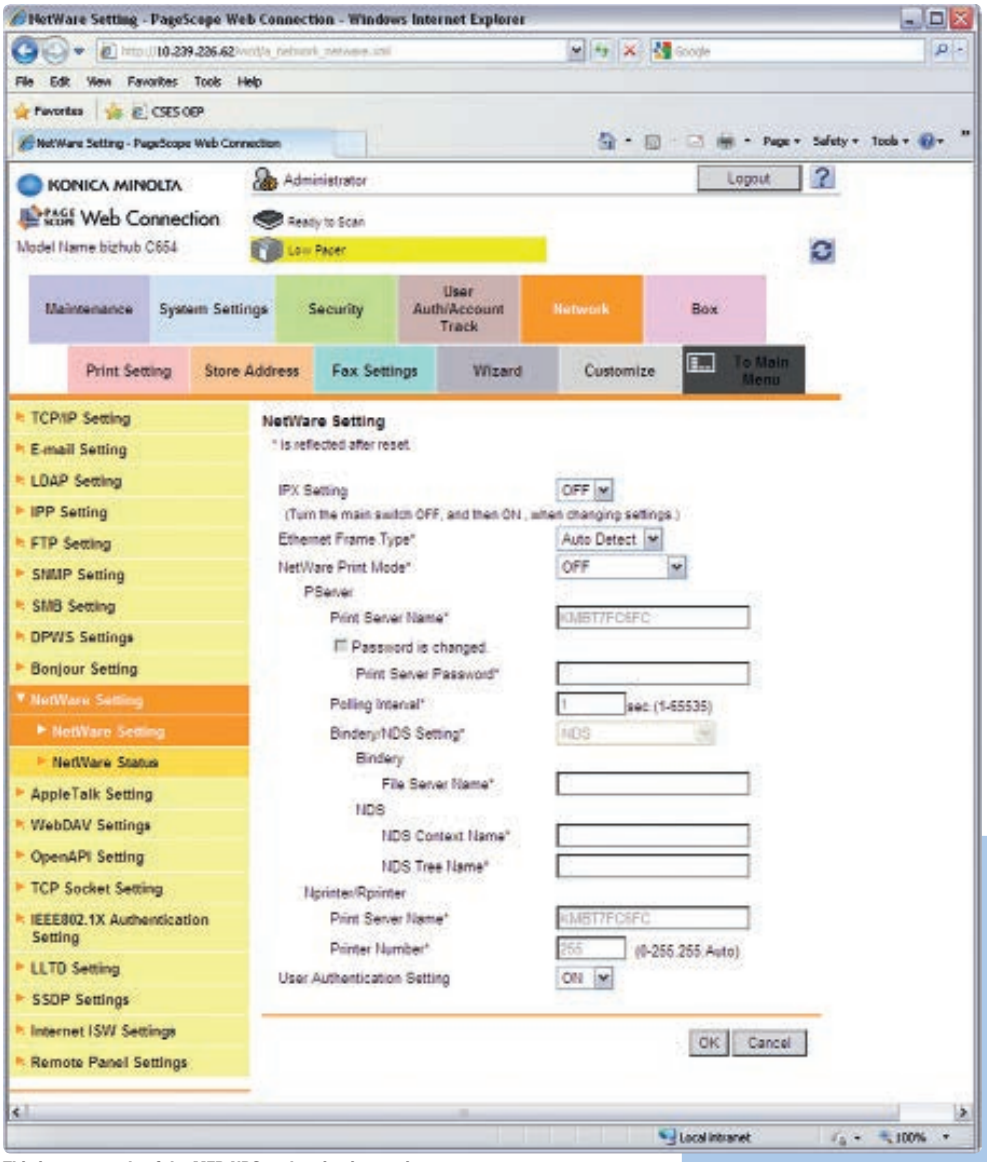


This is an example of the MFD 802.1x authentication settings.

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 MFDs 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.



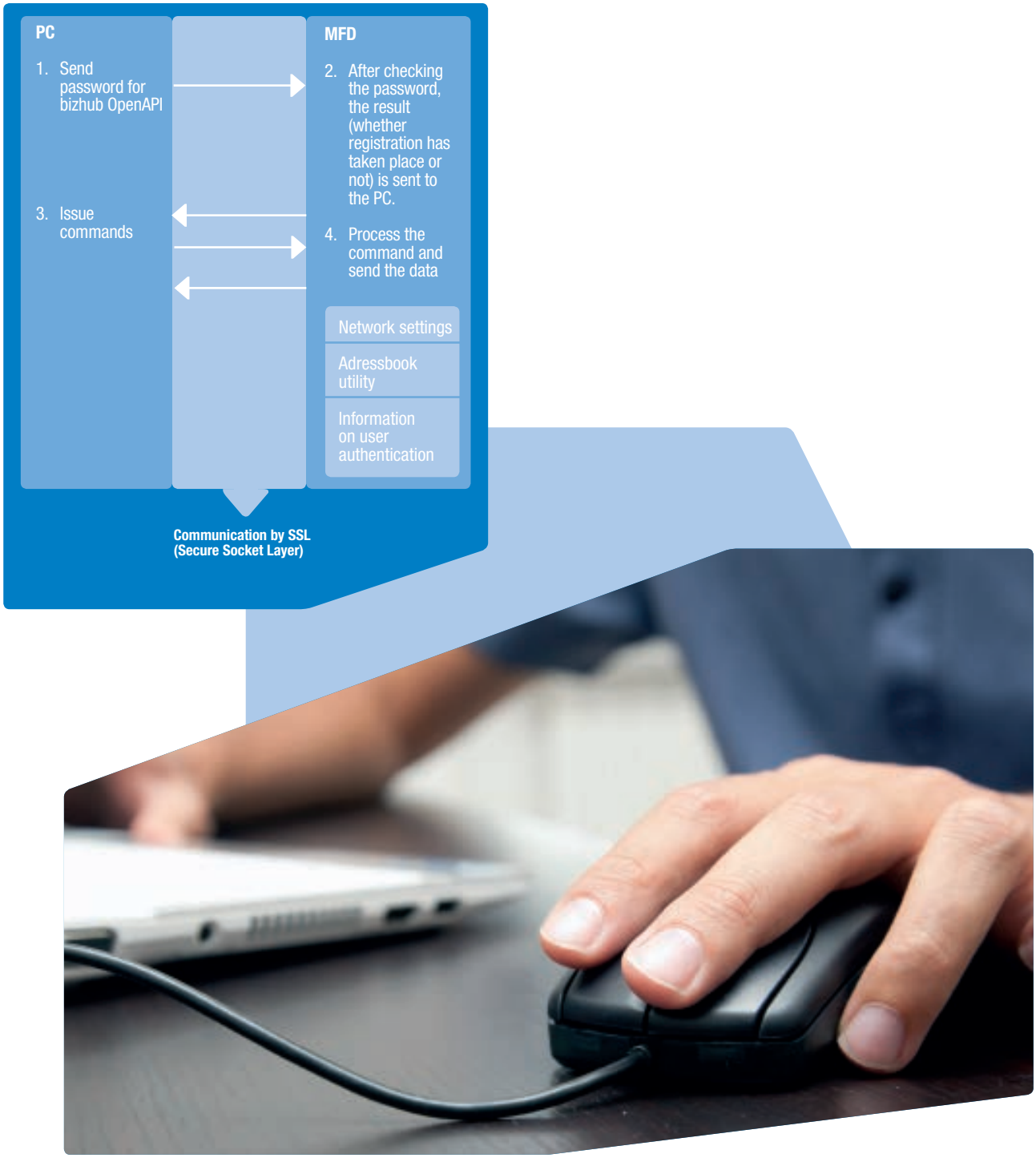
This is an example of the MFD NDS authentication settings.

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.

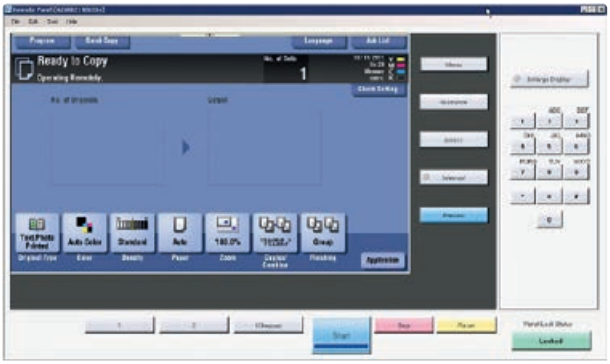
bizhub OpenAPI acquires and sets the data received from devices via networks using the SSL encryption protocol.
By using an original password, communication is rendered more secure.

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



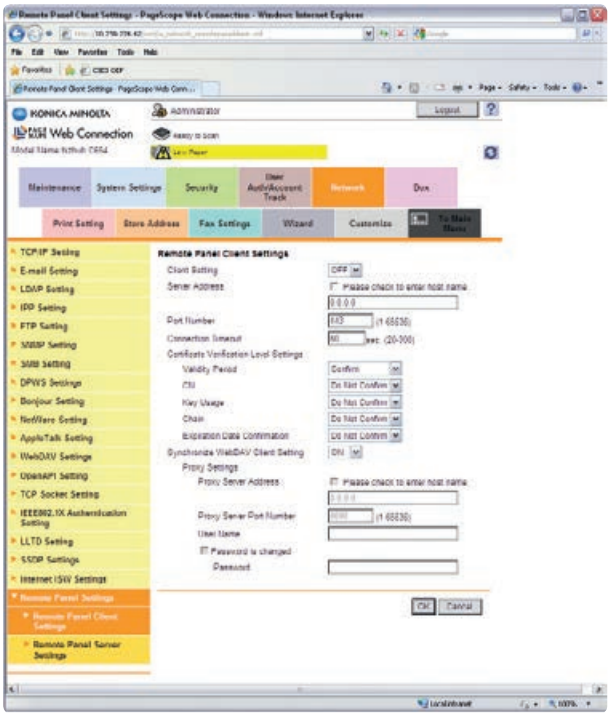
Remote panel

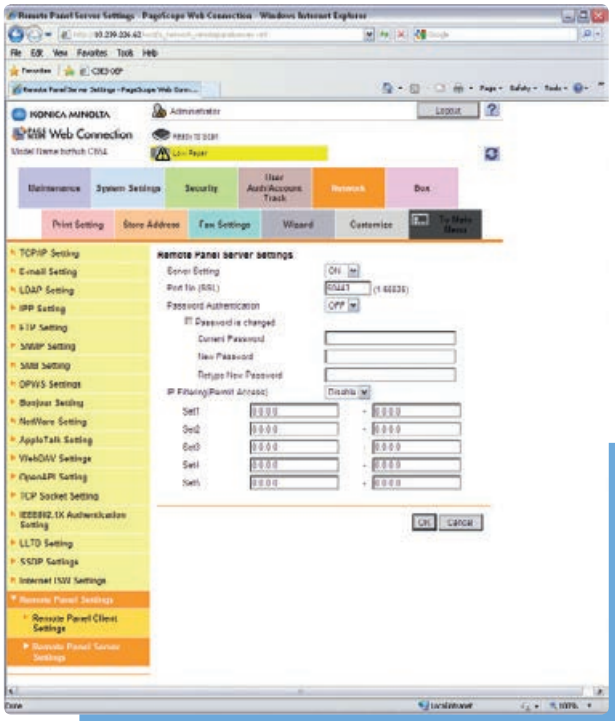
The latest generations of Konica Minolta devices offer the option of a remote panel. This means administrators are able to have realtime access to the MFD panel remotely, e. g. via a Web browser. Every function which is available on the MFD panel can also be executed remotely.



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

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.

PAGESCOPE ENTERPRISE SUITE SECURITY MATTERS

In modern society, where network infrastructure has already developed and information technology has spread, staggering amounts of information are distributed. The information is collected in various forms and is utilised after it has been translated into the higher-level information assets. In corporate activities, protecting these information assets, i.e. managing the risk, is an important task.

This document introduces the basic security functions that are provided by Konica Minolta's PageScope Enterprise Suite.

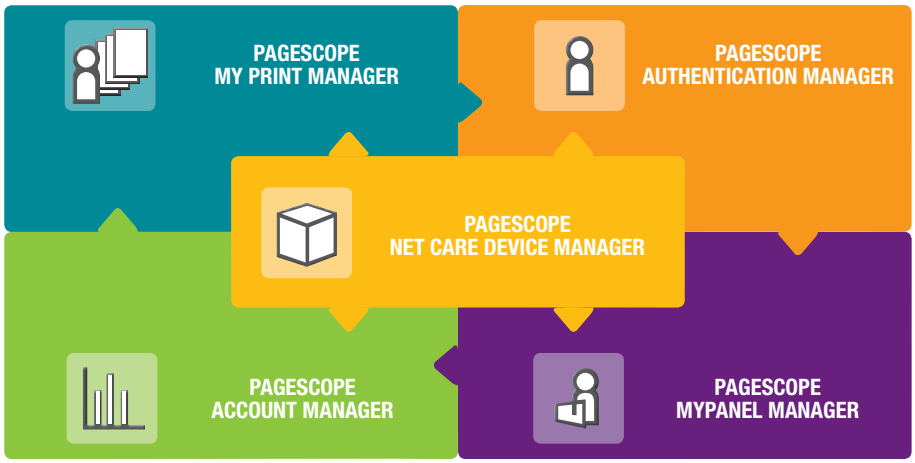
Summary of PageScope Enterprise Suite

PageScope Enterprise Suite is the generic name of the applications required for account management, authority management, panel settings and management for individual users of the devices operating in offices. All applications are running on a server and are operated in the Web browser. Combining them, you can build the system to suit your environment.

PAGE SCOPE Enterprise Suite

PageScope Enterprise Suite mainly consists of the following applications.

PAGE SCOPE Net Care Device Manager	Status management software; consolidates machines on the network
PAGE SCOPE Account Manager	Software for document volume accounting management
PAGE SCOPE MyPanel Manager	Software for panel settings and management for individual user
PAGE SCOPE Authentication Manager	Software for consolidating user authentication
PAGE SCOPE My Print Manager	PageScope My Print Manager



PageScope Enterprise Suite – Communication security

1. User authentication

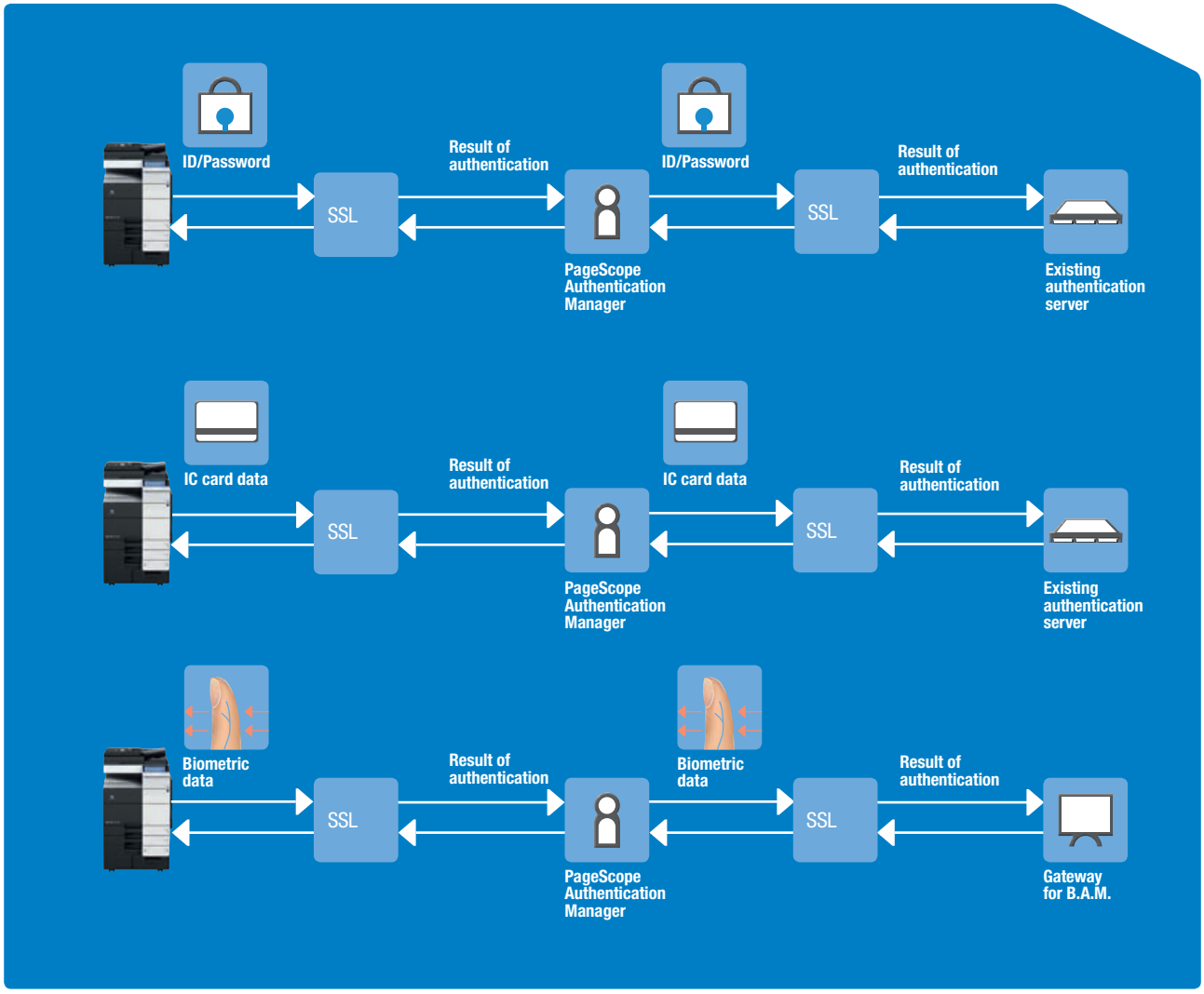
In the communication of authentications by PageScope Authentication Manager, the authentication data is sent and received safely by using SSL. And the permitted functions for each user are enabled.

If the environment is built to cooperate with an office's existing authentication server, it is possible to keep the authentication information within the server.

The authentication methods supported by general authentication servers are shown below. Kerberos authentication or NTLM authentication is enabled for Active Directory; Digest-MD5 authentication and simple authentication for LDAP servers; NDS authentication for NDS servers, and NTLM authentication for NTLM servers.

Authentication data input to MFD for authentication, IC card data read by a card reader, and the biometric information read by a finger vein reader are communicated for authentication using the SSL.

Biometric information (finger vein) is authenticated by Gateway for Biometric Authentication Manager (Gateway for B.A.M.).



Communication of user authentication (ID/password, IC card, biometrics).

2. Sending of counter information

Counter information is the basis of each division and individual. A file in XML format is created in MFD. It is encrypted, and then it is sent to PageScope Account Manager. AES-256 is used as the encryption system for models made after the Mosel/Thames series. For earlier models, DES is used for encryption.

SEND DATA	PROTOCOL	ENCRYPTION SCHEME
Authentication data (user ID, password/IC card data/ biometric data)	HTTP, LDAP	SSL
Counter data	FTP, WebDAV, HTTP	XML file is encrypted and transferred.
MIB	SNMP v1/v3	When SNMP v3 is used, encrypted communication by DES or AES is possible.

3. Port number change

The port number of each application can be changed. Port number change prevents conflict with the port number of the applications other than PageScope Enterprise Suite, and attacks by unauthorised applications. (The port number of PageScope Authentication Manager and PageScope Net Care Device Manager can be changed only during installation.)

For your reference, the port numbers currently used are shown below.

TYPE	PORT NUMBER (DEFAULT)	PURPOSE OF USE
HTTP	80	[Common] Web access to the server * [Net Care Device Manager] Counter reading into MFD ** [Account Manager] Data transmission from Print Log Tool * Counter reading into MFD **
HTTPS	443	[Common] Web access to the server * Communication with Licence Management Server (LMS) ** [Net Care Device Manager] Counter reading into MFD ** [Account Manager] Data transmission from Print Log Tool * Counter reading into MFD ** [Authentication Manager] Communication with MFD Communication with B.A.M server
LDAP	389	[Authentication Manager] Communication with Active Directory Service
SNMP v1/v3	161	[Common] Retrieval of MFD Status confirmation of MFD
OpenAPI	50001, 50002 [In case of SSL: 50003]	[Authentication Manager] Sending login information and result of printing to server Sending upper limit information to MFD [Account Manager] Upper limit management Acquisition of attribute information such as a user etc. from MFD for a counter collection [MyPanel Manager] Sending setting information to MFD
SMTP	25	[Common] Email transmission of the counter information from the server
FTP	21 A suitable port number is allocated each time	[Account Manager] Counter reading into the MFD [Net Care Device Manager] Counter reading into MFD **

*** The client PC accesses the server through port 80, but the port on the client PC side is allocated a port number each time a connection is made.**

**** The server accesses MFD (or License Management Server) through port 80 (443) but the port on the server side is allocated a port number each time a connection is made.**

PageScope Enterprise Suite – Access restriction

Although system administrators at the highest level can configure all settings, authority should be divided into the required units to avoid careless settings in unrelated areas. Concerning access to PageScope Enterprise Suite, four types of user level are provided. Only system administrators and the specified users are allowed to configure settings and management of software. For example, the user specified as an administrator of PageScope Net Care Device Manager can register and remove the devices of the managed object. Nobody other than the specified user can execute such operations.

Access to PageScope Enterprise Suite is performed in a Web browser. If authentication is completed successfully on the first login screen, the operations are allowed.

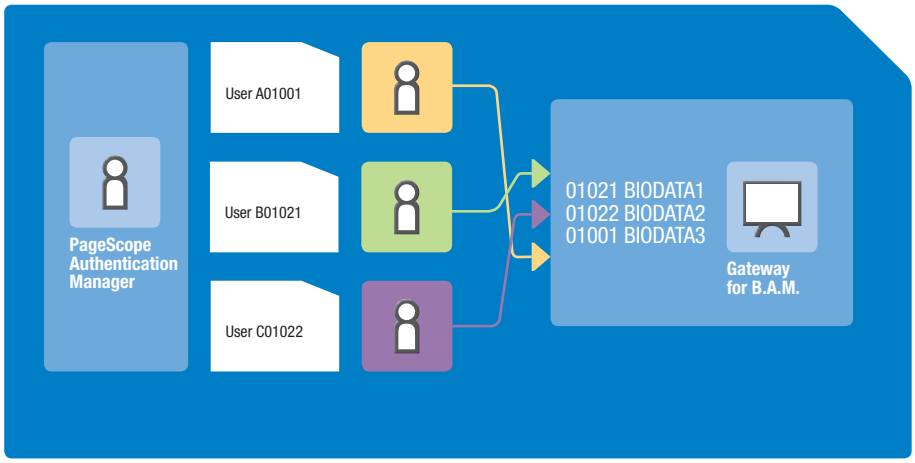
TYPE	DESCRIPTION
User	General user. It is only possible for users to change their own password.
Group Administrator	The user specified as Group Administrator can manage the devices and the users within the group. There are three types of groups: user group, account group, and device group. And it is possible to share responsibility for the management of each group.
Application Administrator	The user specified as Application Administrator (set for each application) can manage application. There are four types of application unit: Authentication Manager, Account Manager, MyPanel Manager, and Net Care Device Manager. And it is possible to share responsibility for the management of each application.
System Administrator	It is possible to manage all software, such as the settings of the Group Administrator or Application Administrator.

PageScope Enterprise Suite – Data management

1. Management of IC card information and biometric information

Although IC card information is managed in the database of PageScope Authentication Manager, it is also possible to use the IC card information managed by an existing authentication server.

Biometric (finger vein) information is managed in the database of Gateway for Biometric Authentication Manager (Gateway for B.A.M.). When information such as a password or IC card has been leaked, it is possible to change the password or IC card. For biometric information, however, this is not possible. Therefore, you should handle biometric information carefully. If only biometric information has been leaked, it is not possible to determine whose biometric information it is. And the biometric information to be managed includes only the features extracted. The information cannot be used in other systems because it is the data for Gateway for B.A.M. only.



Link between Gateway for B.A.M. and biometric information.

2. IC card data and finger vein information registration

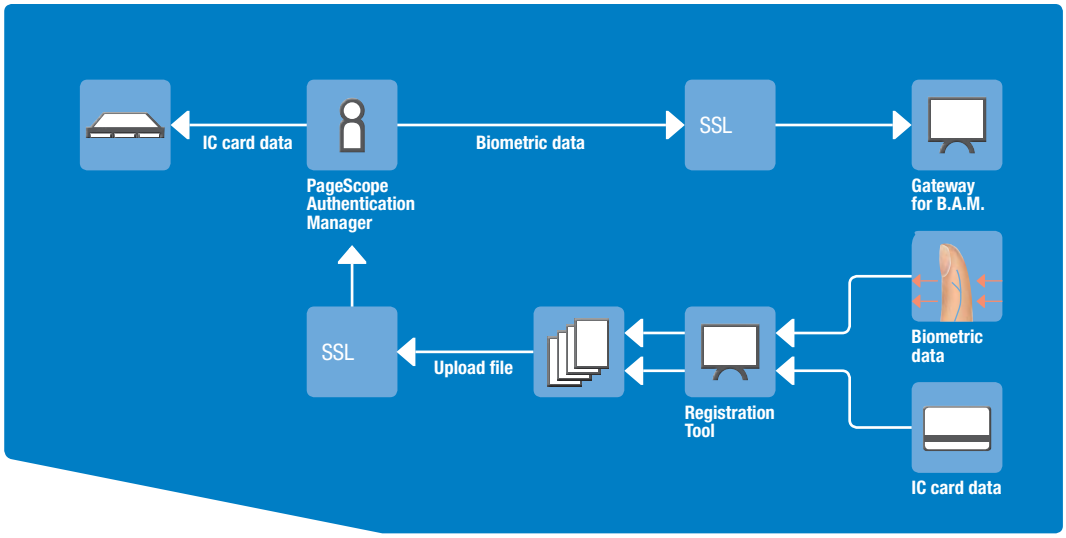
IC card and biometric (finger vein) information is registered in the database of PageScope Authentication Manager using the exclusive Registration Tool software. The Registration Tool is software to be installed on a client PC. IC card or finger vein information is read by a reader. It is output as a file to a client PC once, and it is registered on the registration screen of PageScope Authentication Manager by uploading the file. When uploading a file, data is sent safely using SSL.

Only a user who is registered as an administrator of Pagescope Authentication Manager can perform the registration.

Uploaded IC card data is registered and managed on the database of PageScope Authentication Manager.
Biometric information is registered and managed on Gateway for B.A.M.

The files that are used between the PageScope Authentication Manager and Registration Tool can be encrypted (AES-256) and saved.

Note: When using IC card data from the existing authentication server (Active Directory or LDAP server only), the Registration Tool is not required.

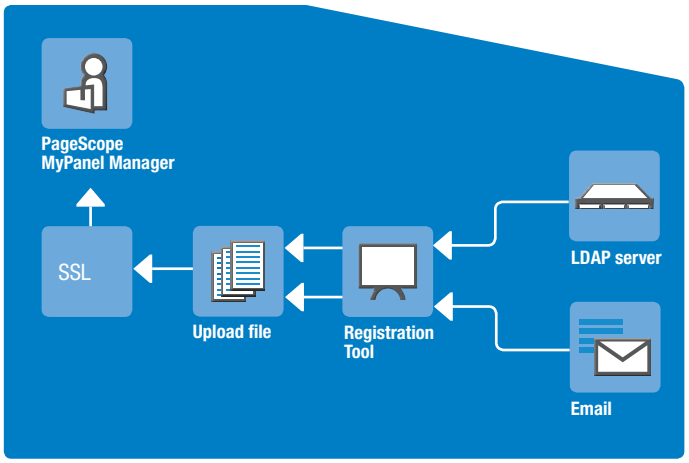


IC card/biometric information registration using the Registration Tool.

3. Registration using PageScope MyPanel

MyPanel is registered in the database of MyPanel Manager using the exclusive Address Importer. Address Importer is the software to be installed on a client PC. Address data is exported from Outlook or an LDAP server. It is output as a file to a client PC once, and it is registered on the registration screen of MyPanel Manager by uploading the file. When uploading a file, data is sent safely using SSL.

Only a user who is registered as an administrator of MyPanel Manager can perform the registration.

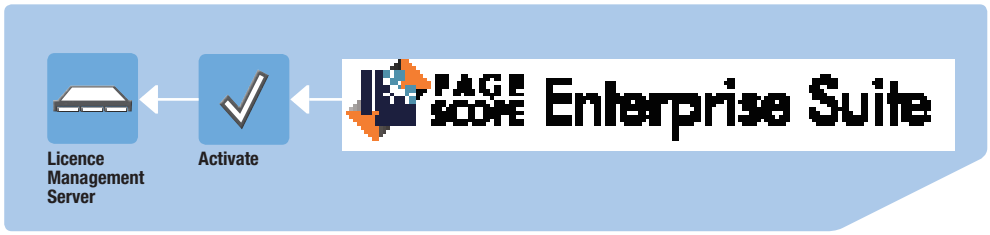


PageScope MyPanel registration using the Address Importer.

Licence management for PageScope Enterprise Suite

The PageScope Enterprise Suite software must be purchased. In accordance with the devices to be managed, please purchase the basic software module and the required number of licences. Communicate with the licence management server on the Internet managed by Konica Minolta, and confirm the availability of the licence key. After that, PageScope Enterprise Suite is available.

The key to enter for activation is a unique key that Konica Minolta issues, and it is tightly controlled by Konica Minolta. In communication with the Licence Management Server, data is sent safely using SSL.



Activation to Licence Management Server.

SCAN SECURITY

POP before SMTP

To secure access of the MFD 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 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)

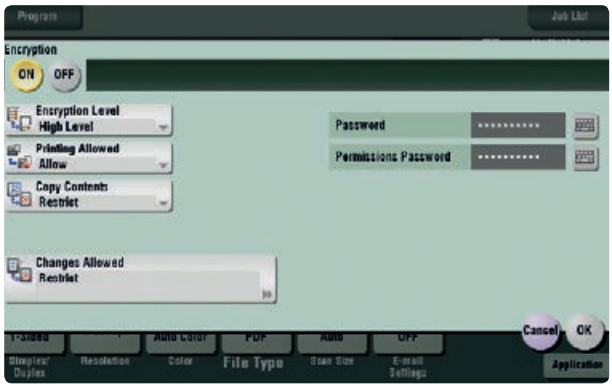
SMTP (Simple Mail Transfer Protocol) authentication can be activated on bizhub MFDs. This authorises a device to send emails. For those customers who do not host their email services, the use of an ISP mail server is possible and supported by the machine. SMTP authentication is required by, for example,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

S/MIME

For email transmission, the MFDs support S/MIME (Secure/Multipurpose Internet Mail Extensions) encryption.
S/MIME encryption is based on email certificates that can be registered on the MFD 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 at a high security level. For example, if an email is sent accidentally to a wrong destination, the email information can still only be opened by the intended recipient, who is the only one in possession of the “private key” necessary for decryption.

Encrypted PDF

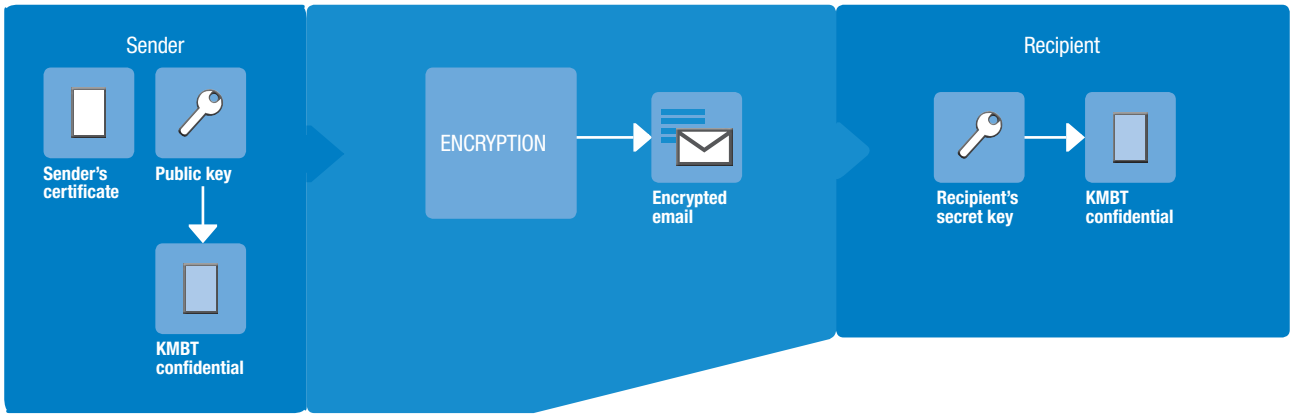
bizhub OP-based products can encrypt scanned files in PDF format before sending them to a destination across the network. The user has the ability to encrypt a scanned file by selecting the encryption key on the bizhub’s control panel. The encryption option supports the PDF file type, and will require the decryption code to open the file from the recipient of the scan.
This feature is very similar to the Adobe Acrobat encryption process where a password is 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 MFD scan settings for PDF encryption (bizhub C654).

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 MFD, certificates and/or public keys stored on the LDAP server can be used.



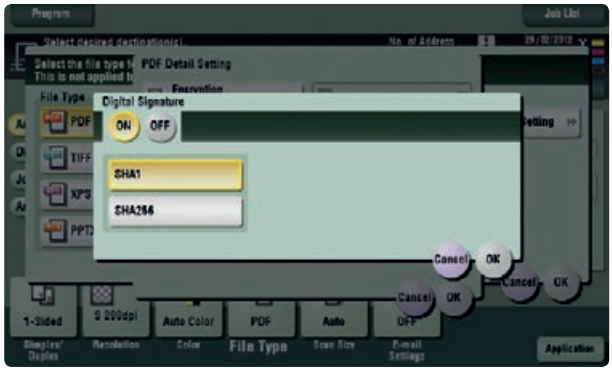
This illustration shows the encryption process via digital ID.

PDF digital signature

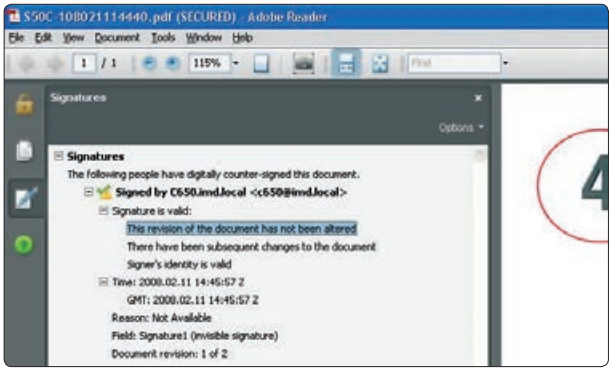
To prevent tampering with MFD-created PDF documents, it is possible to add a digital signature. The digital signature is based on the SSL certificate installed on, or used by, the MFD.

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 recognise invalid document sources.



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



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.

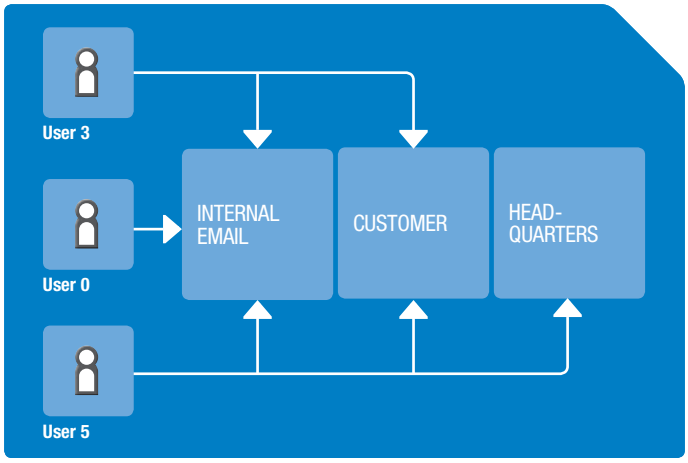
Manual destination blocking

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

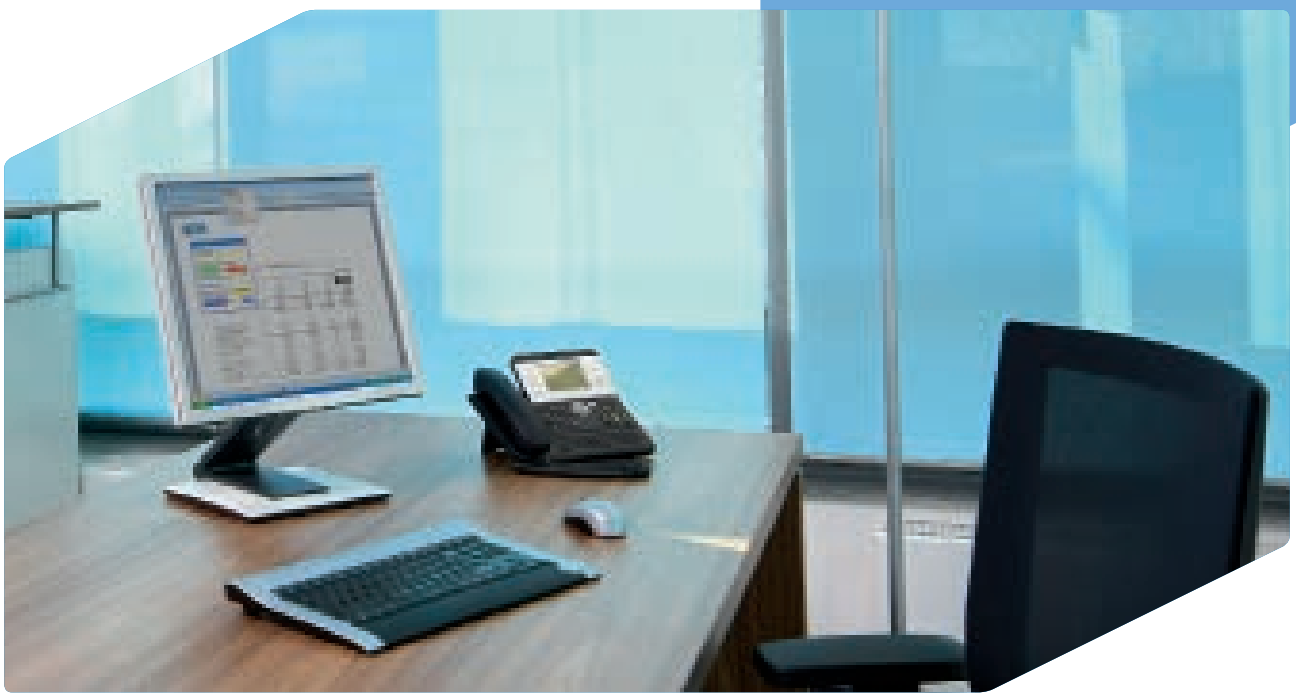
In addition to preventing the direct input of destinations, the user can be blocked from changing the FROM address for an email transmission. If the machine is set to authentication, the user’s email address stored in the authentication data or Active Directory will automatically be used.

Address book access control

The destinations (e.g. email, SMB, FTP) stored in the MFD 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

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 unauthorised users.

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

Unauthorised access lock

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

Mode 1	The machine lock-out will be released after a certain time (1–60 minutes)
Mode 2	In addition to mode 1, the number of wrong attempts can be specified (1–5)

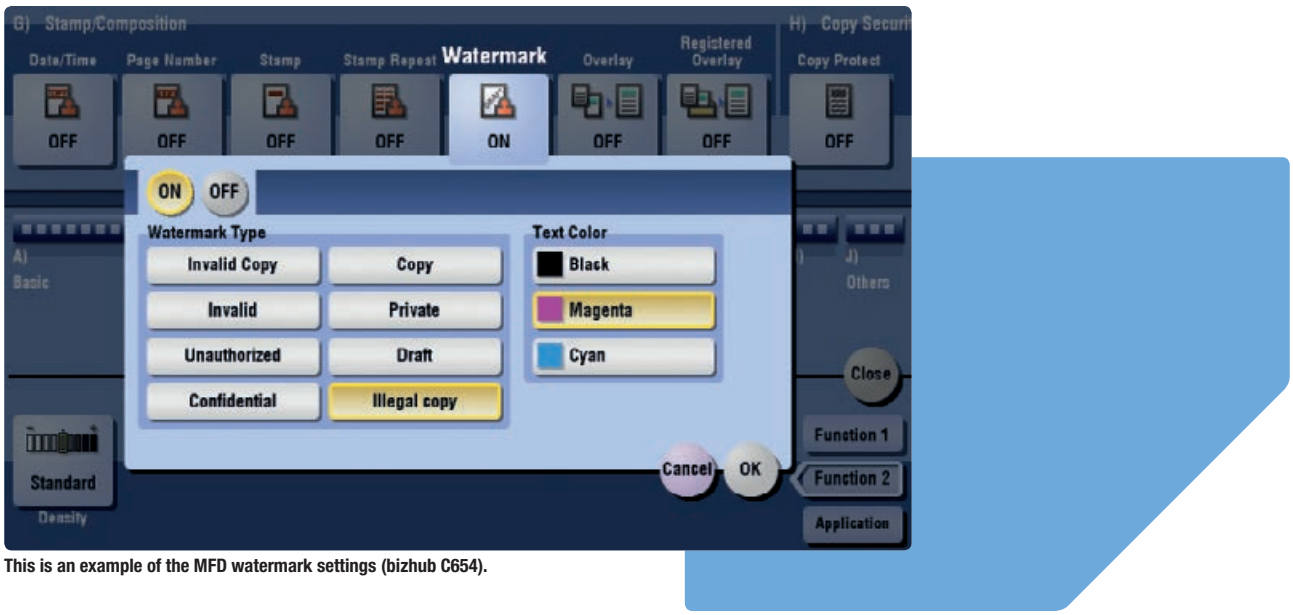
The unauthorised access lock can be extended to the system user box for confidential documents (secure print box). The same modes will be applied in the case of unauthorised access to this document storage location.

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 the easy identification of illegal copies made of this limited issue of documents.

Watermark/Overlay

All copies, prints and scans created on the MFD 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.

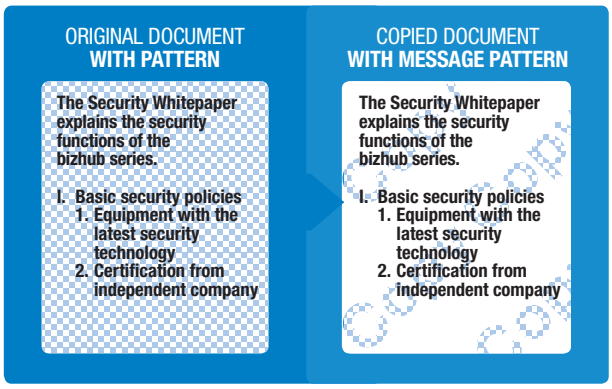


This is an example of the MFD watermark settings (bizhub C654).

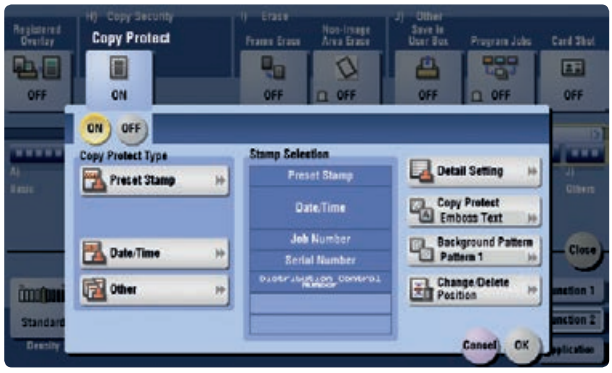
Copy protection via watermark

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.

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



This illustration shows the copy protection functionality.

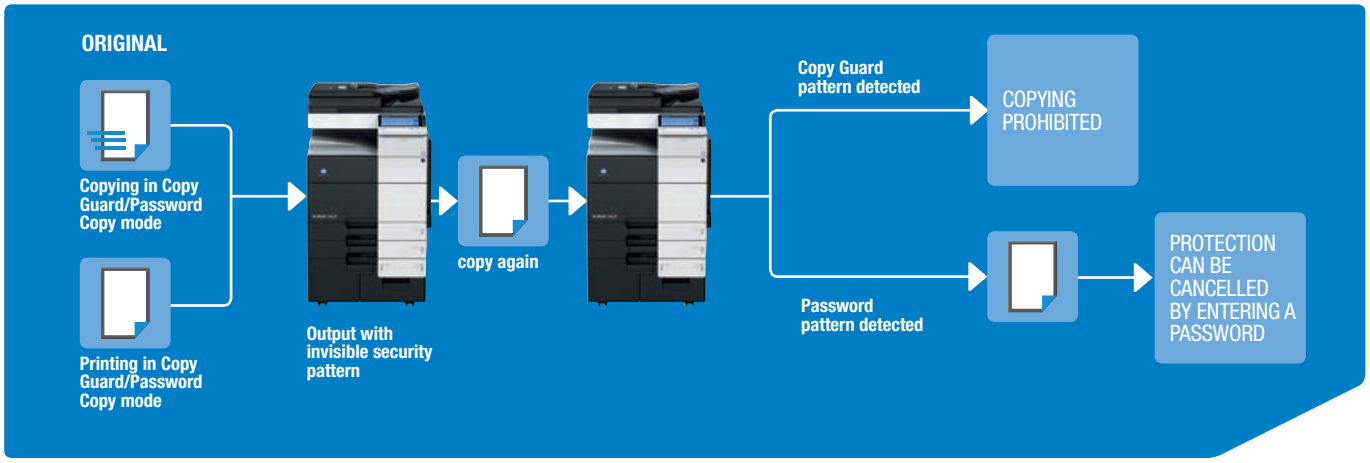


These are examples of the MFD copy security settings (bizhub C654).

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 MFD 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 MFD 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 unauthorised access to fax information, confidential or not.

SECURITY
FEATURES & AVAILABILITY

Features	Multifunctional colour systems				Multifunctional b/w systems							Print systems			
	bizhub C25	bizhub C35	bizhub C224 C284 C364 C454 C554	bizhub C654 C754	Konica Minolta 240f	bizhub 20	bizhub 36 42	bizhub 215	bizhub 223 283 363 423	bizhub 552 652	bizhub 501 601 751	bizhub C35P	bizhub C353P	bizhub 20P	bizhub 40P
Access control/Access security															
Copy/print accounting	/	x	x	x	x	/	x	x	x	x	x	/	x	/	o
Function restriction (copy/print/scan/fax/box/colour)	x***	x	x	x	x	x	x	/	x	x	x	o	x	/	/
Secure printing (lock job)	x	x	x	x	x	x	x	x	x	x	x	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	x	x	x	o	x	/	o
Finger vein scanner	/	/	o	o	/	/	/	/	o	o	o	/	o	/	/
IC card reader	/	o	o	o	/	/	o	/	o	o	o	/	o	/	/
Event log	/	/	x	x	/	/	/	/	x	x	x	/	x	/	/
Data security/Document security															
Data encryption (hard disk)	/	x***	x	x	/	/	x***	/	x	x	o	/	o	/	/
Hard disk data overwrite	/	x	x	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	x	x	x
Port and protocol access control	x	x	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	x	x	x	x
IP sec support	x	x	x	x	/	/	x	/	x	x	x	x	x	/	x
S/MIME	/	x	x	x	/	/	x	/	x	x	x	/	/	/	/
IEEE 802.1x support	x	x	x	x	/	/	x	/	x	x	x	x	/	/	x
Scanning security															
User authentication	/	x	x	x	/	x	x	/	x	x	x	/	/	/	/
POP before SMTP	x	x	x	x	x	x	x	x	x	x	x	/	/	/	/
SMTP authentication (SASL)	x	x	x	x	x	/	x	/	x	x	x	/	/	/	/
Manual destination blocking	/	x	x	x	/	/	x	/	x	x	x	/	/	/	/
Others															
Service mode protection	x	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	x	x	x
Data capturing	/	/	x	x	/	/	/	/	x	x	x	/	x	/	/
Unauthorised access lock	/	x	x	x	/	/	x	/	x	x	x	x	x	/	/
Copy protection via watermark	/	x	x	x	/	/	x	/	x	x	x	/	x	/	/
Encrypted PDF	/	x	x	x	x	/	x	/	x	x	x	/	/	/	/
PDF signature	/	/	o	o	/	/	/	/	o	o	o	/	/	/	/
PDF encryption via digital ID	/	/	o	o	/	/	/	/	o	o	o	/	/	/	/
Copy Guard/Password Copy	/	/	o	o	/	/	/	/	o	o	/	/	/	/	/
ISO 15408 certification															
ISO 15408 EAL3 certified	/	x	x**	x**	/	/	x**	/	x	x**	x	/	x	/	/

x = standard o = option / = not available * for print only ** in evaluation * with reservations**

NOTES

KONICA MINOLTA

Common Criteria Validated

Your Konica Minolta Business Solutions Partner:

CDT Group Ltd
Geodis Building
Coronation Road
High Wycombe
Bucks
HP12 4PW
Tel 01494 532222
www.citydigital.com

08/2012