EPSON

Security Guidebook

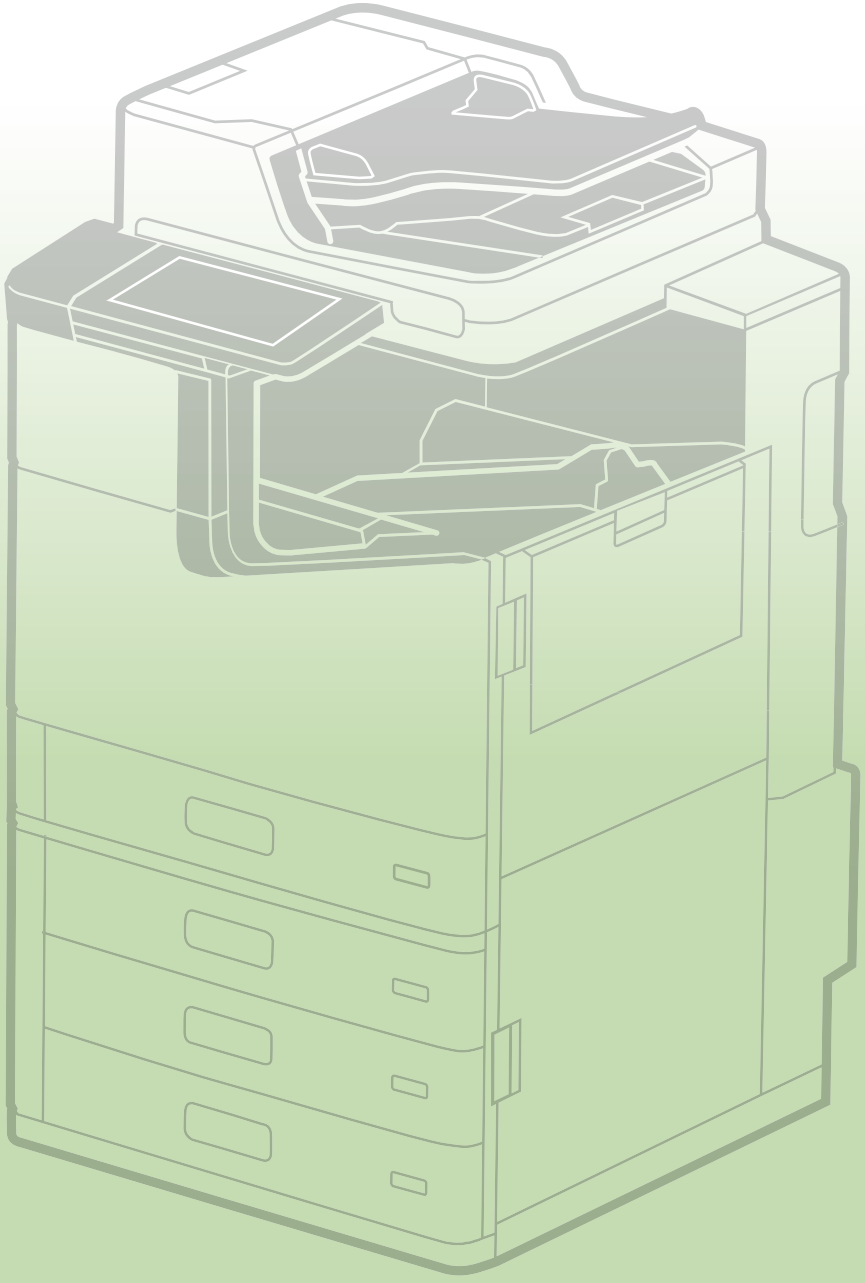


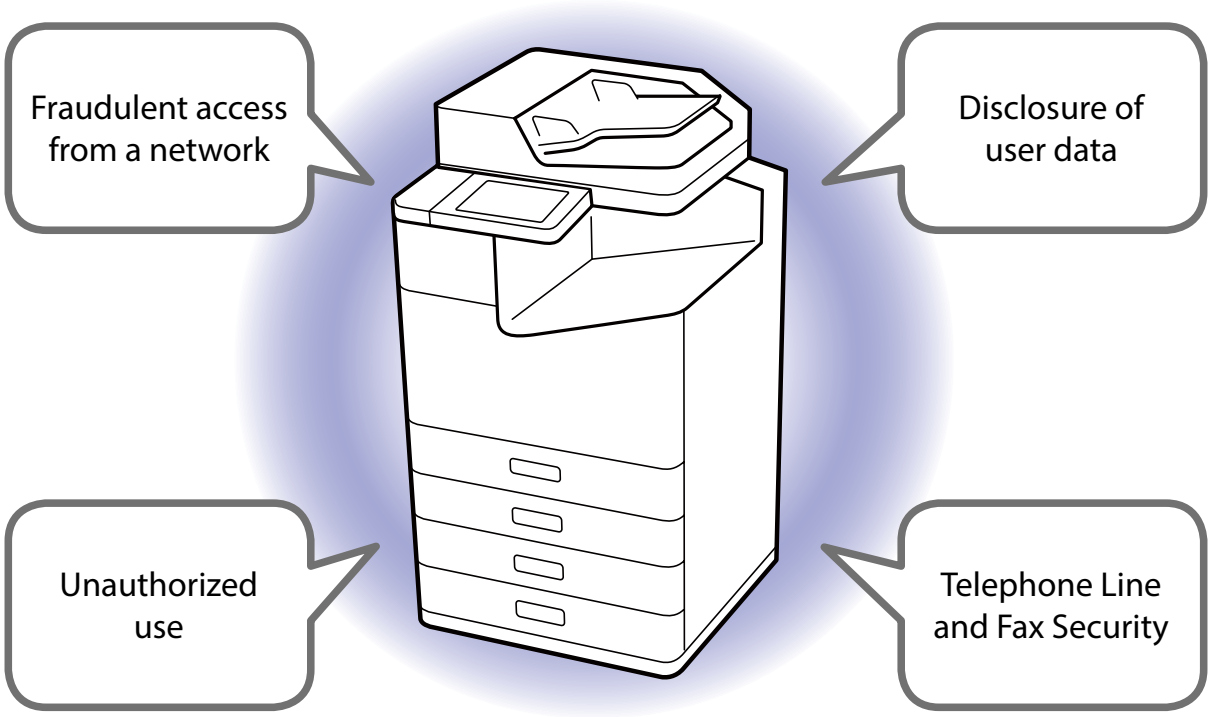
Table of Contents

1. Introduction

At Epson, we have been enhancing the network-compatible features of our products to improve customer convenience.

Meanwhile, the increasing sophistication and complexity of cyberattacks by malicious third parties have increased threats to devices connected to the network, raising concern about security measures.

Because Epson's products are equipped with a variety of features, proper consideration for security is necessary, especially when they are connected to a network, as is the case with computers and servers.



This guidebook introduces Epson's approach to security and advice for the customer, and guides you through the security functions available for use.

The icons next to each function in the text have the following meanings.

: Security features with this mark are the minimum settings that should be done by the administrator.

: Security features with this mark can only be configured by the administrator and are available to users in the configured security environment.

: Security features with this mark can be set and used by administrators and users.

: Other security features. Applicable for security features built into products as part of their specifications.

Check your product's manual for how to set up security.

Note that the security functions and compliance with security standards outlined in this guidebook vary depending on the product being used. Some products may not have such features or do not comply with such security standards. So, be sure to refer to the list of features in the separate Security Guidebook for the compatibility of each product.

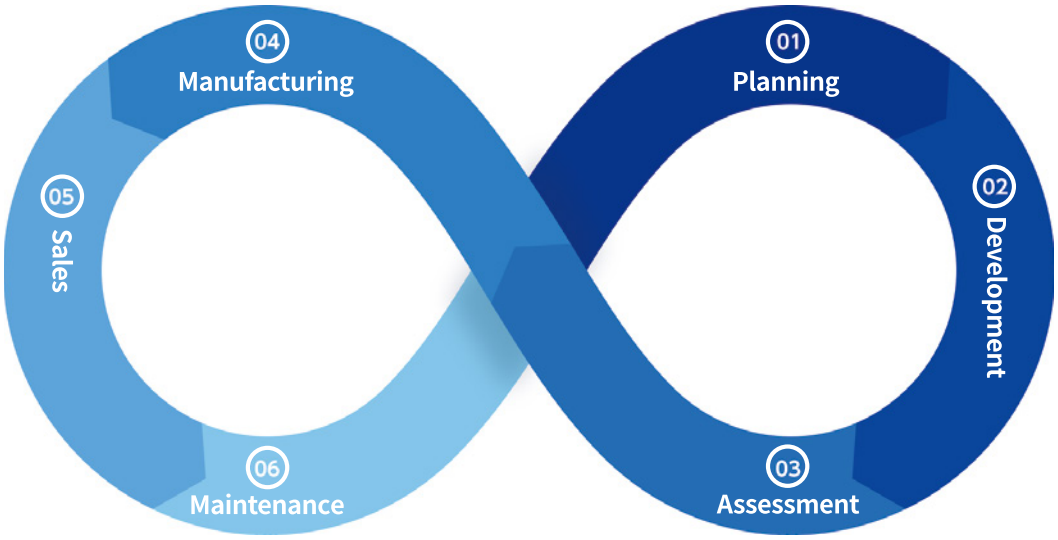
2. EPSON's Security Basic Policy

At Epson, we take the following approach regarding security so our customers can use our products safely and with ease.

2-1. Basic Policy

Epson views product security as the cornerstone of product quality.

We practice product (endpoint) security throughout the entire lifecycle from planning, development, evaluation, manufacturing, sales, and maintenance to ensure that customers can use our products in more secure conditions by closely examining the diverse usage environments for each product genre.



① Planning

At the product planning stage, we continuously monitor the newest security trends and potential vulnerabilities. We also listen to our customers' requests, identifying and analyzing security-related requirements. This way, we eliminate potential problems in our products before any risks can materialize.

② Development

Using our original common platforms and technologies cultivated throughout the development of a wide range of products, from office/home printers to commercial/ industrial small and large format printers, we strive to enhance the protection against security risks.

③ Assessment

In addition to thorough in-house testing, we also involve third-party organizations for objective security assessment. With our strict security verification system, we conduct the assessment from different angles to ensure high security for our products.

④ Manufacturing

To ensure the highest quality of our manufacturing operation, we have implemented a thorough information asset management system at our factories, where we install software that enables the functionality of our products.

⑤ Sales

We are committed to supporting our customers by proposing and implementing solutions to minimize security risks depending on the use environment and operational conditions. We also make sure to quickly address any vulnerabilities that may arise after the installation of our products.

When products need to be replaced and disposed of, we make sure to reset the devices to the factory default settings to prevent confidential information leaks.

⑥ Maintenance

We quickly respond to security-related issues and concerns reported by clients who purchase our products.

2-2. Providing Information

We actively provide our customers with information and actively keep them aware of security.

2-3. Support in Responding to Vulnerabilities

We are constantly addressing vulnerabilities.

- We test for vulnerability using the industry's standard tools and strive to ship products free of vulnerabilities.
- We regularly monitor information about vulnerabilities from open source software used in the firmware of our products.
- When new vulnerabilities are found, we promptly analyze them and provide information and countermeasures.

2-4. Compliance with Codes and Standards

We strive to comply with and obtain security standards.

3. What You Should Do When You Install Your Product

To ensure optimal security, read the following during installation and configure the necessary settings according to your usage environment.

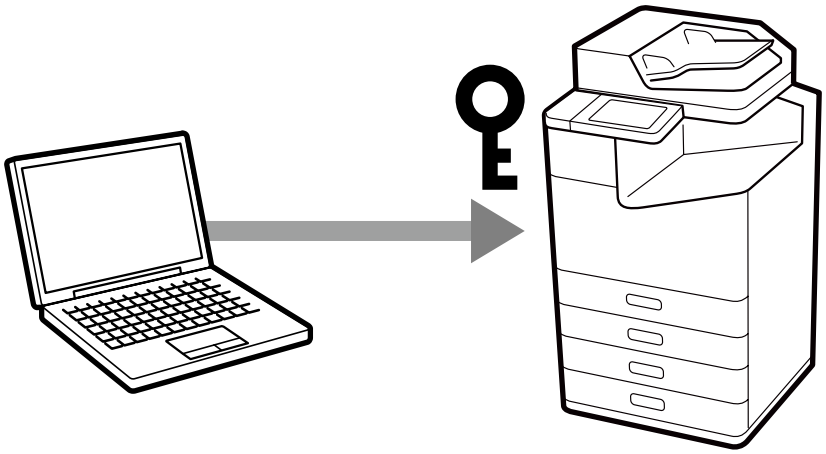
3-1. Administrator Password

We strongly recommend setting up an administrator password during installation of each product.

The general settings and network settings that are stored in the product may be accessed or changed illegally if an administrator password is not set or if the product is left at its factory default settings. There is also the risk of not safeguarding personal and confidential information, such as address books, IDs, and passwords.

The administrator password should be a complex character string that is difficult for other users to guess. It should consist of 8 or more characters, including not only English letters but also symbols and numbers. You can set up the administrator password directly in the settings of the product's control panel or through the network.

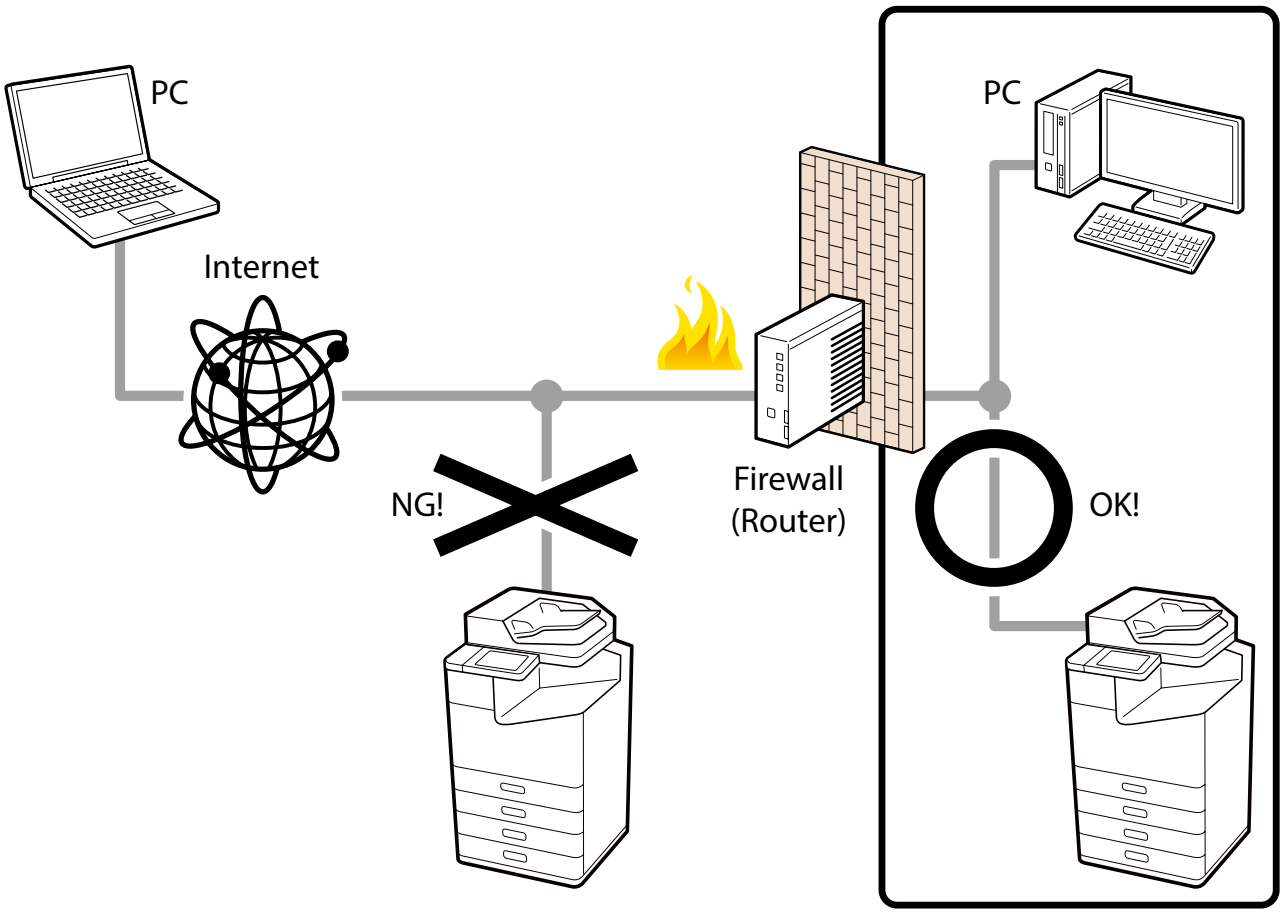
So, some products have individual passwords set at the factory to enhance security.



3-2. Internet Connection

Install products on a network protected by a firewall without connecting directly to the internet. We recommend setting up and utilizing a private IP address when you do this.

Even when using the product in an IPv6 environment, be sure to restrict access to the product using a firewall or other means to prevent direct access to the product from the internet.



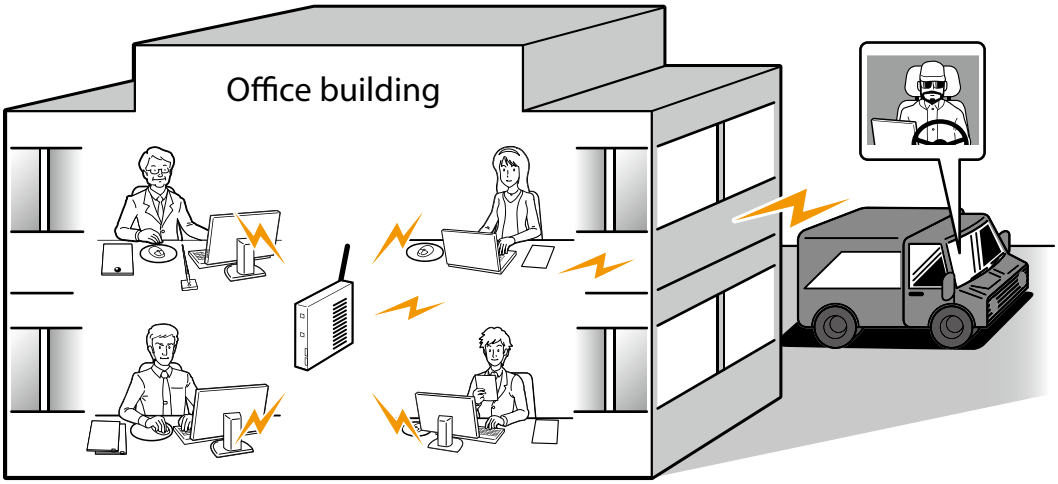
Management interfaces, such as a web management screen, are included for the products' network functions as well as printing. Although Epson conducts vulnerability testing and strives to ship products that are free of vulnerabilities, direct connection to the internet poses unexpected security risks, such as unauthorized operation and information leaks, to the customer's network and devices connected to the network.

3-3. Wireless LAN Network

When using a wireless LAN network, set up the wireless LAN's security appropriately.

The advantage of wireless LAN is that you can freely connect to the product via a network to communicate with computer and smart phone terminals if you are within range of a signal. On the other hand, problems like the following, caused by malicious third parties, may occur if security is not properly set up.

- Personal information, such as your print data, scan data, ID, and password, may be seen by others (intercepted)
- Communication content may be fraudulently rewritten (falsified)
- Certain people or devices may be impersonated and used for communication (identity theft)



See the product manual for the procedure to set up a wireless LAN.

3-4. Disabling Unused Protocols and Functions

Disable protocols and functions that are not used.

Each protocol and function can be allowed or prohibited individually, preventing security risks if they happen to be used unintentionally.

3-5. Update to the Latest Firmware and Software

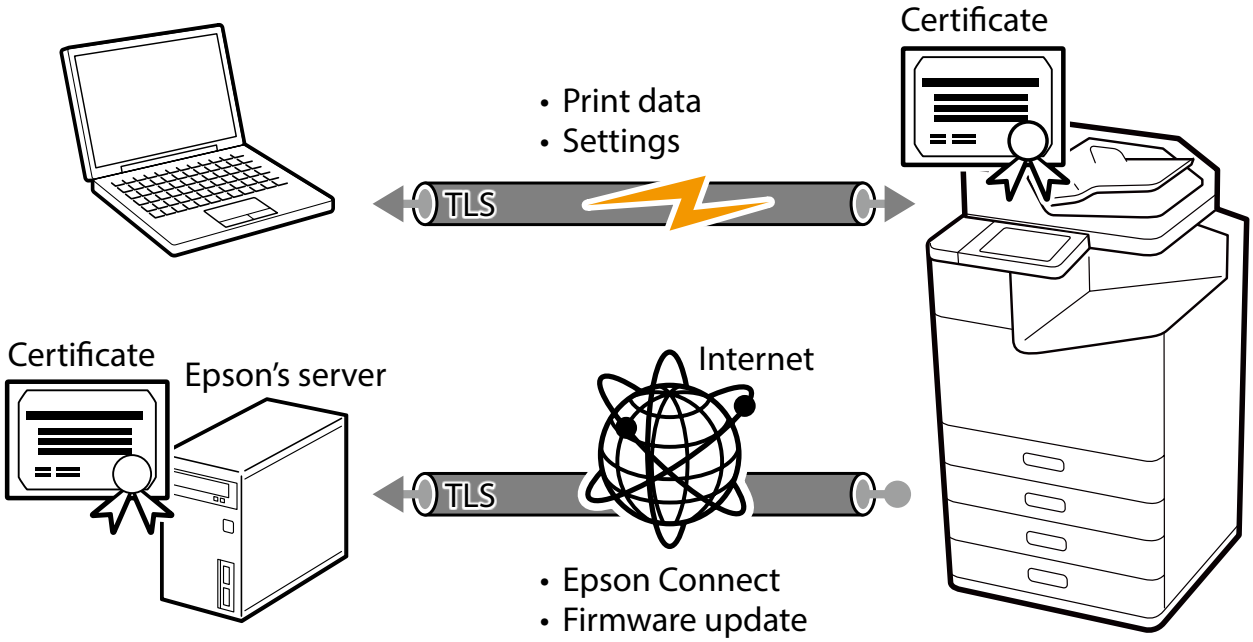
We provide the latest firmware and software as needed. Be sure to update to the latest firmware to use the product.

The latest firmware and software include not only additional functionality, but also fixes for defects and vulnerabilities. For more information on the firmware or software, see the history of modifications for the firmware or software.

4. Network Security

4-1. TLS Communication

Since transmissions are protected by TLS, you can prevent the disclosure of setting information and the content of print data by using the IPPS protocol for printing and configuring your product via your browser. You can also prevent information from being sent to unauthorized devices by using the server validation function, importing the CA-signed certificate, and working with the in-house public key infrastructure (PKI). Encryption strength can be configured to use a much safer encryption algorithm. You are also protected by TLS when you access the Epson server on the internet through the product for Epson Connect and firmware updates.



You can select the version and encryption strength of the TLS to be used.

The supported TLS versions and encryption strengths are as follows.

TLS Version

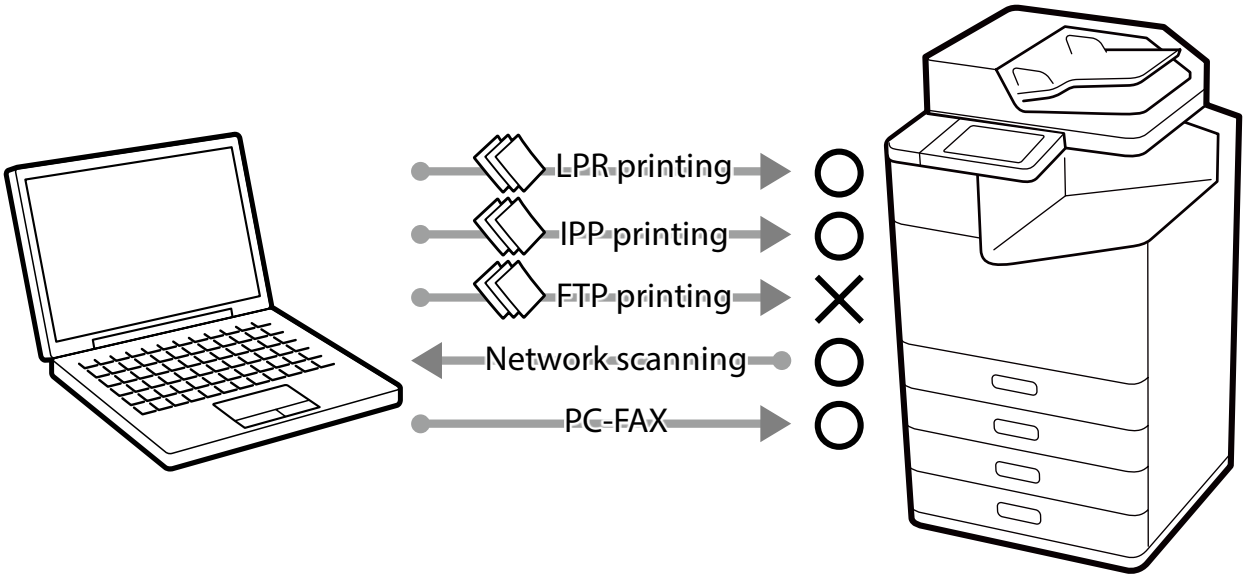
- TLS1.1
- TLS1.2
- TLS1.3

Encryption strength

- 80bit
- 112bit
- 128bit
- 192bit
- 256bit

4-2. Controlling Protocol Permissions and exclusions

The product communicates through various protocols when printing, scanning, and sending a PC-FAX. You can prevent security risks from unintended use before they happen by setting up individual permissions and prohibitions for each protocol.



See the appendix for security risks when protocols and features are enabled and for limitations when they are disabled.

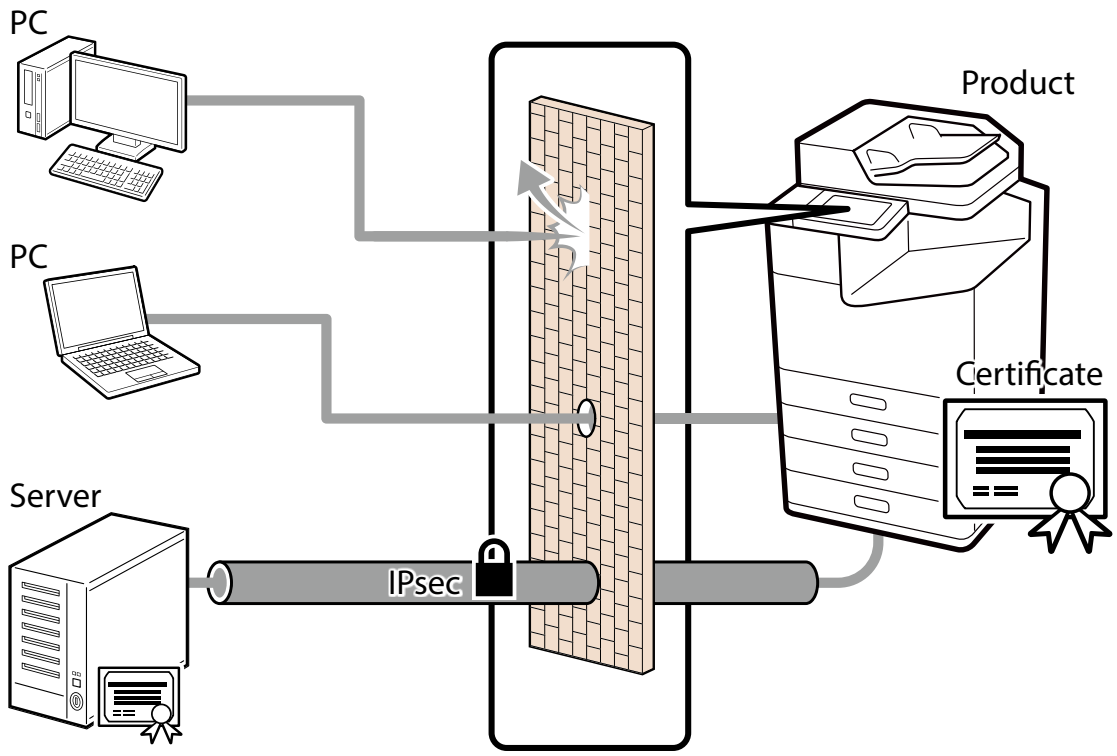
The protocols and features that can be allowed or prohibited are as follows.

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW (Port9100/Custom Port)
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Microsoft network sharing
- Network Scan (EPSON Scan)
- PC-FAX

4-3. IPsec/IP Filtering

You can filter IP addresses, types of services, reception and transmission port numbers, etc. by using the IPsec/IP Filtering function. Depending on the combination of these filters, you can set up whether to accept or block data from a particular client and to accept or block specific types of data. Likewise, you can communicate with stronger security by combining protections by using IPsec.

Insecure printing protocols and scanning protocols also become protected objects because protection in IP packet units (encryption and certification) is included in protection by using IPsec. Pre-shared keys and certificates are supported in the IPsec authentication methods.



The supported algorithms and key exchange methods are as follows:

Key Exchange Method

- IKEv1
- IKEv2

ESP Encryption Algorithm

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256

- 3DES

ESP/AH Authentication Algorithm

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

The basic policy affects all users who access the product. Set up individual policies to control access based on your specific needs.

4-4. IEEE802.1X Authentication

IEEE802.1X is a standard for controlling access at each port of the network device. IEEE802.1X networks are compiled of RADIUS servers (authentication servers) and switching hubs that have an authentication function.

Epson products are compliant with IEEE802.1x and can be connected to a network environment that contains some confidential information.

The following authentication methods and encryption algorithms are supported:

Authentication Method

- EAP-TLS
- PEAP-TLS
- PEAP/MSCHAPv2
- EAP-TTLS

Encryption Algorithm

- AES128
- AES256
- 3DES
- RC4

4-5. SNMP

SNMP is a protocol for monitoring the status of and changing settings of supported equipment and management tools.

SNMPv1 and SNMPv2c do not support encryption of communications and should be used within a network protected by a firewall or something similar. Also, to use SNMP communications, change the community name from the default value.

SNMPv3 can be used to authenticate and encrypt SNMP communications (packets) for monitoring status and configuring changes with compatible device management tools. This can ensure confidentiality when changing settings or monitoring status over the network.

SNMPv3 supports the following authentication and cryptographic algorithms.

SNMPv3 authentication algorithms

- MD5
- SHA-1

SNMPv3 encryption algorithms

- DES
- AES128

4-6. SMB

SMB is a protocol for sharing files over a network.

SMB1.0 and SMB2.0 do not support encryption of communications and should be used within a network protected by a firewall or something similar.

SMB3.0 can be used to authenticate and encrypt SMB communications (packets) with compatible devices. This can ensure confidentiality for file sharing over the network.

4-7. WPA3

The product supports WPA3 which is the latest authentication and encryption technology for Wi-Fi (wireless LAN). WPA3 provides a more robust and stronger protection to safeguard your data over the wireless network.

4-8. Separation Between Interfaces

The product includes a USB interface, standard wired LAN interface, additional wired LAN interface, wireless LAN interface, and fax interface. Each interface is independent, restricting access only to protocols that can be handled by that interface, and does not provide any direct transfer or routing capabilities. As a specific example, access from a public telephone line (fax line) is restricted to processing according to fax communication procedures. Any deviation from that procedure will result in disconnection of communication as an error, so there is no risk of unauthorized access. In addition, received fax data is checked for correctness as image data before being imported. There is no risk of malicious malware being planted via the transfer function through the product that could lead to virus contamination or unauthorized access. Only authorized users can execute the transfer function. For example, intrusion of the network from a public telephone line via the product; access to a wired LAN from a wireless LAN; or unauthorized access from the Internet to the product connected to a computer via a USB.

5. Protecting Your Product

5-1. Block USB Connection from Computer

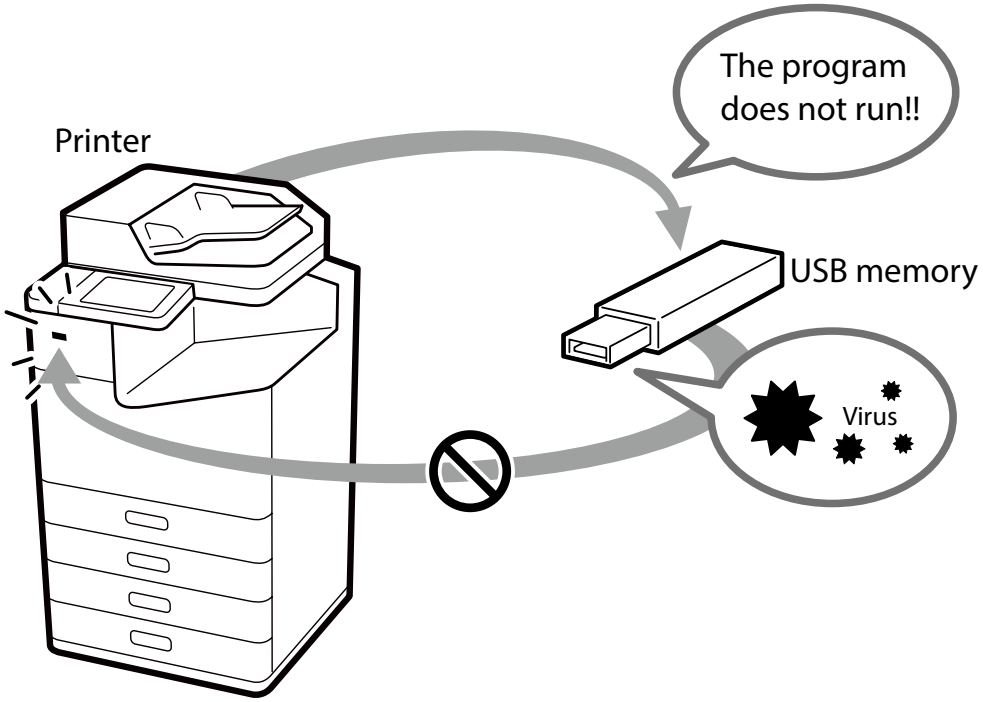
You can disable access to the product via USB connection from a computer. Set this option to prohibit printing or scanning by a direct connection to a computer by a USB cable.

5-2. Disabling the External Interface

You can disable memory cards and USB memory interfaces. This allows you to prevent the illegal duplication of data by unauthorized scanning of confidential documents in the office.

5-3. Handling Viruses Introduced by USB Memory

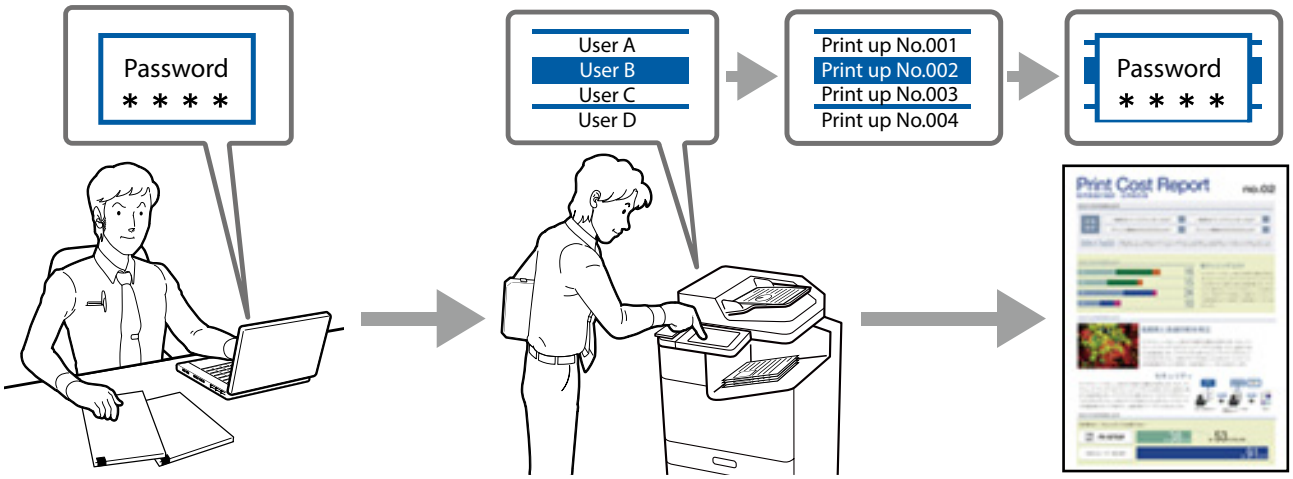
Since there are no executable functions on USB memories for Epson products, there is no danger of the product being infected with viruses via USB memory.



6. Print / Scan Security

6-1. Confidential Jobs

You can ensure document privacy /confidentiality and prevent unauthorized people from viewing unattended output at the device by submitting your documents as a "Confidential Job".



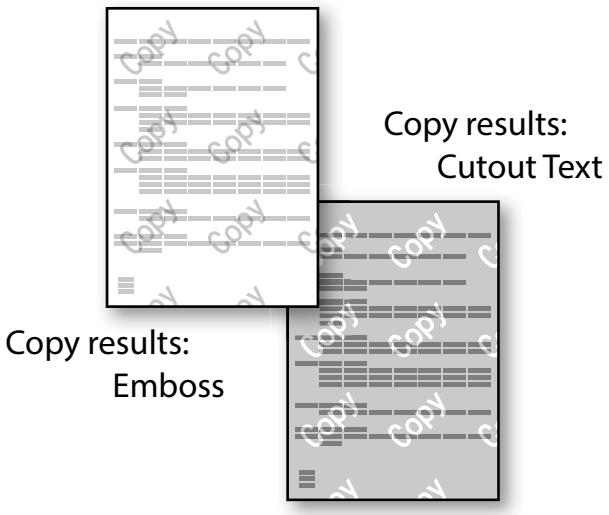
Enter a password to print.

Choose a print job on the product and input the password.

Printing is complete.

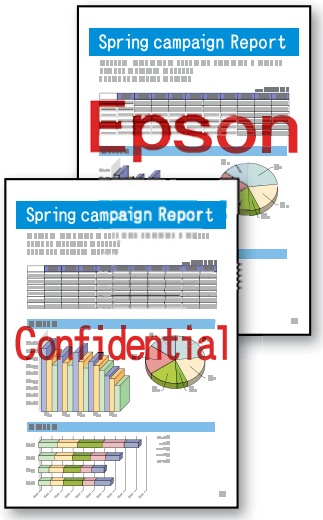
6-2. Anti-Copy Pattern

You can protect the originality of a document with anti-copy watermark printing which creates a transparent watermark pattern on the original output. The transparent watermark will become visible when the original output is used to make copies.



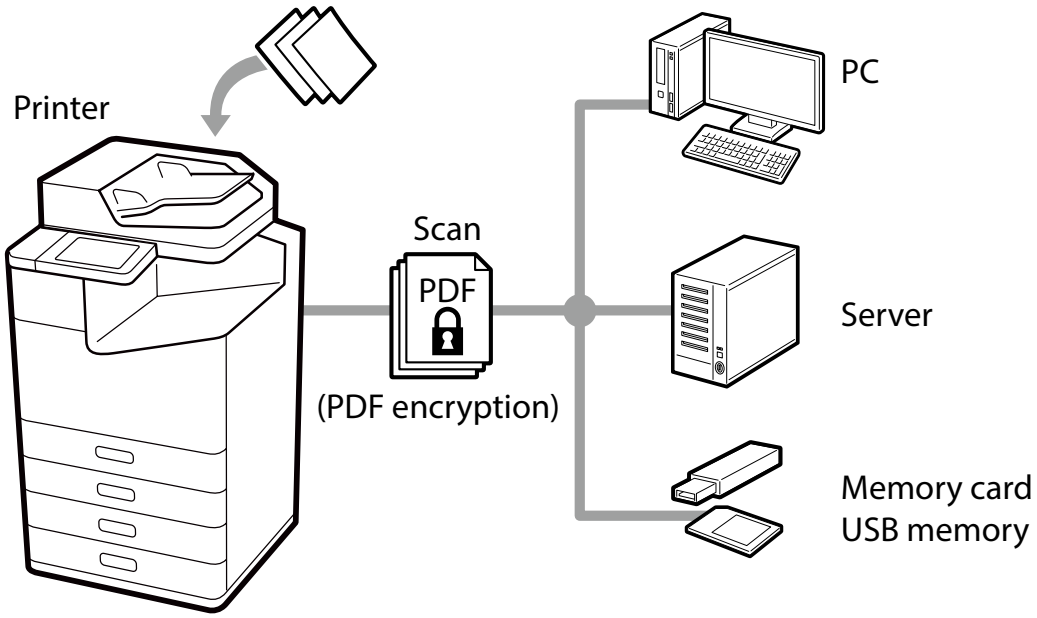
6-3. Watermark

Watermarks such as classified and important (in text or BMP format) can be superimposed on documents. Additionally, you can also choose a "user name" or a "computer name". Reminding the recipient to handle the documents carefully deters unauthorized use.



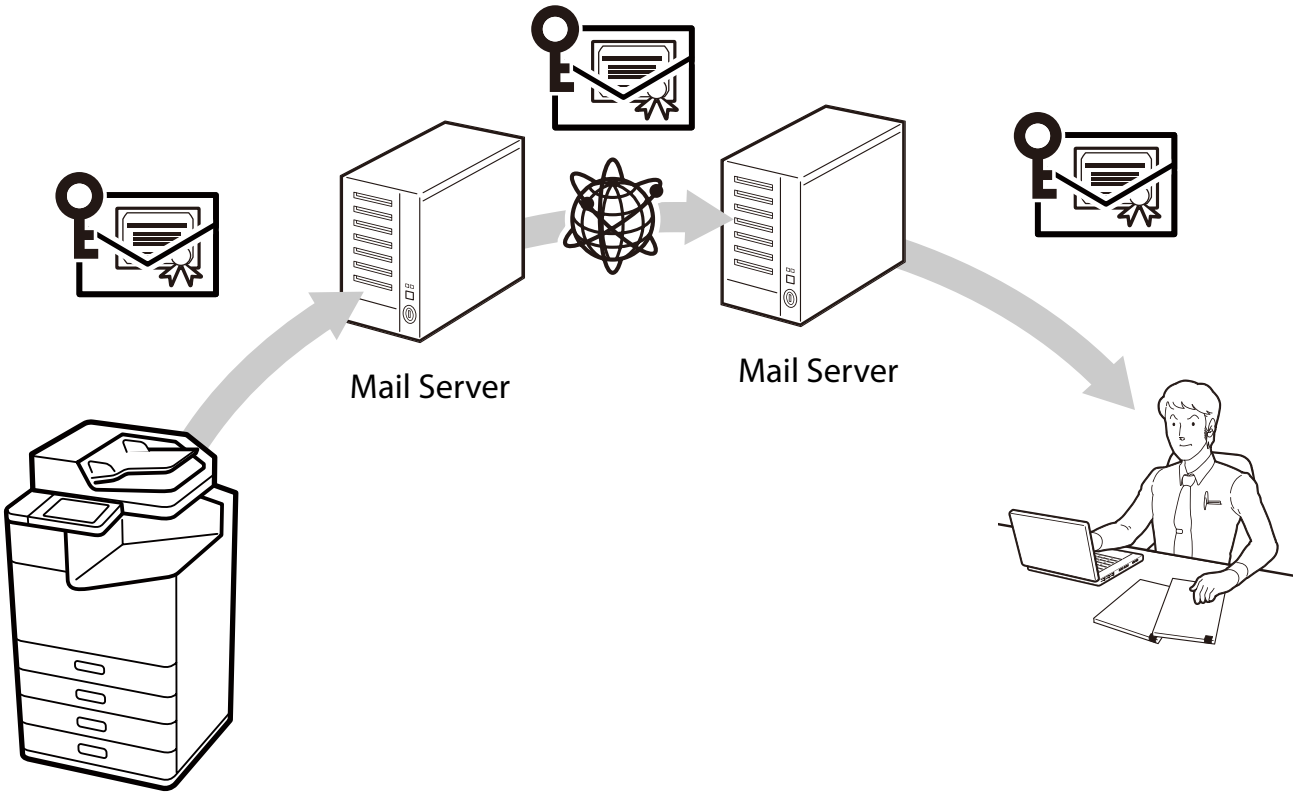
6-4. PDF Encryption

You can scan a document into a password-protected PDF file. This can prevent third parties from viewing documents without authorization.



6-5. S/MIME

Using S/MIME allows you to add a digital signature and/or encrypt an email for Scan to Email and Fax to Email. Even if an email goes through multiple email servers, you can protect the email from being falsified, intercepted, or tampered with. S/MINE will safeguard the authenticity and integrity of the message while protecting data security and enduring non-repudiation.



Supported algorithms are as follows.

Encryption Algorithm

- AES-128
- AES-192
- AES-256
- 3DES

Digital Signature Hash Algorithm

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

6-6. Domain Restrictions

By applying restriction rules to the domain names of email addresses, you can reduce the risk of mistaken transmissions and information leaks for the Scan to Mail and fax forwarding email functions.

6-7. Support for Long Authentication Passwords

Nowadays, setting long passwords is being recommended to increase password security. You can set a maximum of 70 characters as the authorization password used for Scan to Network Folder/FTP, Scan to Email, Email Notification. You can set a password policy for longer passwords for file servers and mail servers.

6-8. Restrictions on File Access from PDL

By disabling file access from PDL (page description language), you can prevent the risk of information leaks from malicious print data that steals files from inside the printer. Even if malicious print data is transmitted, the product can be used safely without files being read.

6-9. Secure Printing

If you want to protect the security of transmission routes for printing, you can use an IPPS encrypted through TLS.

7. Fax Security

7-1. Direct Dialing Restrictions

If you want to enter a fax number directly using the numeric key pad, you can set it up so the fax only sends if you enter the destination twice correctly. You can also set it up so that entering a phone number directly using the numeric keypad is prohibited and faxes are sent only through one touch dialing and to addresses registered in your address book. This can reduce the risk of information leakages from wrong transmissions due to errors in phone number input.

7-2. Confirmation of Address List

You can confirm the selected address before you send a fax. This can reduce the risk of information disclosure from wrong transmissions due to errors when specifying an address.

7-3. Dial Tone Detection

You can prevent wrong transmissions by sending faxes after confirming the detection of a dial tone.

Depending on your country or region, dial tone detection may not be possible.

7-4. Measures Against Abandoned Faxes

"Print fax after viewing" can be set up to save a received fax to the inbox (memory reception) and print it after you have confirmed it on the control panel. This prevents information disclosure and the loss of printed material from received faxes due to printed faxes being left unattended.

Also, you can prevent arbitrary printing and deletion by unauthorized users by setting it up so that a password is required to access the inbox.

7-5. Transmission Confirmation Report

You can confirm that a fax has definitely been sent to the correct address by printing out reports that confirm the transmission details, such as a sending results report, forwarding results report, and sending management report.

7-6. Deleting the Backup Data for Received Faxes

Backup data* for received faxes can be deleted from the control panel. You can also set it up so that backup data is deleted automatically, preventing unauthorized reprints of data from received faxes.

* Backup data for received faxes is saved in the product (factory default settings) so you can reprint faxes in cases where print results are unclear or print results are lost.

7-7. Limit Sending to Multiple Recipients

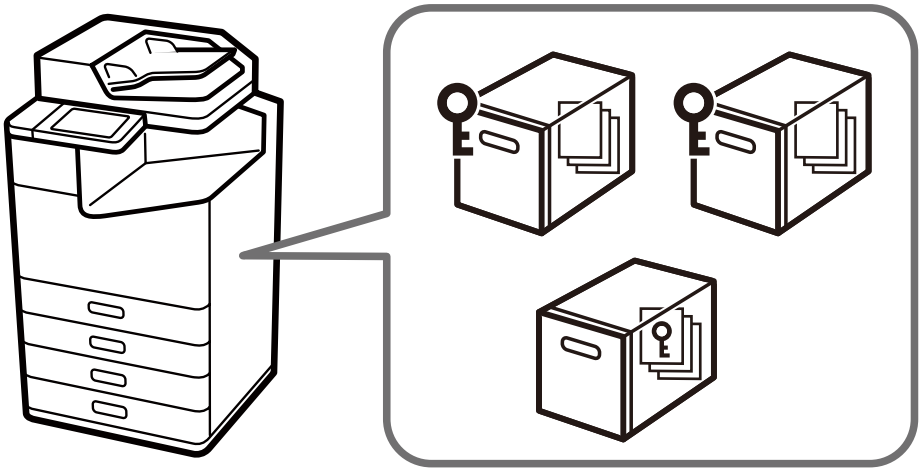
You can set the product so that only 1 recipient can be selected.

By making it impossible to specify multiple recipients, you can decrease the risk of sending a fax to an unintended recipient and disclosing information.

8. User Data Protection

8-1. Storage Security

You can set unique passwords for shared folders and documents on models with shared folders. These passwords can prevent information disclosures, losses, and unauthorized tampering. Also storage operation can be subject to access control. If shared folders are not being used, you can also prohibit the use of the shared folder function.



8-2. Protecting Your Address Book

You can prevent leakage and unauthorized alteration of address book information because an administrator password is required for batch editing of address books stored in the product (when an administrator password has been set up). Also, since address books can be exported as an encrypted file, you can prevent the disclosure of personal information, such as fax numbers and e-mail addresses, when replacing or backing up the product.

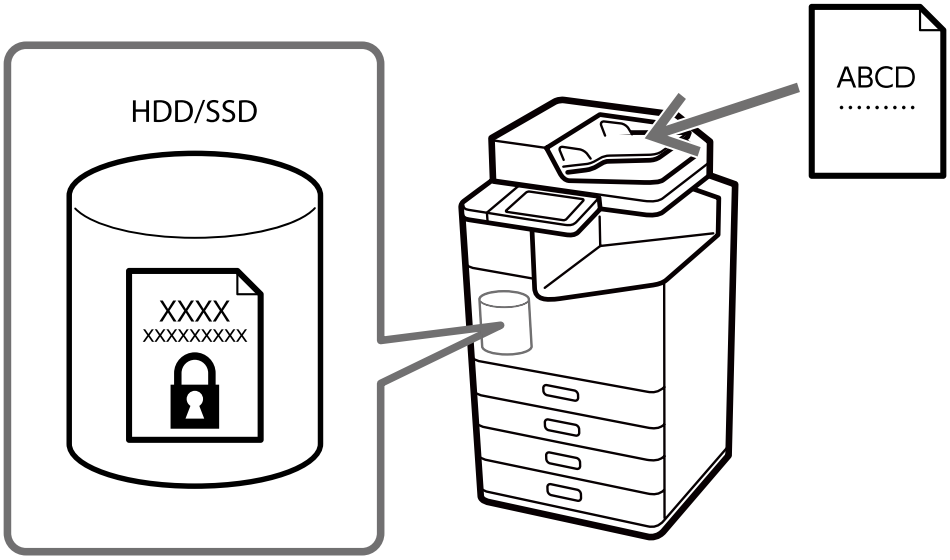
8-3. Data Handling Processed by a Product

Data of Print, Copy and Scan functions is saved temporally in a product, then it is cleared when a job is finished or the product is turned off. Fax data is cleared when sending or receiving faxes completely. Note that although received faxes are saved as data and retained by the backup function, you can change the setting so that the data is automatically erased (see 7-6).

8-4. Encryption of Saved Data in HDD/SSD

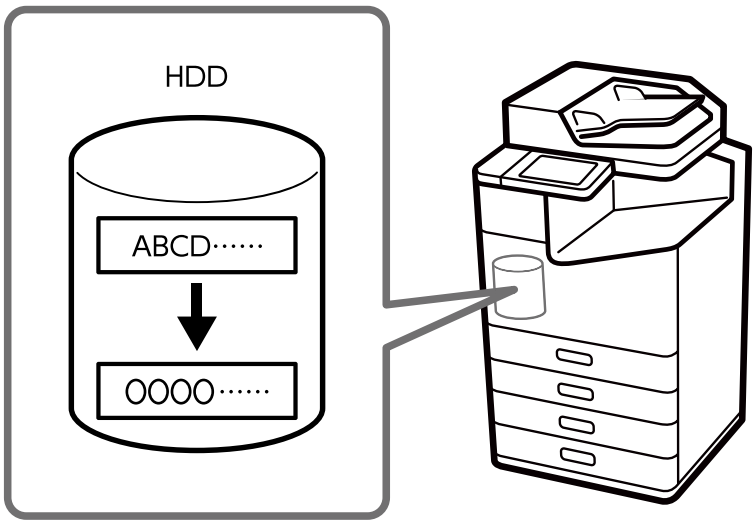
We always protect customer data with encryption when saving data onto an internal HDD/SSD on a product. In the unlikely event of an attack by a malicious third party, the contents of the stored data will not be visible. The HDD/SSD comes with a self-encrypting drive, and the document data is encrypted with AES-256.

Encrypting the data prevents unauthorized access or malicious attack to personal data if the HDD/SSD is stolen.



8-5. Sequential Deletion of Job Data

When this function is enabled, job data temporarily stored on the unit's HDD is automatically erased after being overwritten with a special pattern. This prevents malicious third parties from recovering data from residual job data.



8-6. Password Encryption

You can encrypt passwords that are stored in the product. The information that is encrypted is as follows:

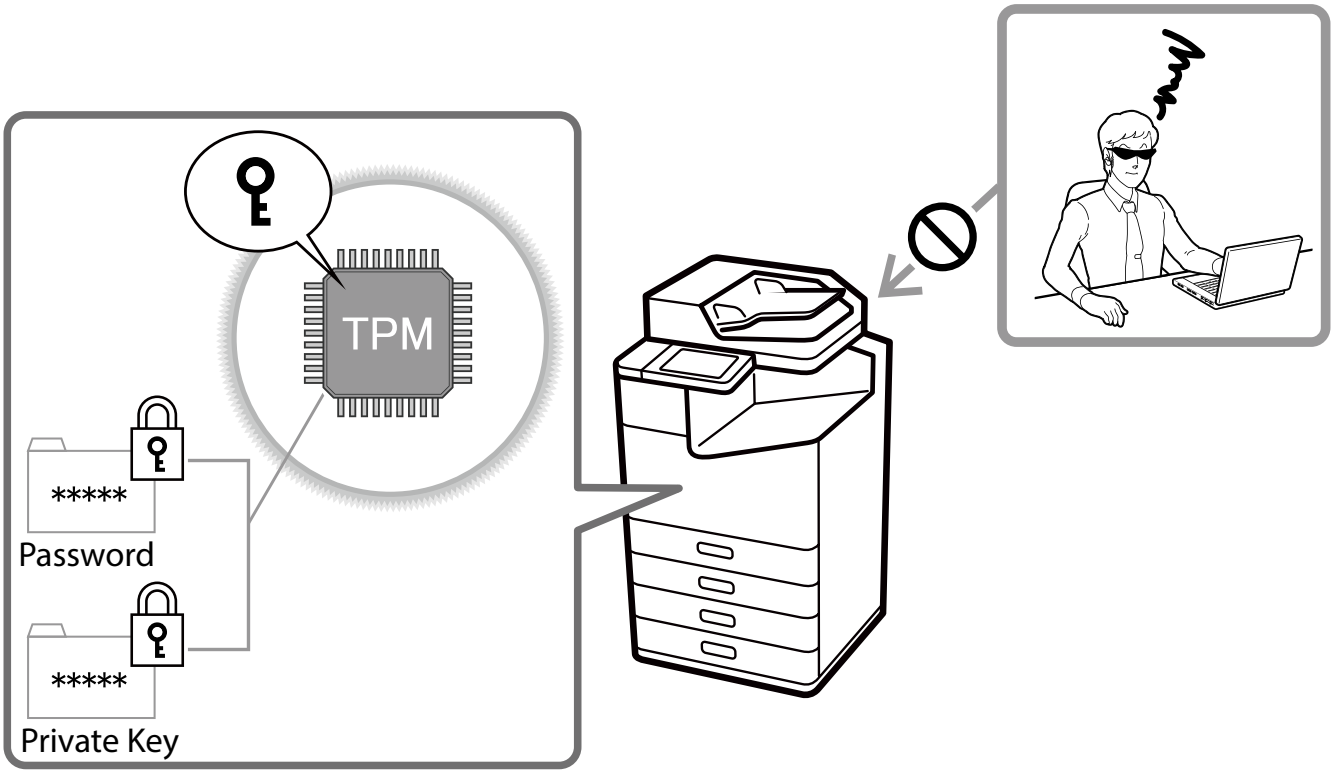
- Administrator Password
- User passwords for Access Control
- Hard Disk Authentication Keys, Certificate Private Keys, etc. Passwords to access for Scan to Network Folder/FTP

8-7. TPM

For models equipped with a TPM (Trusted Platform Module), the encryption keys for restoring encrypted passwords and private key information are stored on the TPM chip. The TPM chip cannot be accessed from outside the printer, protecting it from unauthorized analysis at the hardware level.

The TPM's true random numbers are used for the random numbers used for configurations via browser (Web Config) sessions. TPM's true random numbers are also used to generate authentication keys for encrypted HDD/SSD.

These models are equipped with TPM2.0 specification chips.



8-8. HDD Mirroring

If an additional HDD option is installed, then even if one HDD malfunctions, all functions can be continued with the other HDD without losing any stored data.

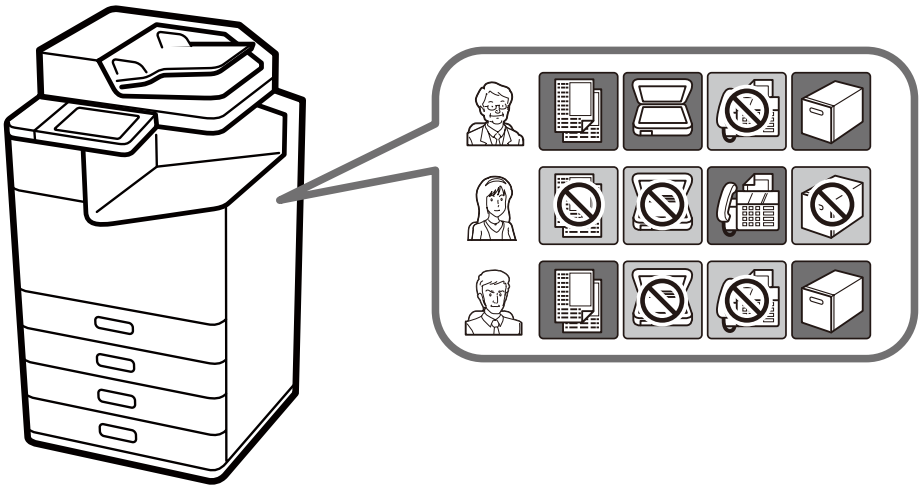
9. Operational Limitation

9-1. Panel Lock

When using panel lock, you must enter the administrator password to gain access to the control panel. When the panel is protected by the administrator password in open offices, public facilities, and similar places, you can prevent users from changing the settings.

9-2. Access Control

You can restrict the use of print, scan, copy, fax*, and box functions for individual users to minimize the security risks based on their roles and job functions. Also, users are automatically logged out after they are inactive in the control panel after a specified duration.



* It is only possible to restrict fax transmission.

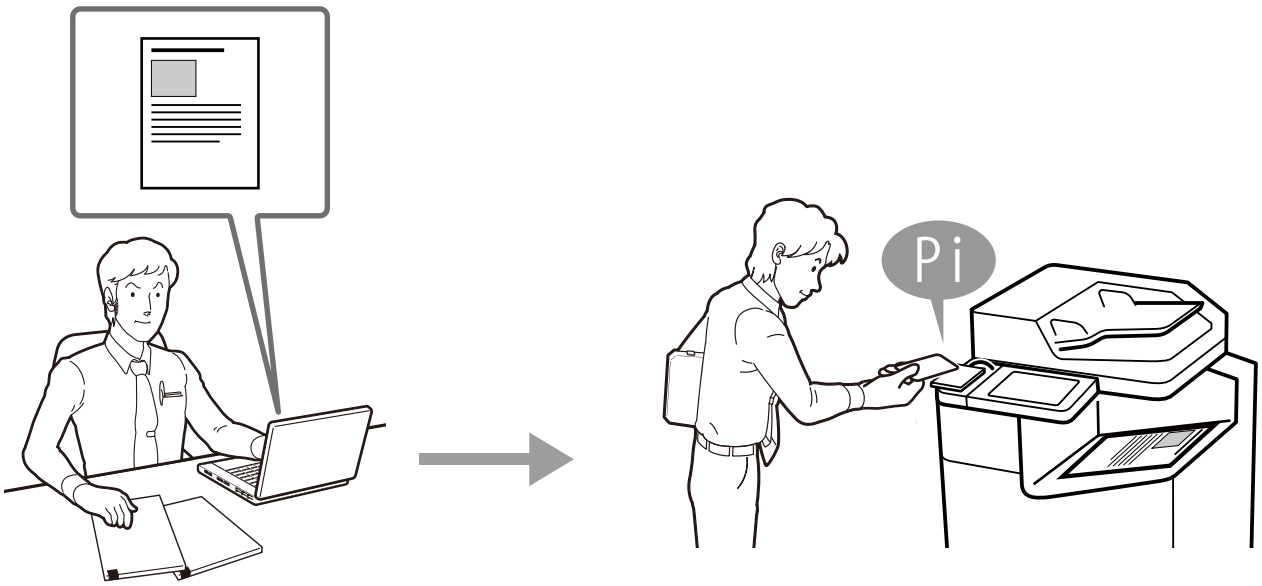
9-3. Authenticated Printing / Scanning

When the optional Epson Print Admin or Epson Print Admin Serverless is installed, you can use authentication devices, such as ID/password authentication and IC card readers, to authenticate users doing printing or scanning. Having users do authentication and operations in front of the product prevent the leakage of information from printed materials or from unattended documents that people pick up by mistake.

Users that are linked by LDAP and registered on the printer can use this as an authentication method.

In addition, with some stand-alone scanners, you can authenticate scanning by ID/password authentication or authentication devices, such as IC card readers, by using main unit authentication or Document Capture Pro Server Authentication Edition.

Users that are linked by LDAP and registered on the printer can use this as an authentication method.



9-4. Password Policy

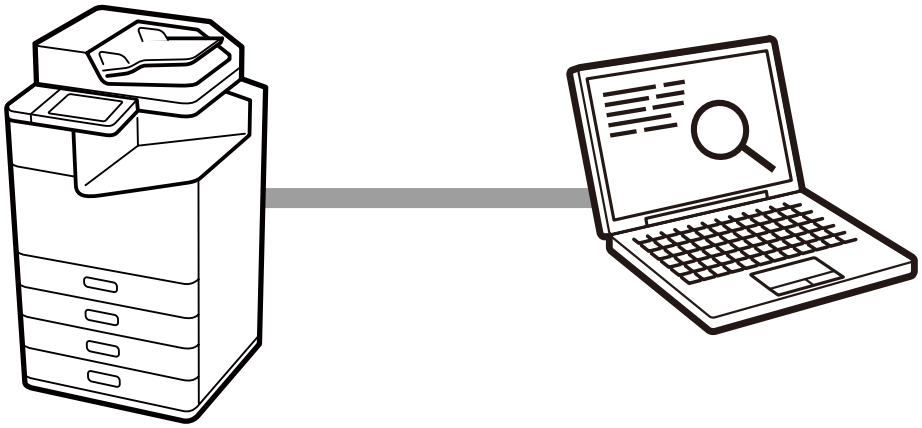
Password policy can be applied for passwords of administrator, access control and fax. A strong password that requires multiple of the following conditions can help prevent password cracking by malicious attackers.

- Minimum number of characters for passwords
- Include / do not include capital English letters in passwords
- Include / do not include lowercase English letters in passwords
- Include / do not include numbers in passwords
- Include / do not include symbols in passwords

9-5. Audit Log

Audit log function can record histories of print, copy, scan, fax and setting change as audit purpose. It can help earlier findings for wrong use and trace from security problems with periodical confirmation of this log.

Up to 20,000 audit logs (up to 5,000 for some models) are retained.



10. Product Security

10-1. Automatic Firmware Updates

If automatic firmware updates are enabled the firmware can be updated automatically at a specified time. Because the updates occur at a specified time, you can always use the latest firmware without interrupting any operations.

10-2. Protection against Illegal Firmware Updates

Authentication with the administrator password is performed during firmware updates. In addition, data communication with the product is protected by HTTPS, and the firmware sent to the product itself is verified as legitimate by signature before the firmware is rewritten. This prevents unauthorized firmware modification by malicious third parties.

10-3. Secure Boot

At startup, the system verifies that the product firmware is legitimate by signature. If it detects that the firmware has been rewritten and is unauthorized firmware, it will stop booting and prompt the user to update the firmware.

10-4. Malware Infiltration Detection

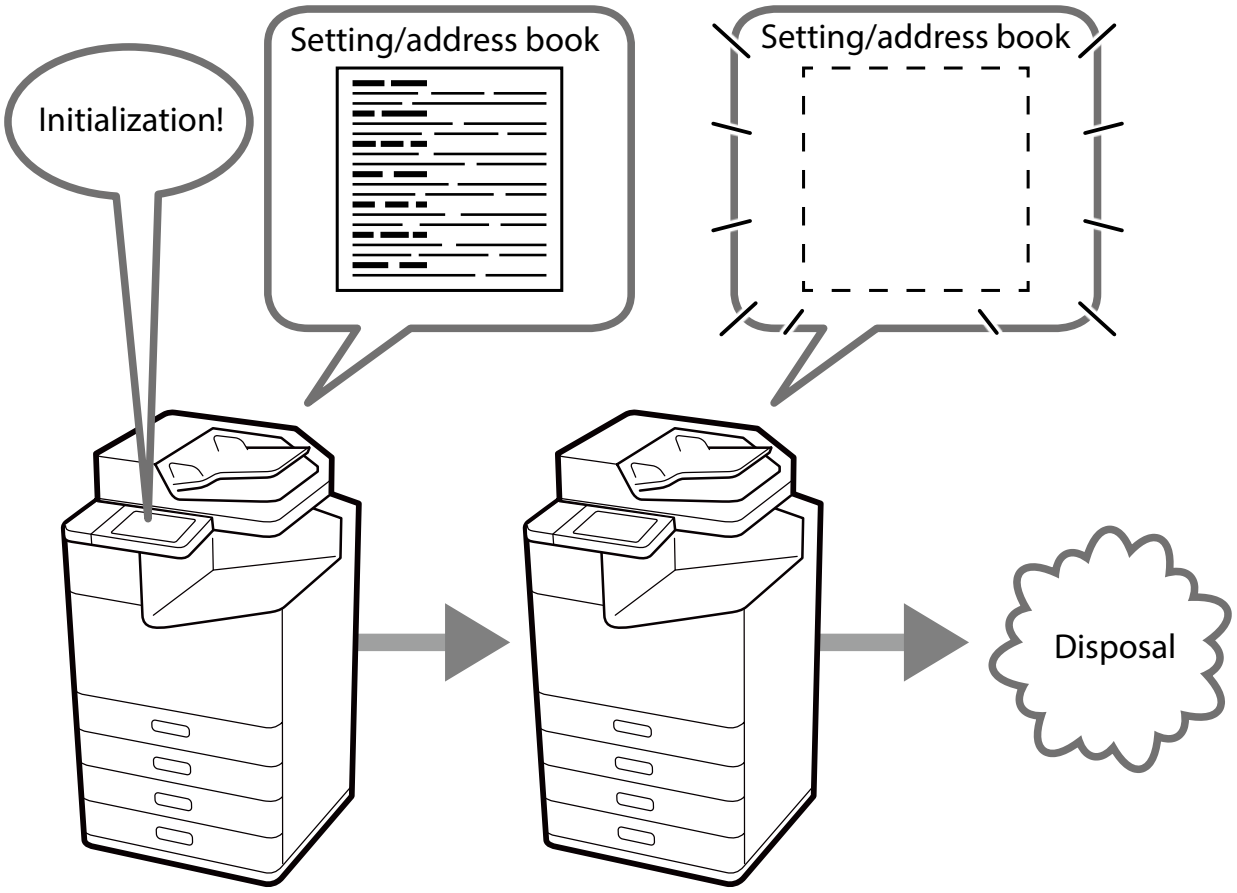
The product is constantly monitored for infiltration of malware into the firmware while the product is running. If malware is detected, the product is rebooted to eliminate the malware.

11. Security Measures When You Dispose of Your Product

11-1. Restore Factory Default

When transferring or disposing of a product, you can return all settings (including in the internal HDD/SSD) back to the factory default (initialization) to prevent the disclosure of confidential information.

In addition, the HDD/SSD can be erased by either "erase by changing the encryption key inside the self-encrypting drive (High Speed)" or "erase by changing the encryption key plus overwriting with a special pattern (Overwrite, Triple Overwrite)".



12. Security Certification and Standards

12-1. ISO15408/IEEE2600.2™

The product has acquired ISO/IEC 15408 certification for compliance with IEEE Std. 2600.2™-2009[*1], an international standard for information security.

IEEE Std. 2600.2™

IEEE Std. 2600.2™ is an international standard that specifies information security criteria for MFPs. MFP security can be comprehensively strengthened by providing standard-compliant security functionalities, such as user identification and authentication, access control, data overwrite, network protection, security management, self-test, and audit logs.

ISO/IEC 15408

ISO/IEC 15408, also called Common Criteria (CC), is an international standard for the independent and objective evaluation of security measures in IT products and systems to determine whether those measures are properly designed and implemented.

Specified versions of firmware, manuals, and other components are evaluated for ISO/IEC 15408 certification. The version of the firmware in a purchased product may differ from the certified version.

There may be some limitations on product functionality when using a certified version.

The CCRA certification logo shows that the product was evaluated and certified in accordance with the Japan Information Technology Security Evaluation and Certification Scheme (JISEC[*2]).
It does not imply a guarantee that the product is completely free from vulnerability.
It also does not imply that the product is equipped with all necessary security functions under every operational environment.

*1 U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009)

*2 JISEC (Japan Information Technology Security Evaluation and Certification Scheme)

Security risks when protocol functions are enabled and limitations when they are disabled

Protocol/ security functions	Security risks when enabled	Limitations when disabled
Bonjour	There is a possibility that information on devices in the network can be read by a third party.	Searches by Bonjour will not be possible from the computer.
SLP	Because the sender is not authenticated, if the sender is spoofed, it can be exploited in an attack to disable the service.	The computer will not be able to use SLP to retrieve or explore information about the device.
WSD	Since communication is not encrypted, there is a possibility that printed data can be read by a third party.	Printing and scanning using WSD will not be possible.
LLTD	There is a possibility that information on devices in the network can be read by a third party.	Devices will not be displayed in "Devices and Printers" in Windows.
LLMNR	There is a possibility that information on devices in the network can be read by a third party.	Searches by LLMNR will not be possible from the computer.
LPR	Since communication is not encrypted, there is a possibility that printed data can be read by a third party.	Printing using LPR will not be possible.
RAW (Port 9100/any port)	Since communication is not encrypted, there is a possibility that printed data can be read by a third party.	Printing using RAW port will not be possible.
IPP/IPPS	For IPP, since communication is not encrypted, there is a possibility that printed data can be read by a third party. For IPPS, there are no security risks.	Printing using IPP/IPPS, such as printing from AirPrint or Mac OS, will not be possible.
FTP	Since communication is not encrypted, there is a possibility that printed data can be read by a third party.	Printing or transferring files using FTP will not be possible.
SNMP	For SNMPv1 and v2c, since communication is not encrypted, there is a possibility that device information and setting data can be read by a third party. For SNMPv3, there are no security risks.	Management tools that use SNMP cannot be used. In addition, management tools and applications provided by Epson will not be available.

Protocol/ security functions	Security risks when enabled	Limitations when disabled
SSL/TLS	Depending on the TLS version and key length you set, the cipher strength may be weak and the cipher may be deciphered.	Connection via HTTPS from a browser will not be possible.
Microsoft Network Sharing	There is a possibility that scanned data or file-shared data can be read by a third party.	Transferring files and network file sharing using SMB will not be possible.
Network Scan (EPSON Scan)	Since communication is not encrypted, there is a possibility that scanned data can be read by a third party.	Scanning via the network will not be possible.
PC-FAX	Since communication is not encrypted, there is a possibility that fax data on the network can be read by a third party.	The PC-FAX function cannot be used.

EPSON

Caution
- Reproduction of this document in part or its entirety is prohibited.
- The contents of this document may change in the future without notice.
- This document is for informational purposes only. For details about utilization, check the manual for each product.

Trademark
- Microsoft is trademark of the Microsoft group of companies.
- Wi-Fi is trademarks of Wi-Fi Alliance.
- Other product names are the trademarks or registered trademarks of their respective companies.

NPD6296-05 EN
©2024 Seiko Epson Corporation