EPSON

Security Guidebook

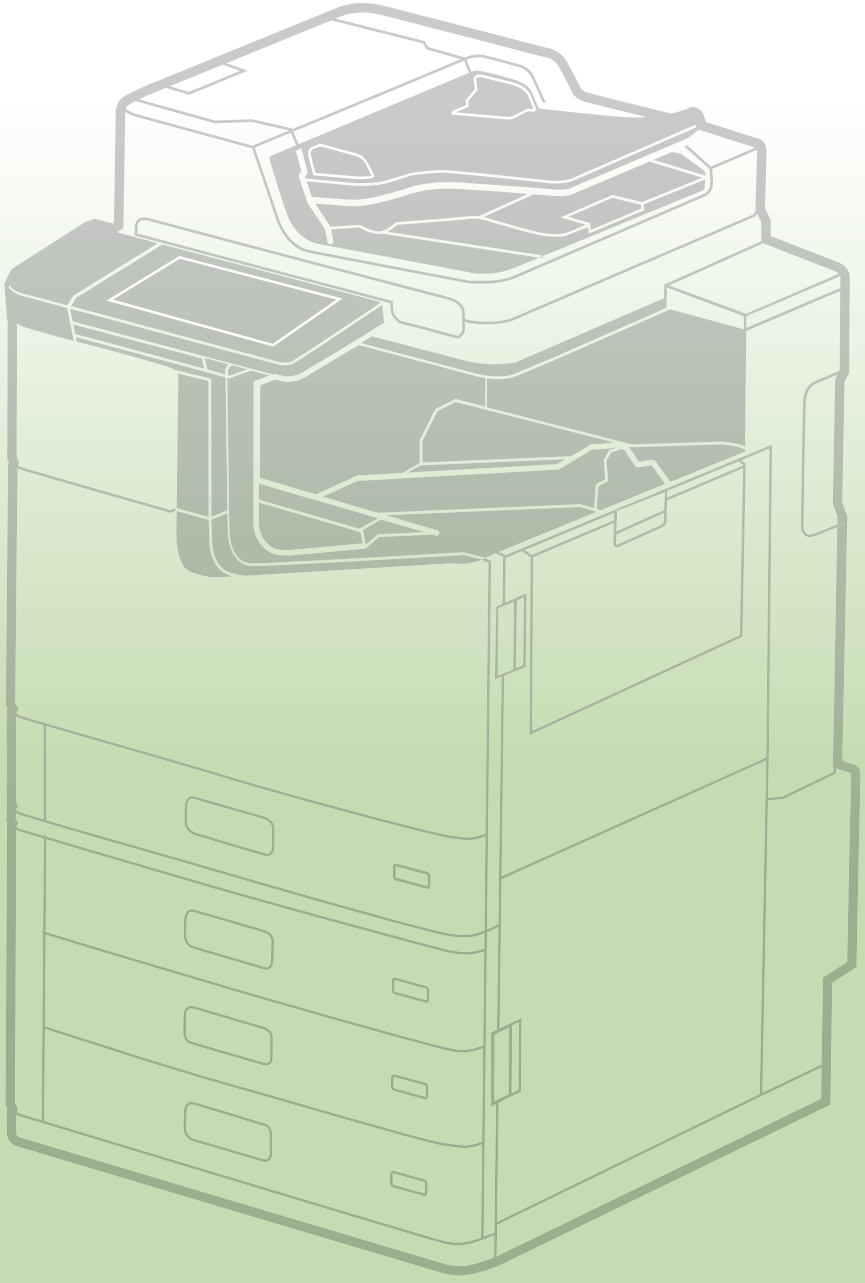


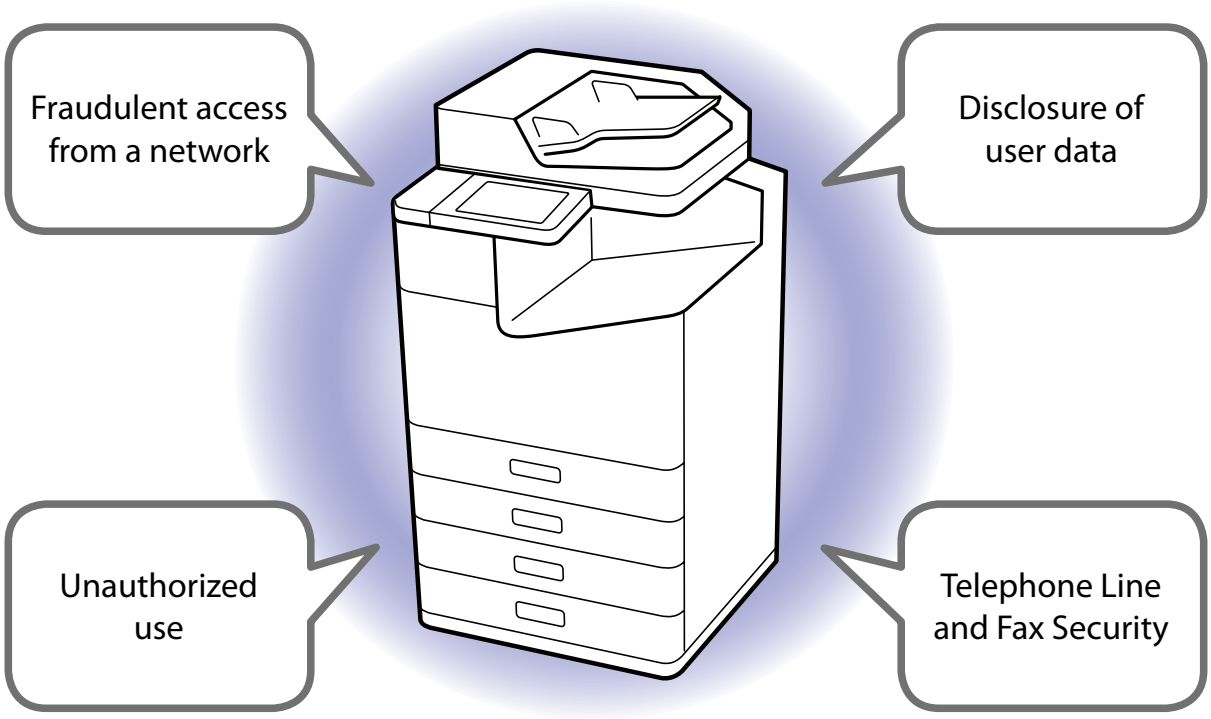
Table of Contents

1. Introduction

Various machines can now be connected to networks due to the development of our information-oriented society.

At Epson, we continue to strengthen the functional network capabilities of our products to improve user-friendliness for our customers.

Epson's products are equipped with a variety of features. Appropriate considerations for security for computers and servers alike are necessary, particularly when connecting to and using a network.



This guidebook introduces Epson's approach to security and advice for the customer, and guides you through the security functions available for use. 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 these functions or comply with these security standards; be sure to use and confirm compliance details in conjunction with the function list in the security guidebook for 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.

1. We treat our products' security as the basis of our products' quality.
   In our manufacturing processes, we consider security throughout the life cycle of the product, from design until the customer is finished using it.
2. We actively provide information and knowledge about security for our customers.
3. We ceaselessly work to create countermeasures against vulnerabilities.
   - Our efforts are focused on implementing vulnerability tests using the industry's standard tools and make efforts to deliver products without vulnerabilities.
   - We regularly monitor information about vulnerabilities from open source software used in the firmware in our products.
   - When new vulnerabilities are found, we promptly analyze them and provide information and countermeasures.
4. We apply security standards.
   ISO/IEC 15408, IEEE Std. 2600.2™
   ISO/IEC 15408 is an international standard for the independent and objective evaluation of security measures in IT products and systems.
   The certification means the security functions confirmed by an independent evaluation as compliance with IEEE Std. 2600.2™ profile for all-in-one printers.

3. What You Should Do When You Install Your Product

The factory default security settings of the product may not be optimized for your security environment. To ensure optimal security, read the following during installation and configure the necessary settings according to your usage environment.

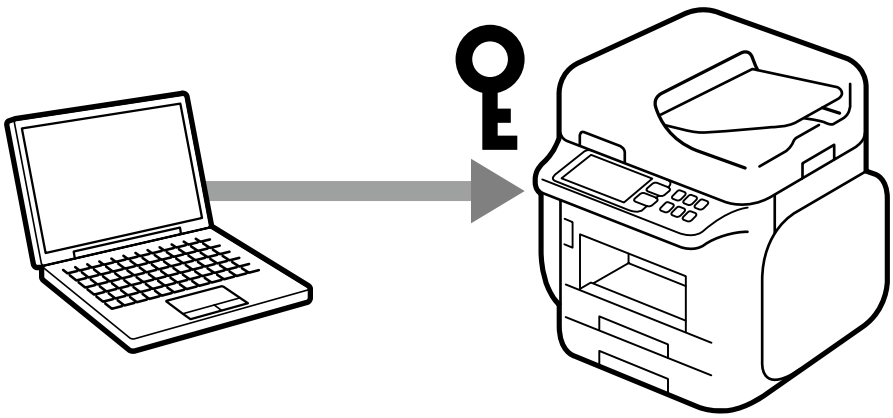
3-1. Administrator Password

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.

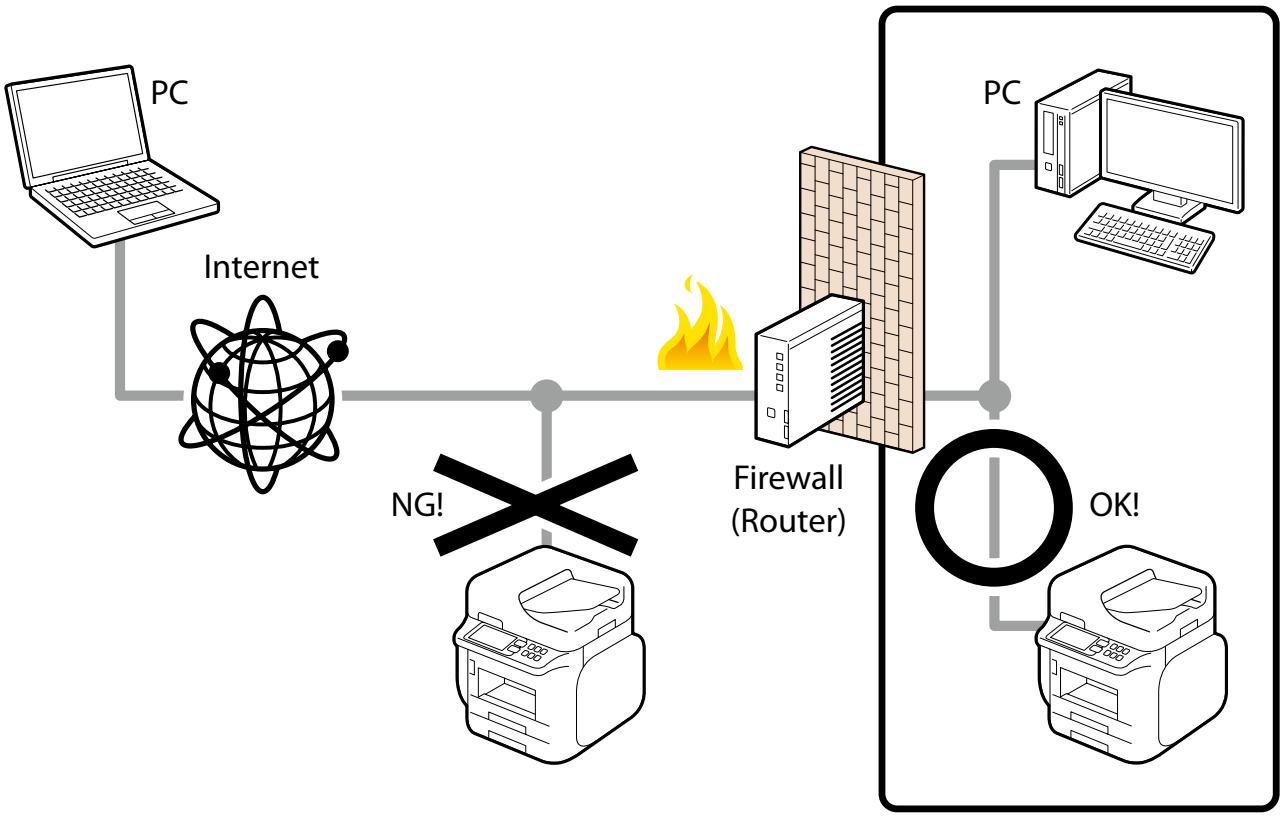
The administrator password should be a complex character string that is difficult for other users to guess. It should consist of 8 or more characters, including not only English letters but also symbols and numbers. You can set up the administrator password directly in the settings of the product's control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

To bolster security, individual passwords are set for some models when they are shipped from the factory.



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.



Management interfaces, such as a web management screen, are included for the products' network functions as well as printing. At Epson, we implement vulnerability tests and make efforts to deliver products without vulnerabilities, but when an Epson device is directly connected to the internet, you are facing unforeseeable security risks to your network, such as unauthorized usage and information leaks.

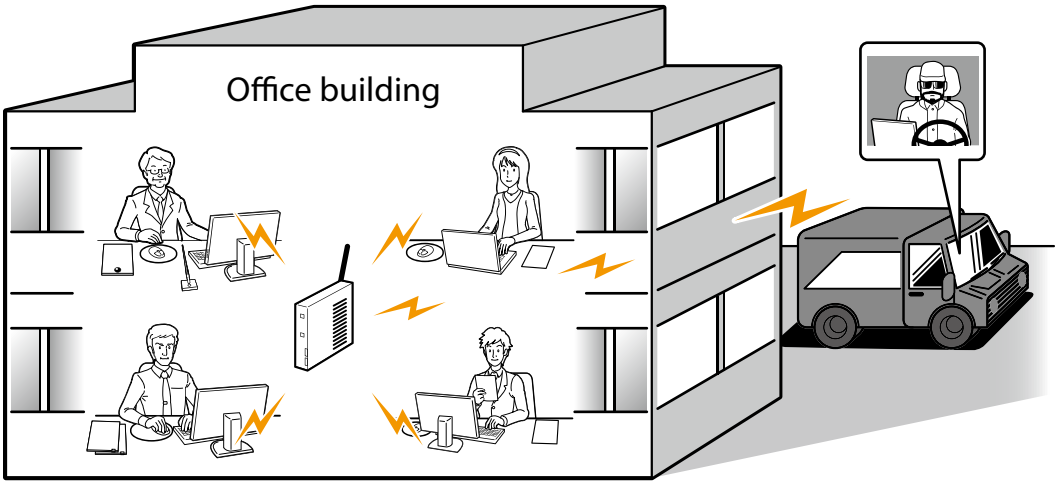
3-3. Wireless LAN Network

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

You can also easily connect to a wireless LAN environment that uses highly safe and complex pass phrases and encryption keys by using WPS (Wi-Fi Protected Setup) and AOSS™ to set up your wireless LAN.

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)



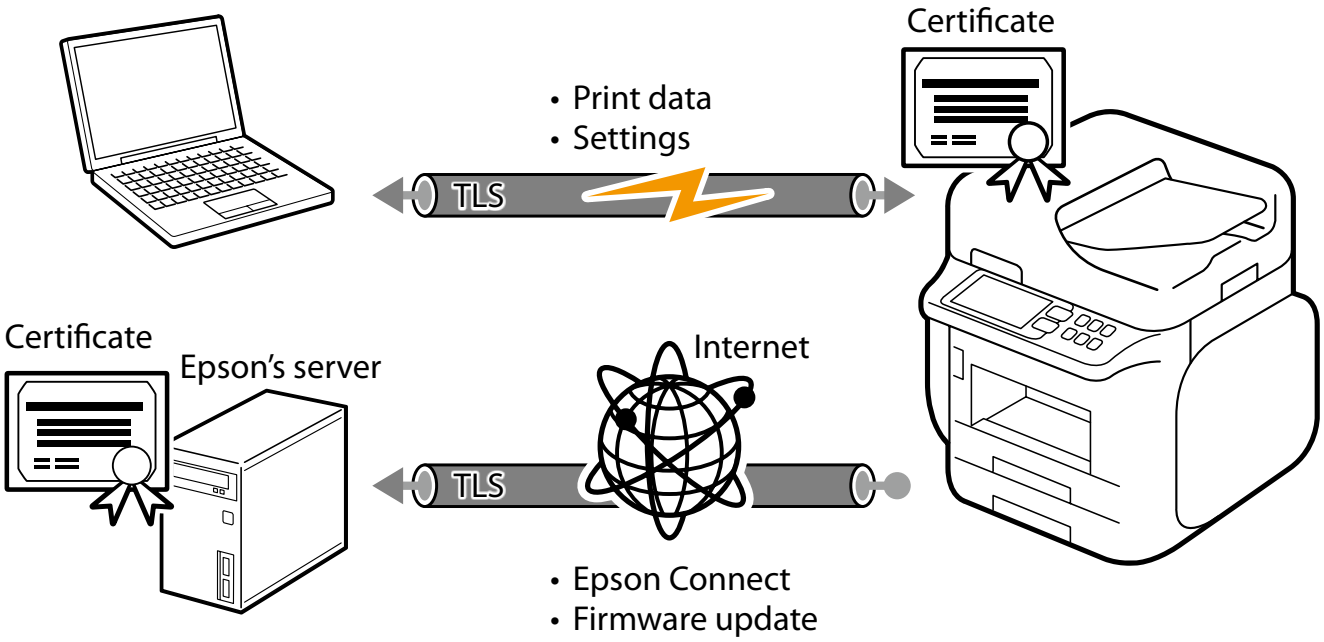
See the product manual for the procedure to set up a wireless LAN.

4. Network Security

4-1. TLS Communication

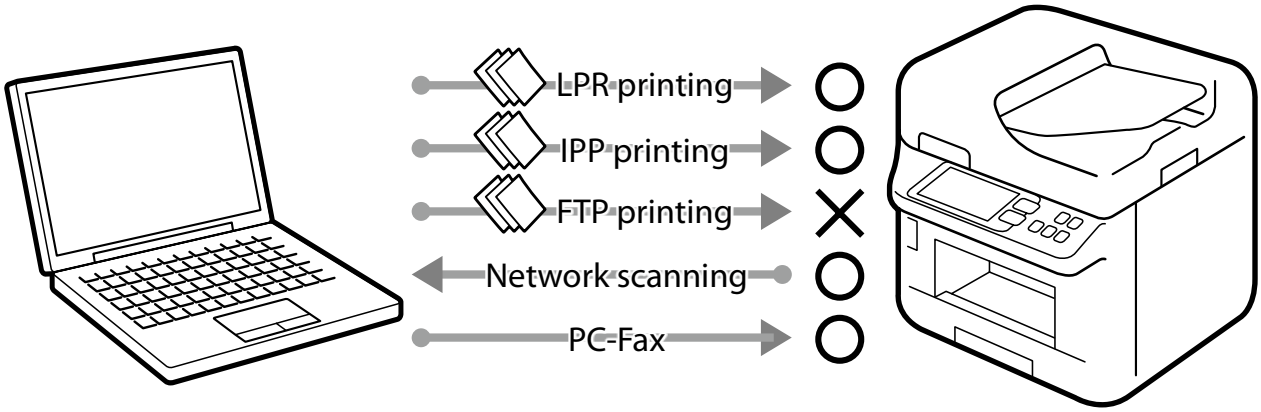
Since transmissions are protected by TLS, you can prevent the disclosure of setting information and the content of print data by using the IPPS protocol for printing and configuring your product via your browser. You can also prevent information from being sent to unauthorized devices by using the server 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.

This product supports TLS versions TLS 1.1, TLS 1.2 and TLS 1.3. Select the encryption strength and the version of the TLS being used.



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.



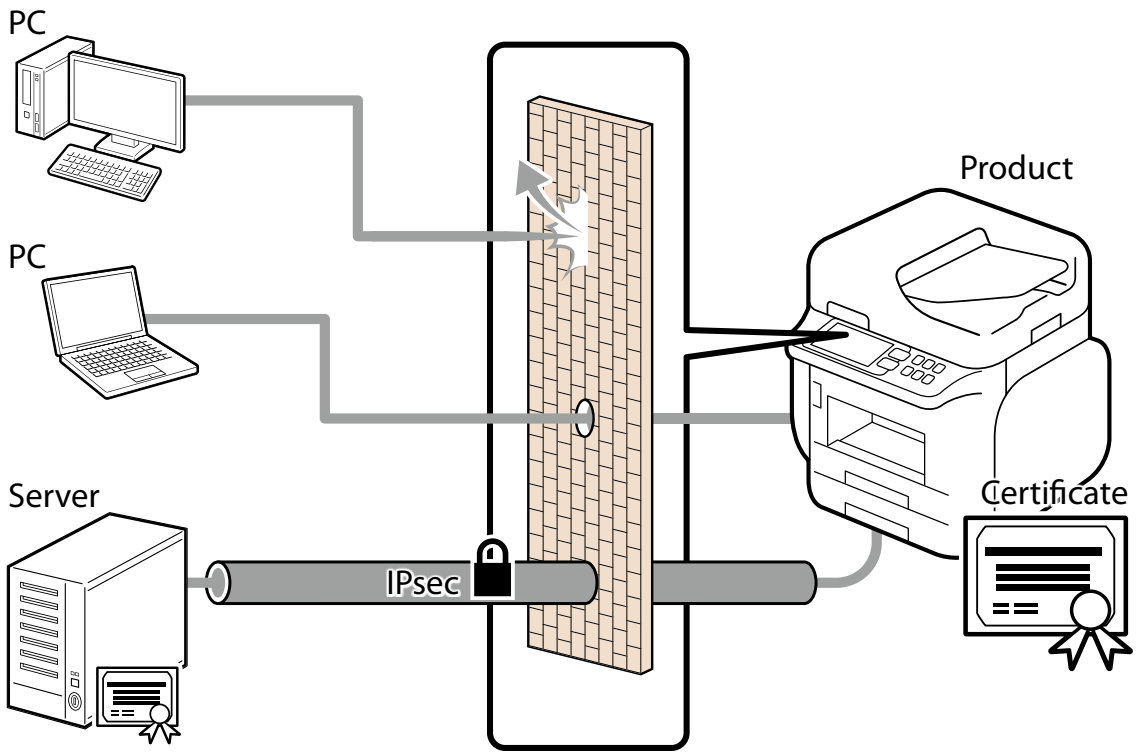
The permissions of the following functions and protocols can be configured and set up individually:

- 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. SNMPv3

By using SNMPv3, you can authenticate and encrypt the SNMP communications (packets) for device setting changes and status monitoring from Device Management Tools to ensure the confidentiality and protection of the data when transmitting through the network.

4-6. 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.

4-7. Separation Between Interfaces

The product includes a USB interface, standard wired LAN interface, additional wired LAN interface, Wi-Fi interface, and fax interface. Each interface is independent and does not include any direct transfer or routing capabilities. As a result, the interface isolation will prevent intruders from compromise the entire system through a single interface therefore eliminating the risks of certain types of security breach. 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

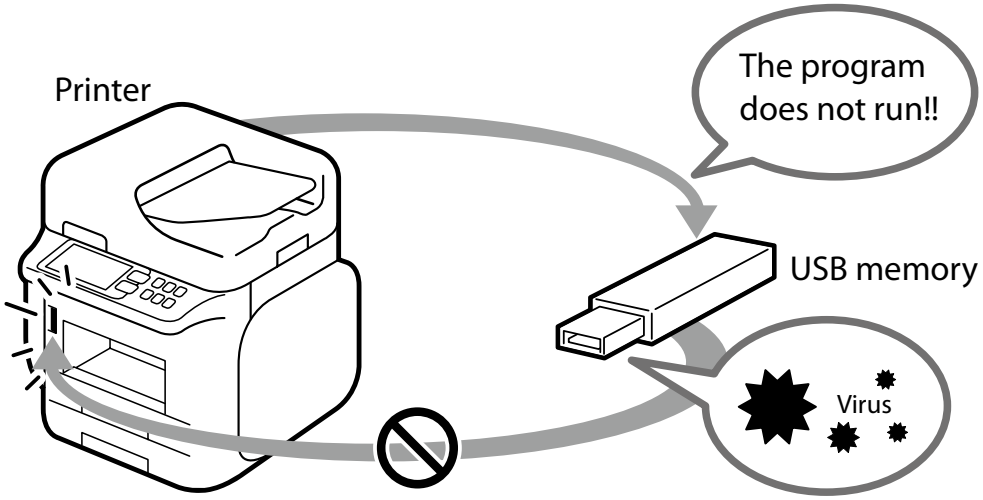
You can disable the access to a product from a computer via a USB connection when you want to prohibit printing and scanning directly from the computer without the use of a network.

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

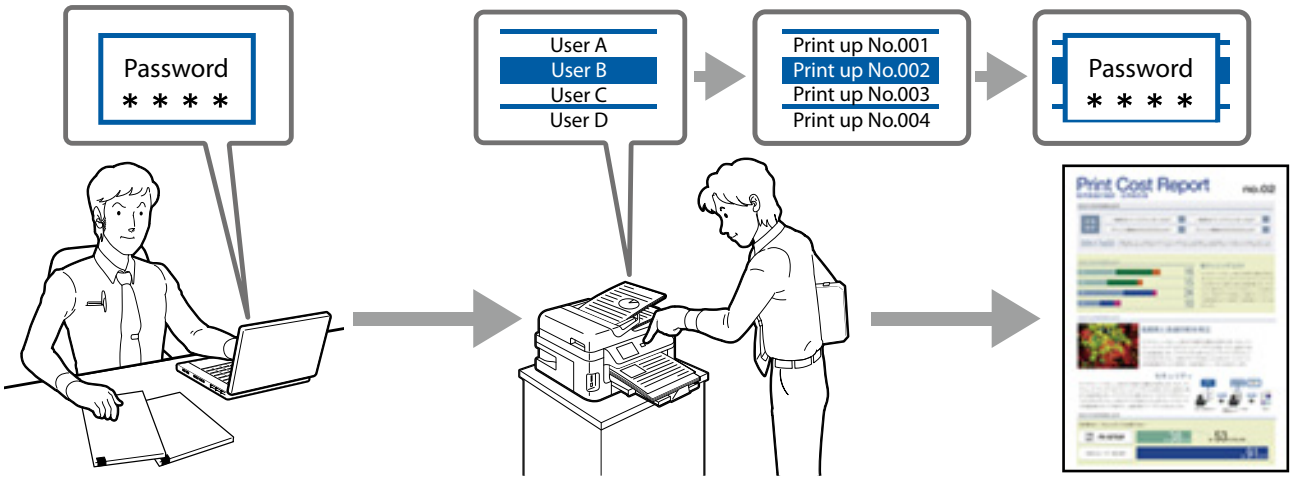
Since there are no executable functions on USB memories for Epson products, there is no danger of the product being infected with viruses via USB memory.



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".



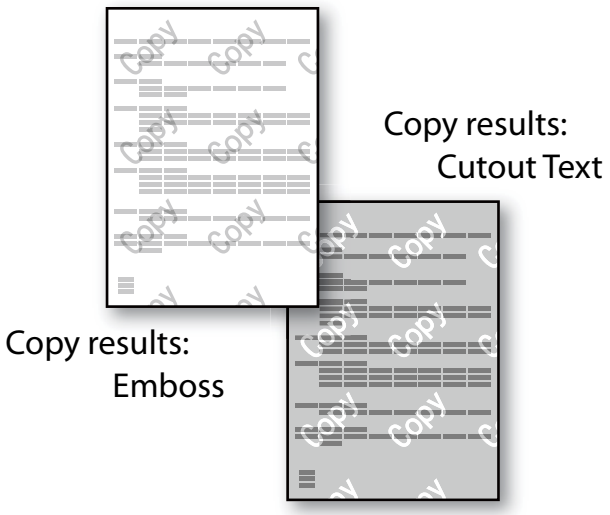
Enter a password to print.

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

Printing is complete.

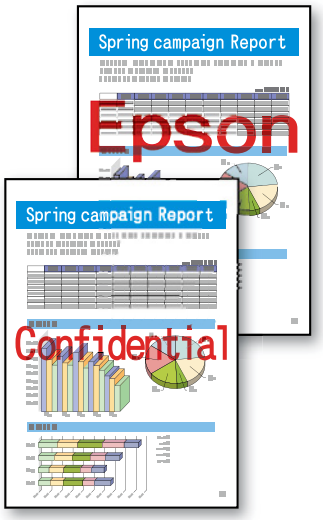
6-2. Anti-Copy Pattern

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.



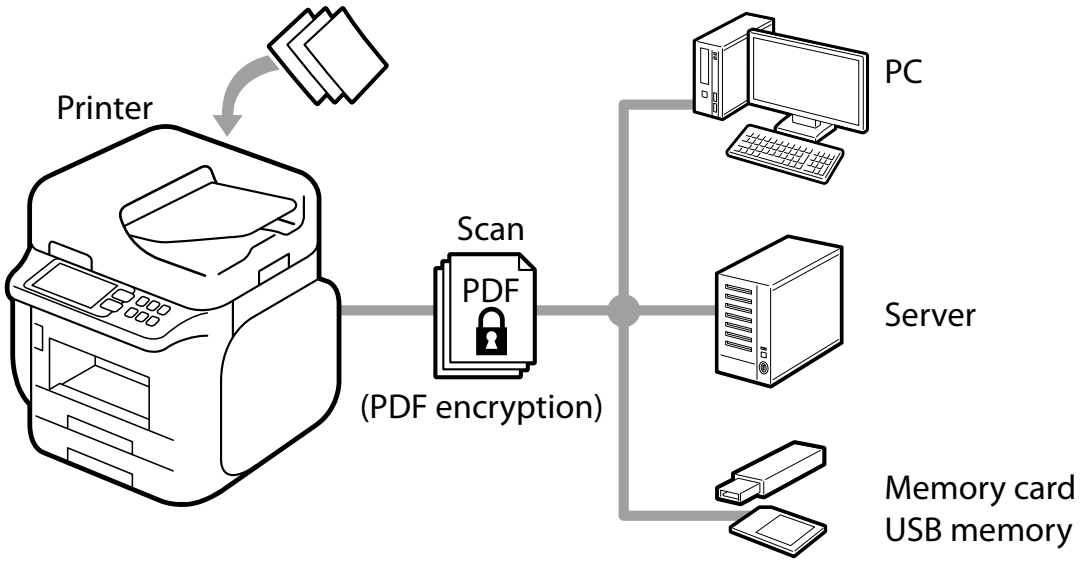
6-3. Watermark

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.



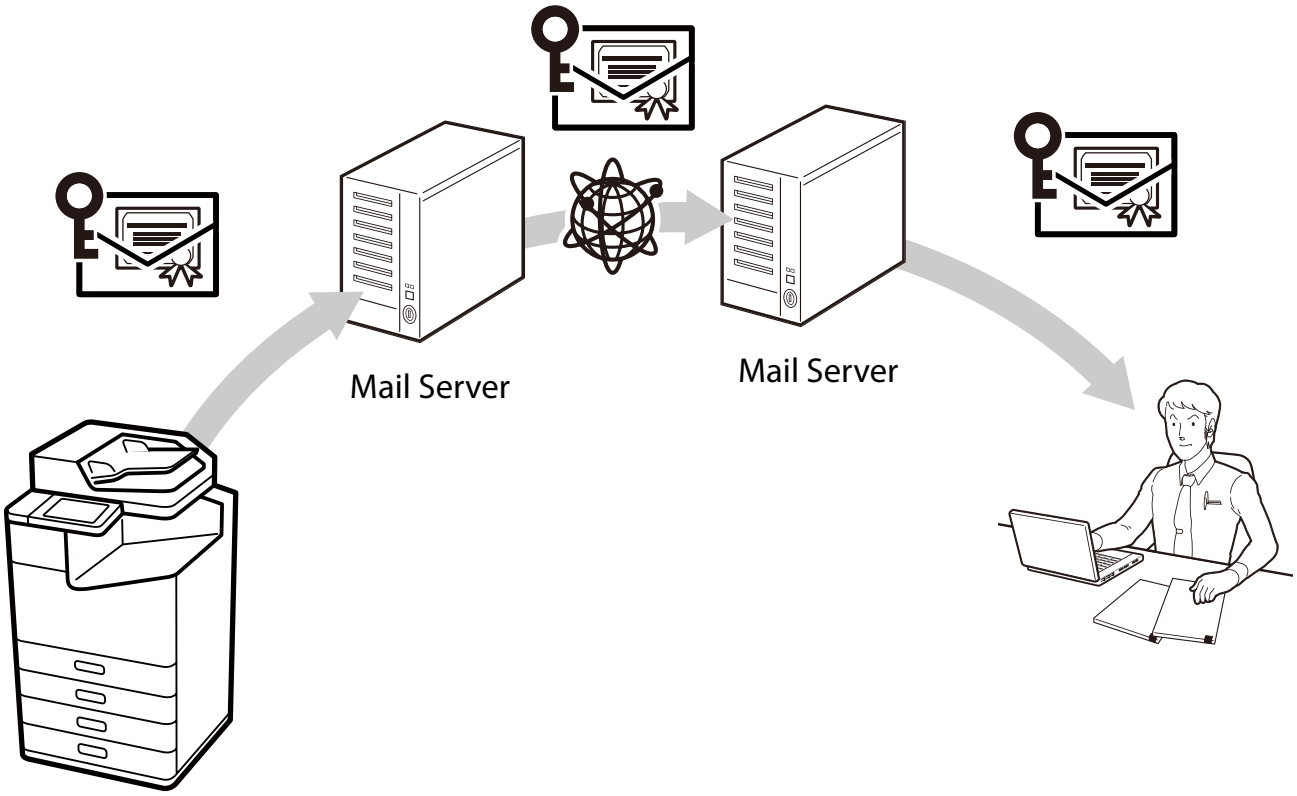
6-4. PDF Encryption

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. Authorization Password for Scan to Network Folder/FTP, Scan to Email, and Email Notification

Nowadays, setting long passwords is being recommended to increase password security. You can now set a maximum of 70 characters as the authorization password used for Scan to Network Folder/FTP, Scan to Email, Email Notification. This allows you to set longer passwords for file servers and email servers that are being operated.

6-8. Default Disabling of 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

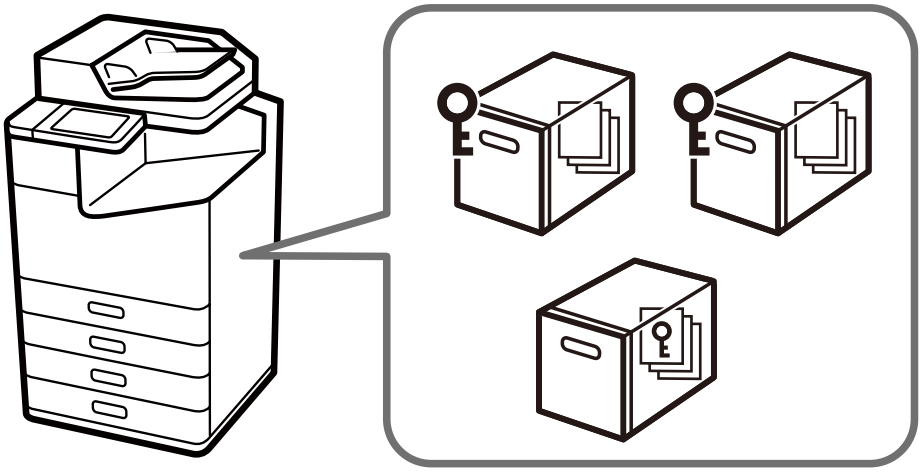
You can set the product so that only 1 recipient can be selected.

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. Box Security

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



8-2. Protecting Your Address Book

When batch editing a product's address book, you can prevent the disclosure of address information and unauthorized manipulation by requiring an administrator password (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.

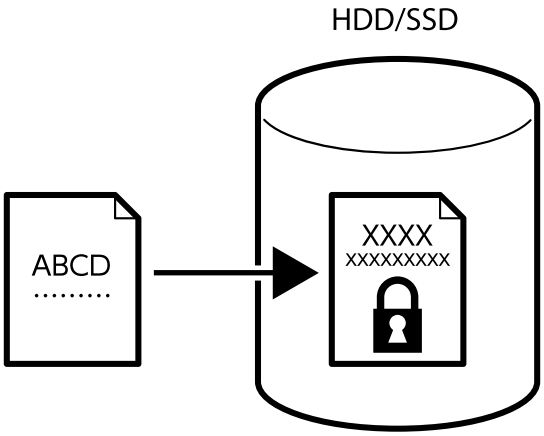
Fax data is cleared when sending or receiving faxes completely. Received faxes can be saved with the back-up function but it can be deleted automatically with setting change (Refer to 7-6).

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.

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

The HDD/SSD comes with a self-encrypting drive, and the document data is encrypted with AES-256.



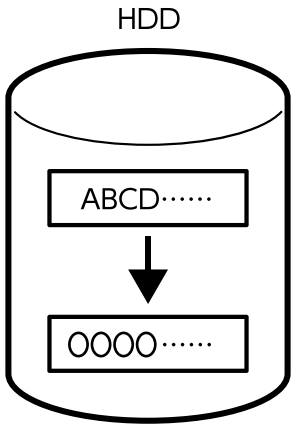
8-5. Sequential Deletion of Job Data

When enabled, the deleted data in the hard disk is overwritten in the following ways to prevent from restoration. There are several options:

(1) Quick deletion: The encryption key is changed to prevent deleted data from restoration.

(2) Secure sequential deletion: The encryption key is changed, and the deleted data on hard drive are overwritten with "0's" to further ensure the deleted data cannot be recovered.

Please refer to the user manual of your product for a detailed explanation on job data deletion.



8-6. Password Encryption

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

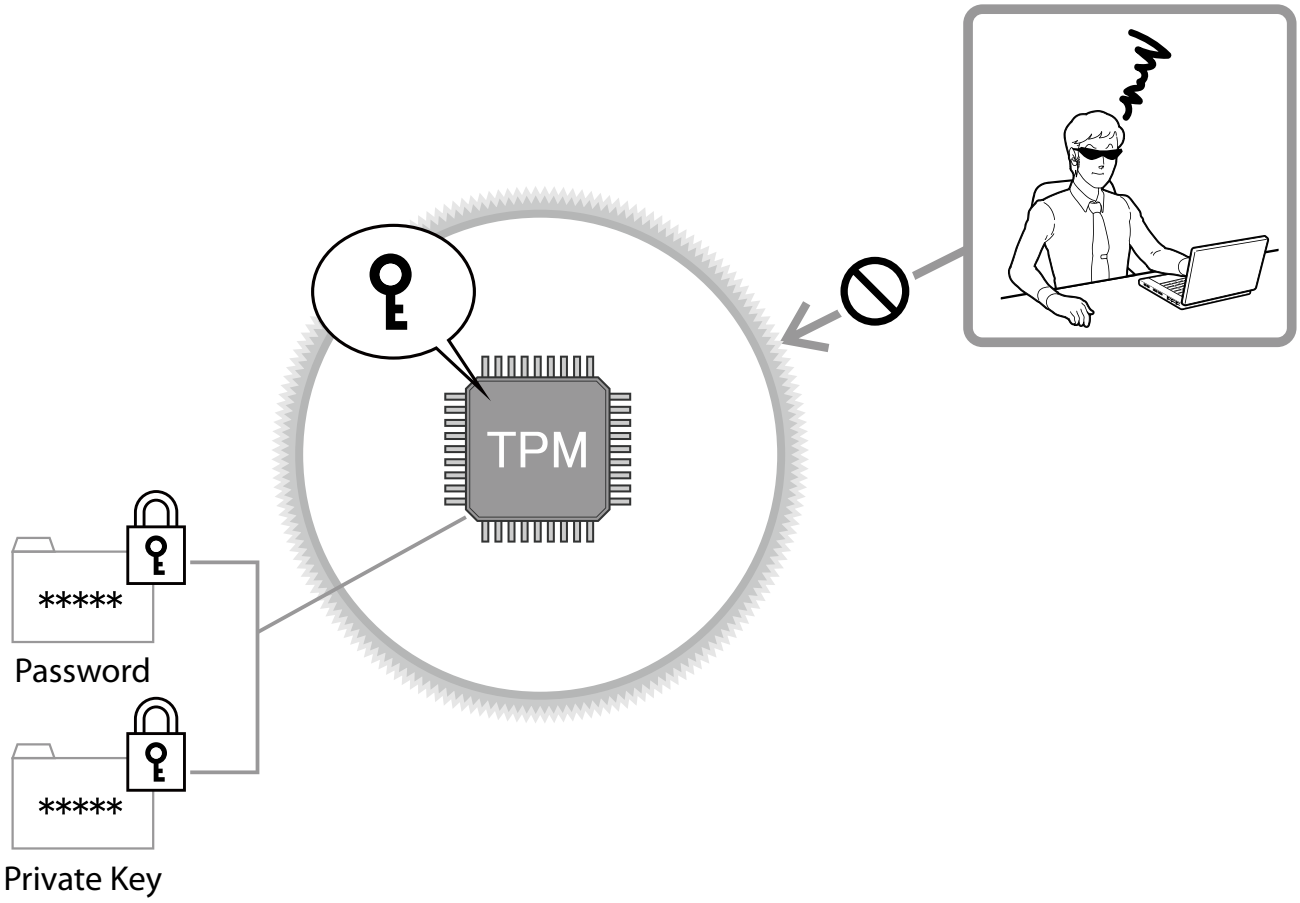
- Administrator Password
- User passwords for Access Control
- Hard Disk Authentication Keys, Certificate Private Keys, etc. Passwords to access for Scan to Network Folder/FTP

8-7. TPM

In models with TPM (Trusted Platform Module), the security level improves as follows:

- The encryption keys for restoring encrypted passwords and private key information are stored on the TPM chip.
- The TPM chip can be protected from unauthorized analysis at the hardware level, since the TPM chip cannot be accessed from outside the product.
- TPM's true random numbers are used as session keys for communication with the browser (Web Config).
- TPM's true random numbers are used in generating authentication keys for the encrypted HDD/SSD.

The product has a TPM 2.0 chip.



8-8. Mirroring of the Hard Disk

When the additional hard disk option is installed, then even if one hard disk malfunctions, no stored data is lost and all functions can continue by using the other hard disk.

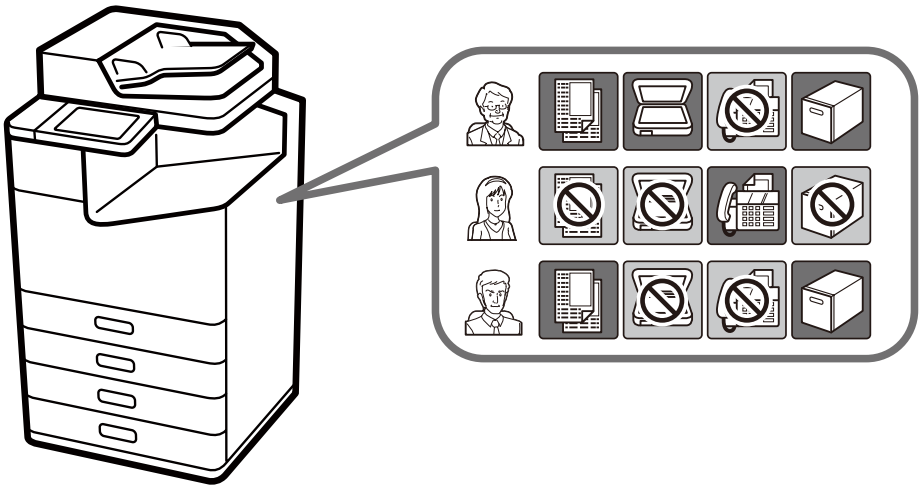
9. Operational Limitation

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.

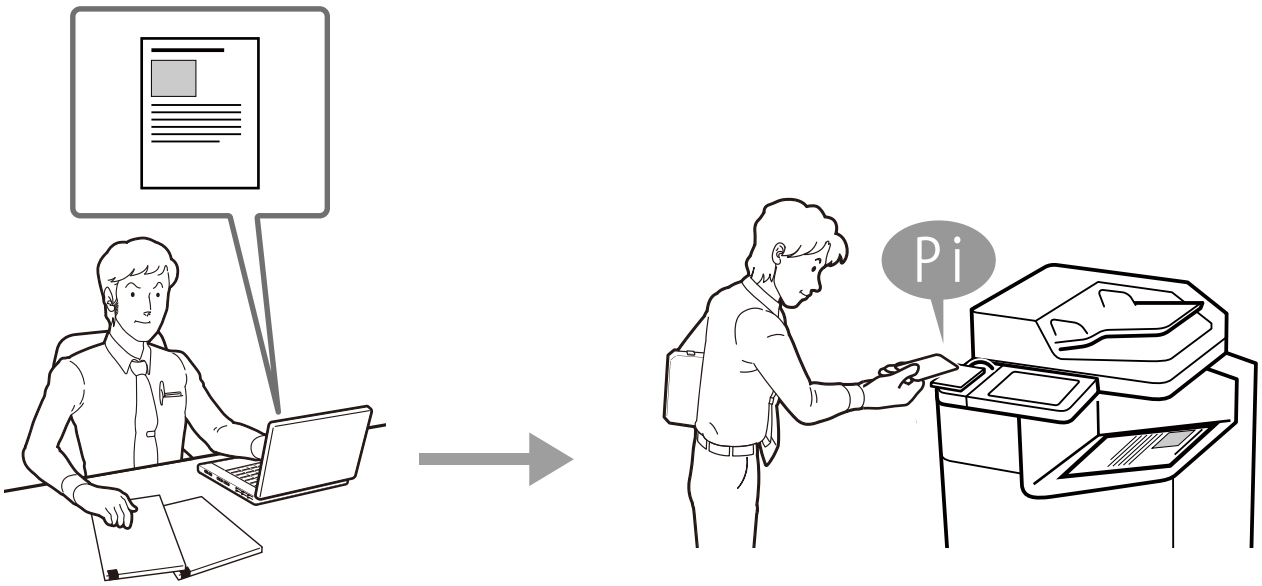
9-3. Authenticated Printing / Scanning

When using the optional "Epson Print Admin / Epson Print Admin Serverless" you can require authentication at a registered devices before releasing a submitted document for printing. This prevents sensitive and unattended documents being obtained from the output tray of the device by unintended individuals.

There are multiple authentication options including the use of a PIN code, a user name and password pair, an ID Card reader, which all can be integrated with an LDAP server.

With a stand-alone scanner, you can use Document Capture Pro Server Authentication Edition or stand-alone authentication.

There are multiple authentication options including the use of a PIN code, a user name and password pair, an ID Card reader, which all can be integrated with an LDAP server.



9-4. Password Policy

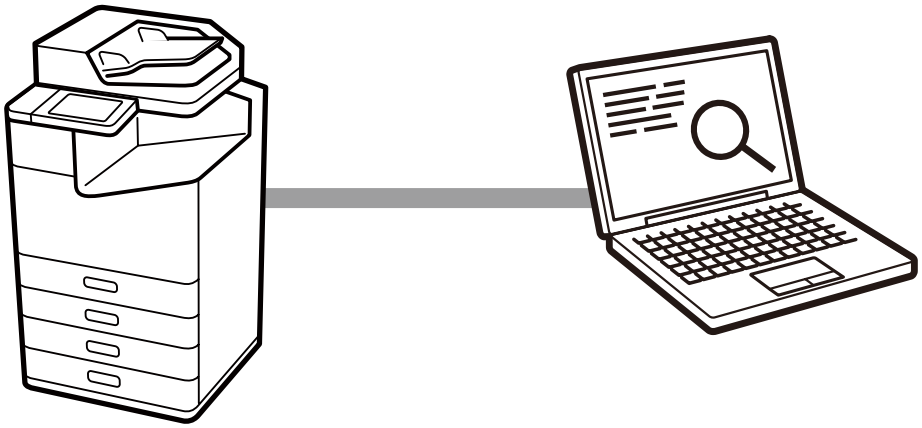
Password policy can be applied for passwords of administrator, access control and fax. A strong password that requires multiple of the following conditions can help prevent password cracking by malicious attackers.

- 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.

Furthermore, up to 20,000 audit logs 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, and the firmware sent to the product itself is verified as legitimate by signature before the firmware is rewritten. In addition, communication with the product is protected by HTTPS. 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.

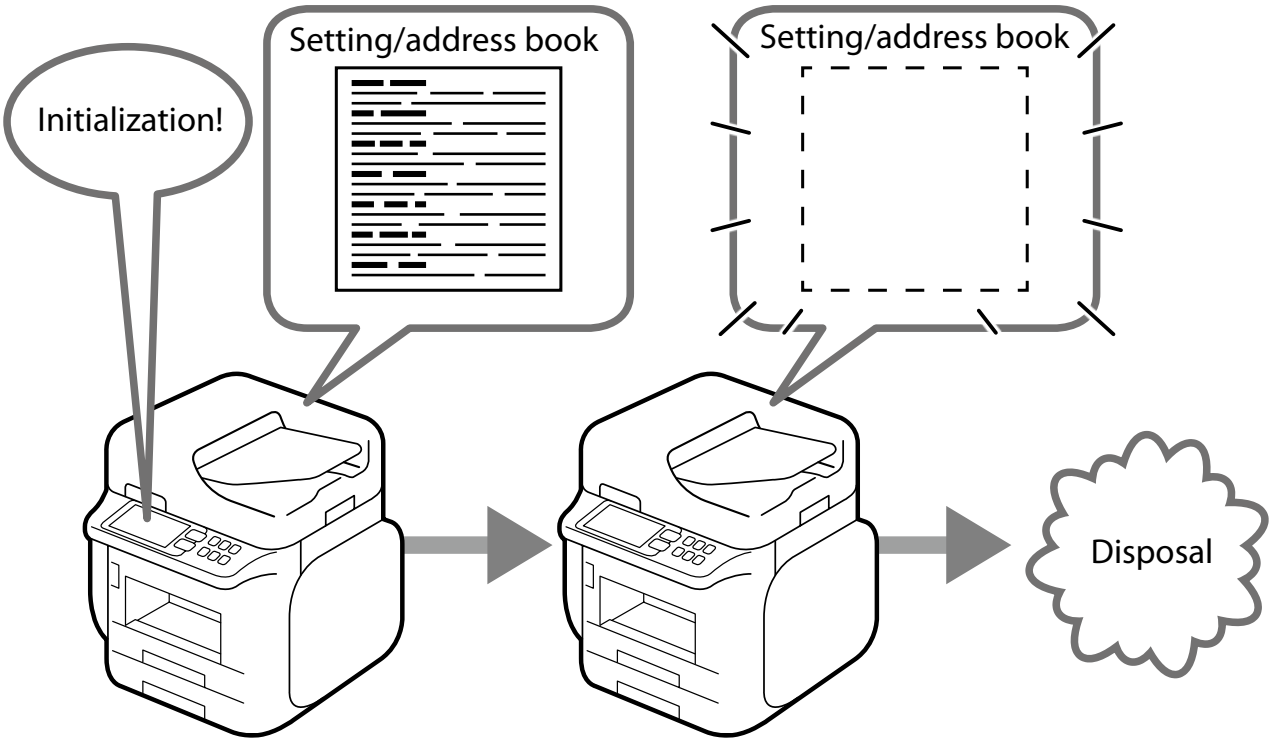
10-4. Malware Infiltration Detection

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.



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*, 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).
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.

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

EPSON

NPD6296-03 EN