

IF IT WORX, IT'S



# **Security Best Practices for UTAX MFPs and Printers**

# Introduction

## Overview

With the rapid development of digital information networks in society, the various IoT devices connected to these networks improve convenience. The IoT devices for office use handle various types of sensitive information. Whereas, the IoT devices are exposed to recent advanced and diversified threats, such as unauthorised access to the IoT devices via a network, and tapping or alteration of the information in transit over a network. Multifunction products (MFPs) and printers (referred to as “products” hereafter) are no exception. Like a PC, when using the product and connecting it to a network, the customer’s attention is necessary.

UTAX UK Ltd. (referred to as “UTAX,” hereafter) is part of a group of Kyocera Document Solutions (referred to as “Kyocera,” hereafter) companies committed to helping meet the security challenges organisations face in their environments, including federal, state, and local governments; the Department of Defense; enterprises; and healthcare, education, and financial sectors. We enhance customers’ information security and privacy through products and services that are secure, reliable, and compliant with international legal requirements and security standards\*<sup>1</sup>.

UTAX helps ensure our customers’ security policies are configured to their sector best practices. By referring to this document, customers can consider the security posture of their organisation.

*\*1: GDPR, California IoT Security Law, ISO/IEC27001, ISO/IEC27017\*<sup>2</sup>(Cloud Security), ISO/IEC15408 (Common Criteria), HCD-PP, IEEE 2600, DoD 5220.22-M ECE, VSITR, FIPS 140-2/FIPS 140-3, HIPAA, GLBA, PSTI, Data Protection Act 2018, Cyber Essentials Plus and others.*

*\*2: Kyocera obtained ISMS Cloud Security certification (the new-cloud-centric security certification) ahead of all other MFP and printer manufacturers as of November 17, 2017.*

## **Purpose**

The purpose of this document is to advise customers (i.e., administrators) of security measures pertaining to appropriate security settings and to help you enhance UTAX product security in your workplace. UTAX provides customers with a variety of security features for its product. We recommend the configurations written in this document be used as much as possible while applying the security settings to your specific environment and the product life cycle from the time of the product installation and operation through decommission phase. In order to ensure the best performance and most effective use of the product, please read this document thoroughly before setting the security features provided by the product. Refer to the *Operation Guides* for more information on other configurations.

## Target Audience

The target audience for this document is intended for:

- administrators,
- other customers.

The target audience should understand the following:

Under the current cybersecurity environment, it is important that customers (i.e., organisations) should manage their endpoints (i.e., products) and resources to protect network and information assets. It is also essential that customers (e.g., administrators) should educate their organisation's employees on how to use network-connected products properly. For example, user authorisation management<sup>\*3</sup> should be well determined and set by the organisation to prevent privileged escalation. Therefore, customers may rest assured to use UTAX product in the secure environment with the correct settings.

\*3: See "User Authorisation Management" described in [Security White Paper for UTAX MFPs and Printers.](#)

### NOTE

*Only administrators should have access to the high security level of features such as network configuration, system configuration, printing protocols and ports. The administrators should determine who can access the address book, who can add, edit or remove entries from the address book. Administrators can define, enforce, and prohibit various security settings. In other words, the administrators should take full responsibility for controlling and managing the product and for making sure that no improper operations are performed.*

## **Edition Notice**

The information contained in this document is subject to change without notice. It could include inaccuracies or typographical errors. Changes or improvements in this document may be incorporated in later editions. Changes or improvements in the product or software are made at any time as needed.

Not all security features and software are supported on all UTAX products in every market. Some security features and software apply to certain product models only. Customers can obtain more information about the product from the *User Guides*, *Operation Guides*, or by contacting your nearest sales companies in your respective regions.

## **Limitations**

The document is intended to help you configure the minimum-security settings for your user's environment. Please note that you are responsible for independently evaluating the information described in the document, as well as the usage of UTAX products or services, especially those connected to your network environment. The information in the document is subject to change without notice.

The information in the document is provided "as-is" without warranty of any kind, whether express or implied. Although care has been taken when compiling this information, UTAX makes no representations or warranties about the accuracy, completeness or adequacy of the information provided herein, nor fitness for a particular purpose, and shall not be liable for any errors or omissions. The only warranties for UTAX' products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty.

# Recommendations when using your UTAX

## product

This section explains how the appropriate security settings on the product help users feel confident in protecting their critical data/information at rest and in transit in a secure manner, including possible security risks.

### NOTE

*The following settings described in this document are indicated only as suggestions/recommendations for security best-practice in common workplaces. Determine the recommended settings before configuring the UTAX products in user's environment.*

## In the Installation Phase

### Identification, Authentication and Authorisation

#### Administrator Password

We strongly recommend the password should be set suitably for each user's environment to ensure that users can use UTAX products securely with ease. By factory default, a unique password is set for each machine. However, the administrator password should be changed from its factory default value. The administrator password should be complex and difficult to guess and should not be shared with anyone who does not need access.

If the administrator password is not set, and the product is left at its factory default settings, there is a risk that alteration or unauthorised access to the device settings and network settings stored in the product could be allowed. This causes the possibility of sensitive and personal information leaks.

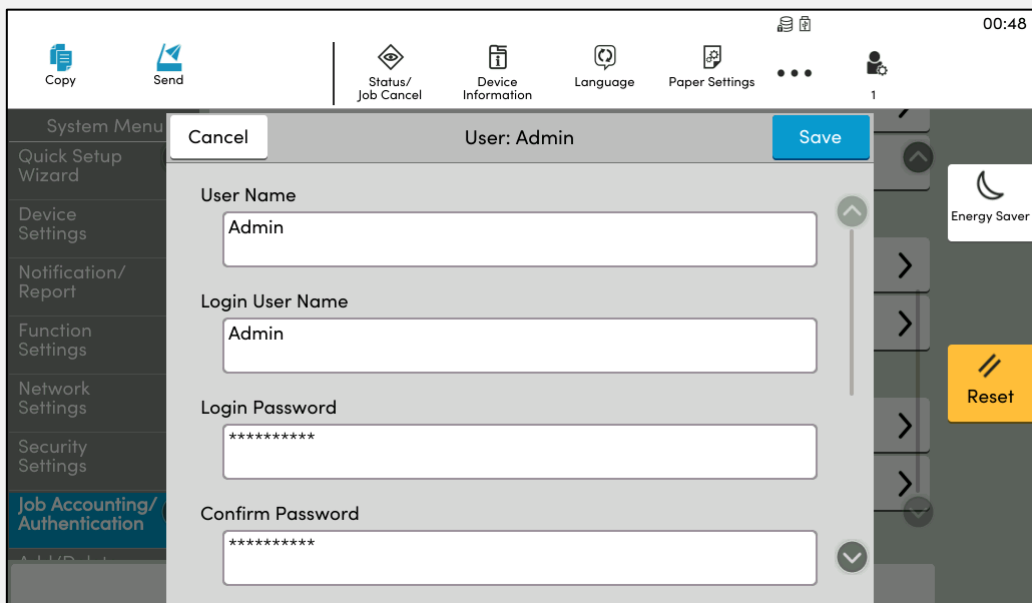
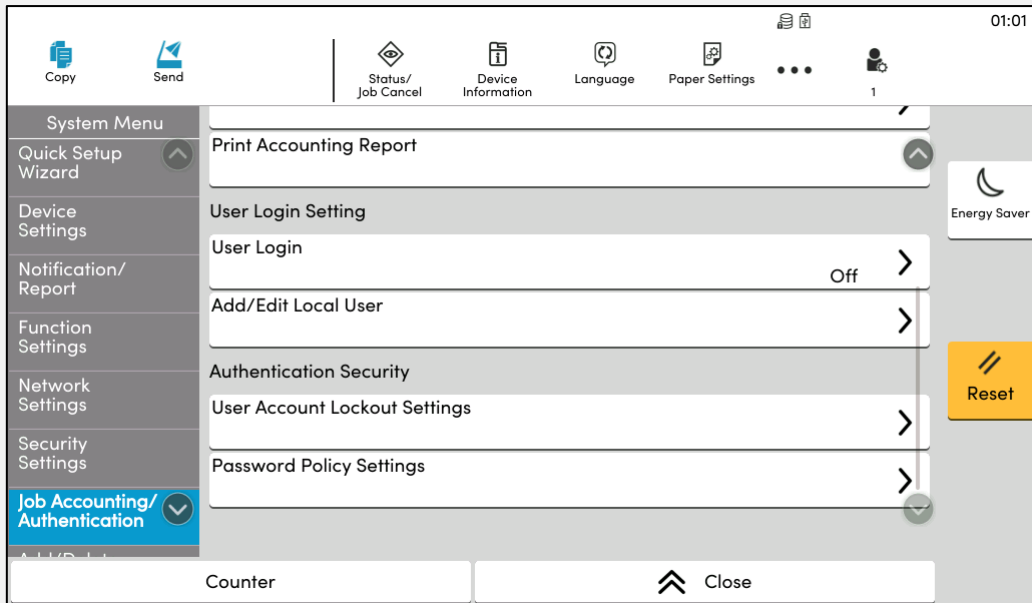
The unique administrator password setting helps protect the product against unauthorised access or use.

E.g.)

<From the Operational Panel of the product>

## Configuring Administrator (Admin) Password Setting

1. Click **Job Accounting/Authentication** > **User Login Setting** > **Add/Edit Local User**.
2. Select **Admin**.
3. Input **Login Password** and **Confirm Password**.
4. Click **Save**.



The screens may vary depending on the product model.



## Password Policy

Password policy should be set that encourages users to employ unguessable strong passwords.

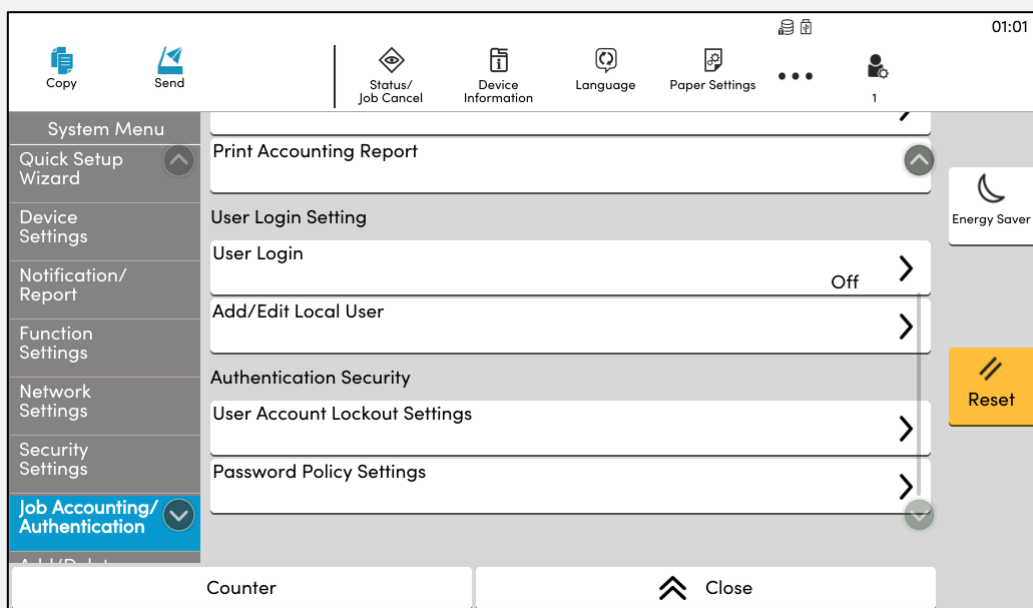
A password that does not meet the password policy should be prohibited. Otherwise, it is easy to be analysed by attackers.

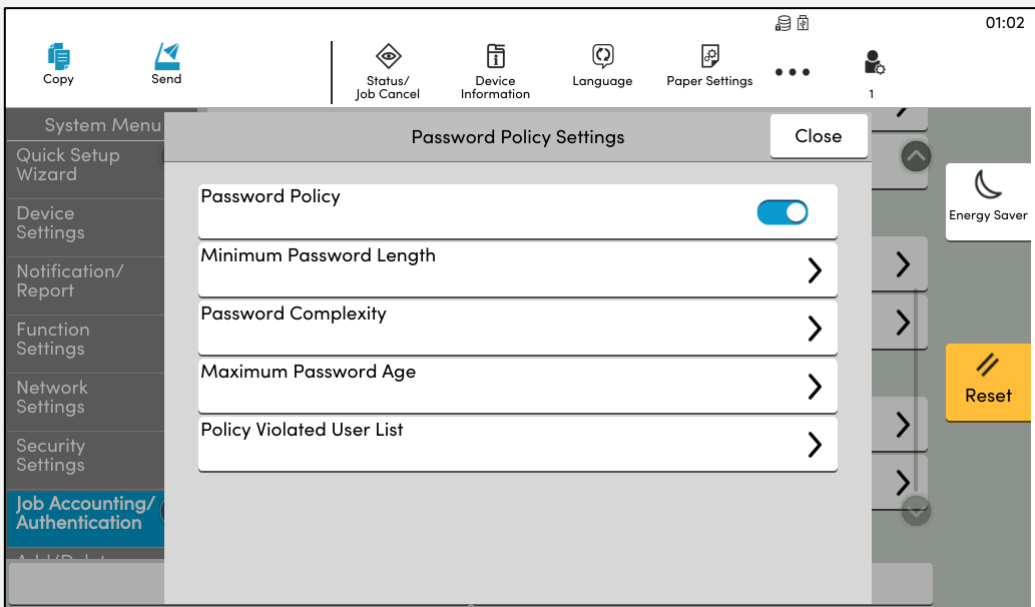
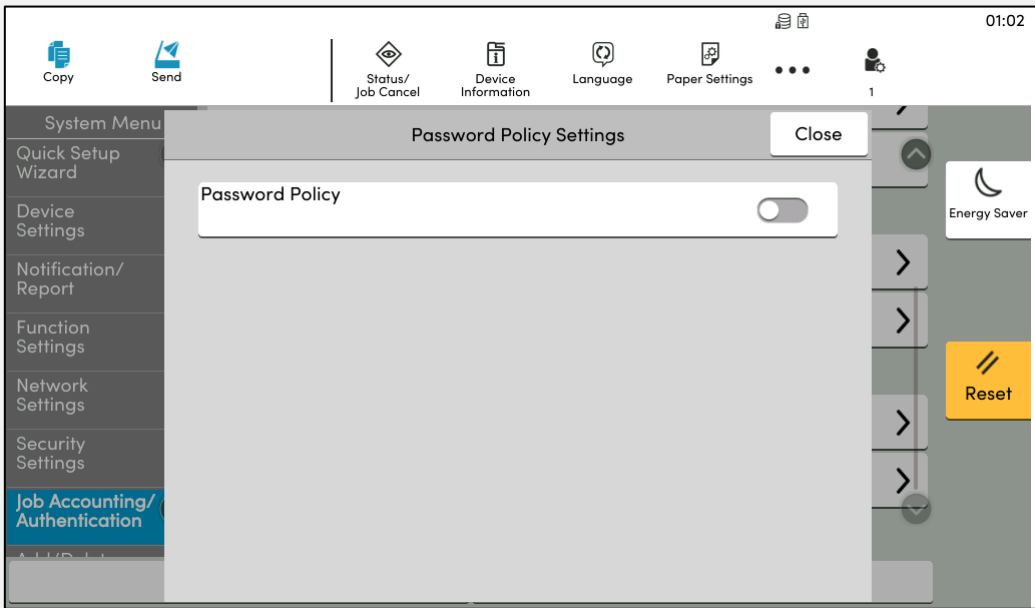
The password policy helps prevent simple passwords from being set by users and guards against unauthorised access by a third party.

E.g.)

<From the Operational Panel of the product>

1. Click **Job Accounting/Authentication** > **Authentication Security**.
2. Select **Password Policy Settings**.
3. Switch to **On** > **Password Policy**.





The screens may vary depending on the product model.

E.g.)

<From Web Connection>

## Configuring Password Policy Settings

1. Click **Security Settings > Device Security**
2. Specify the required settings such as **Password Policy Settings** as indicated in the red box.
3. Click **Submit**.

**Security Settings : Device Security**

**Authentication Security Settings**

**Password Policy Settings**

Password Policy :  On

Maximum password age :  On

1 day(s)

Minimum password length :  On

8 character(s)

Password complexity :

- Reject common PW and 3 consecutive same chars
- At least one uppercase letter (A-Z)
- At least one lowercase letter (a-z)
- At least one number (0-9)
- At least one symbol

Password Policy Violated User List :

**User Account Lockout Settings**

Lockout Policy :  On

Number of Retries until Locked : 3 time(s)

Lockout Duration : 1 minutes

Lockout Target :  All  Remote Login Only

Locked out Users List :

**Unusable Time Settings**

\* : For these settings to take effect, click Submit and then restart the device and network.  
Restart the device or network on this page: [Restart/Reset](#)

## User Account Lockout Policy

User Account Lockout Policy should be set to strictly control access to the product.

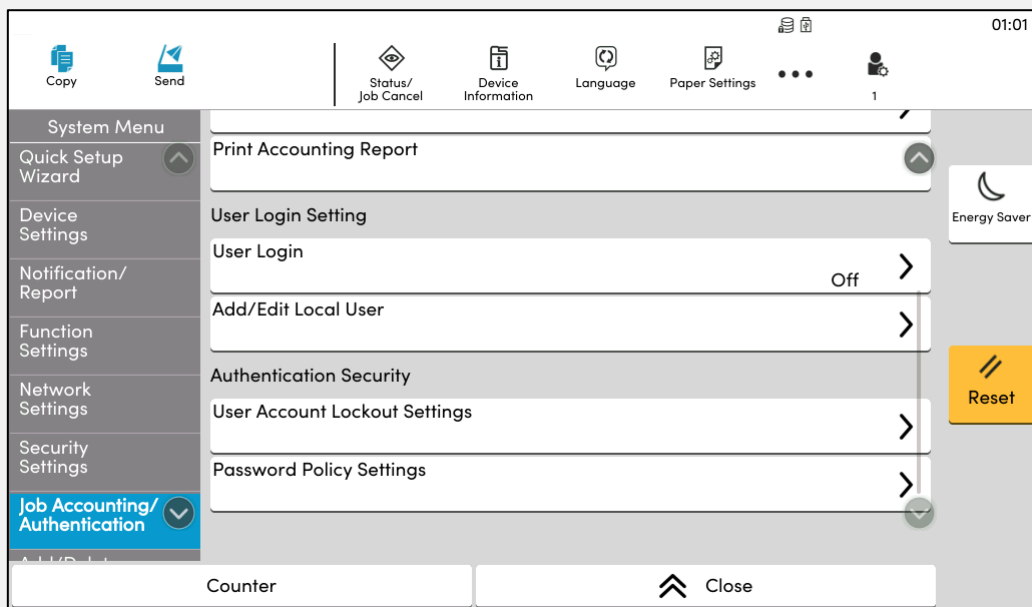
The User Account Lockout Policy detects failed login attempts with incorrect passwords that has repeatedly occurred more than the pre-set number of times and immediately locks the user account for a certain period of time.

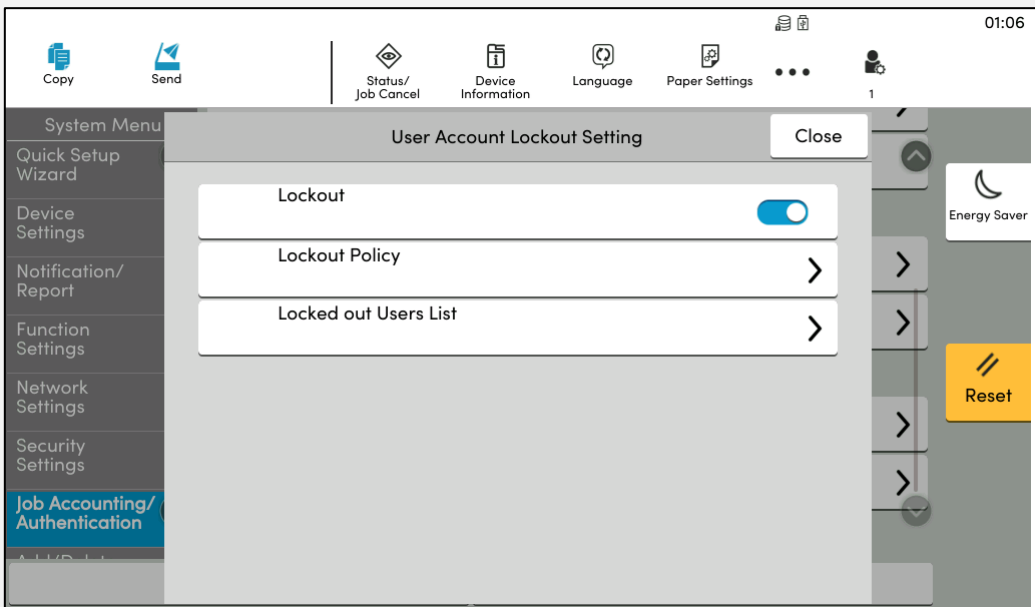
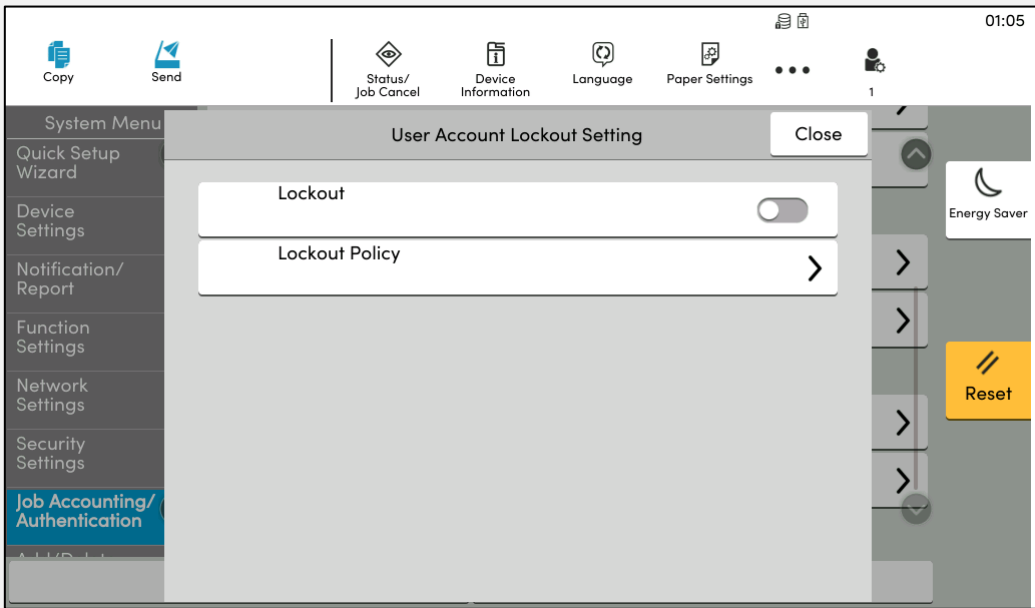
The User Account Lockout Policy helps guard against Denial of Service attacks or Brute Force attacks on the product.

E.g.)

<From the Operational Panel of the product>

1. Click > **Job Accounting/Authentication** > **Authentication Security**.
2. Select **User Account Lockout Settings** > **Lockout, Lockout Policy**.
3. In Lockout, Switch to **On**.





The screens may vary depending on the product model.

E.g.)

<From Web Connection>

## Configuring User Account Lockout Policy Settings

1. Click **Security Settings > Device Security**.
2. Specify the required settings such as **User Account Lockout Settings** as shown in the remote screen.
3. Click **Submit**.

Home

Device Information / Remote Operation

Job Status

Document Box

Address Book

Device Settings

Function Settings

Network Settings

**Security Settings**

Device Security

Send Security

Network Security

Certificates

Management Settings

Links

### Security Settings : Device Security

#### Authentication Security Settings

Password Policy Settings

Password Policy :  On

Maximum password age :  On

1 day(s)

Minimum password length :  On

8 character(s)

Password complexity :

- Reject common PW and 3 consecutive same chars
- At least one uppercase letter (A-Z)
- At least one lowercase letter (a-z)
- At least one number (0-9)
- At least one symbol

Password Policy Violated User List :

**User Account Lockout Settings**

Lockout Policy :  On

Number of Retries until Locked : 3 time(s)

Lockout Duration : 1 minutes

Lockout Target :  All  Remote Login Only

Locked out Users List :

#### Unusable Time Settings

\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)

## Product Management Interface

Access credentials (i.e., an administrator login and password) input to the product management interface should be registered in advance.

If access to the product management interface by general users is not restricted, this could cause unauthorised use or setting change of the product.

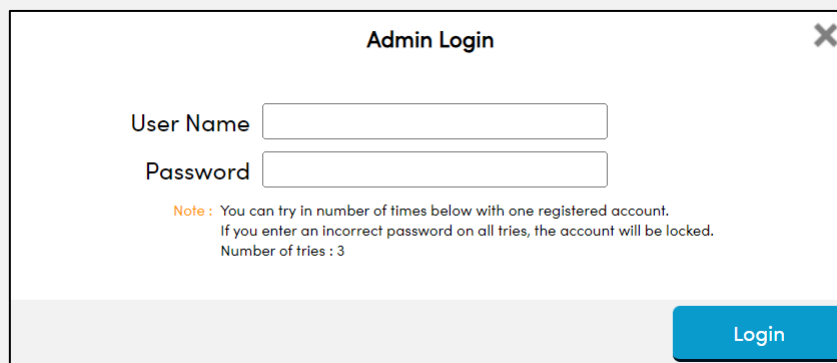
UTAX offers the product management interface (i.e., Command Center Remote extensions) that enables a user who has an administrator privilege only to have real time access to check and change various settings of the UTAX product over the network remotely (via a web browser), thereby protecting the product against unauthorised use and changing settings.

E.g.)

<From Web Connection>

### Configuring Web-Based Administrator Login

1. Click Login or **Admin Login** in the upper right corner of the remote screen, then the Admin Login screen appears.
2. Enter the **User Name** and **Password**.
3. Click **Login**.



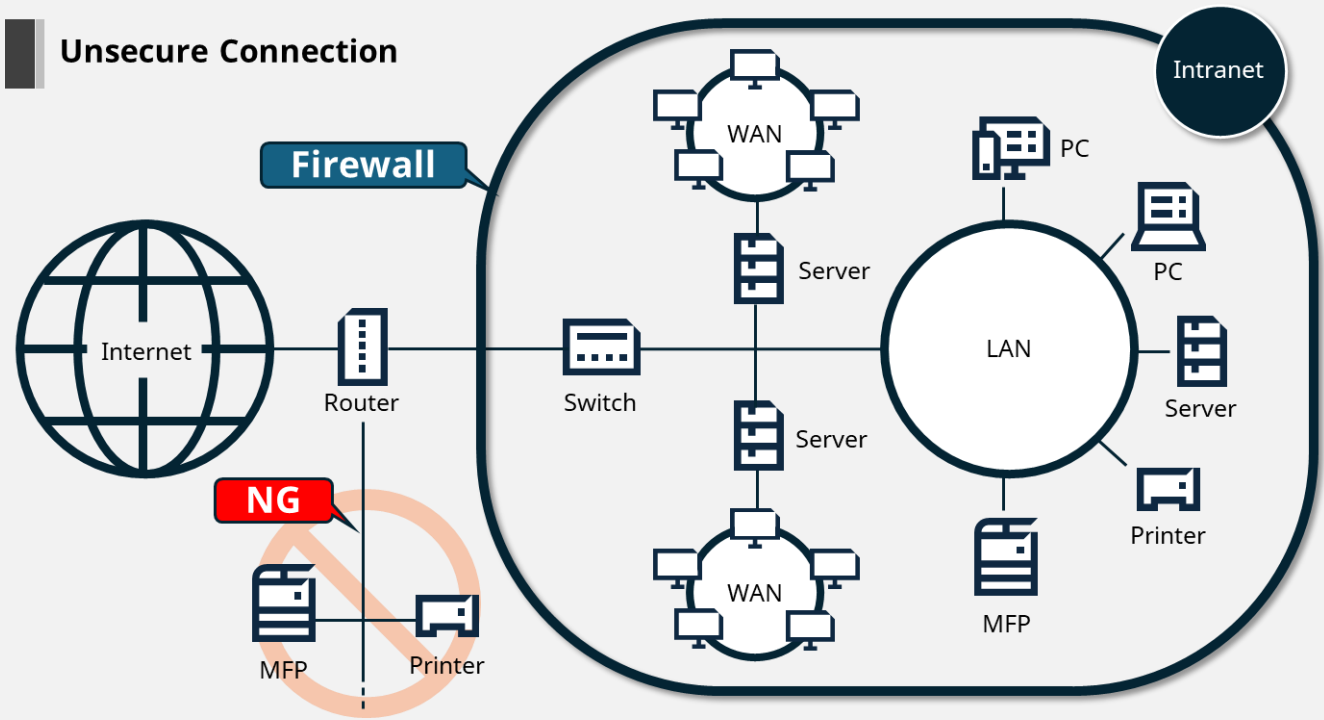
The screenshot shows a web-based login window titled "Admin Login" with a close button (X) in the top right corner. Below the title, there are two input fields: "User Name" and "Password". Below these fields is a note: "Note: You can try in number of times below with one registered account. If you enter an incorrect password on all tries, the account will be locked. Number of tries : 3". At the bottom right of the window is a blue button labeled "Login".

# Network Security

## Internet Connection

A product should not be connected directly to the Internet. A local IP address should be assigned to the product, which is connected to an internal network (LAN) with firewall/router protection, separated from the external network.

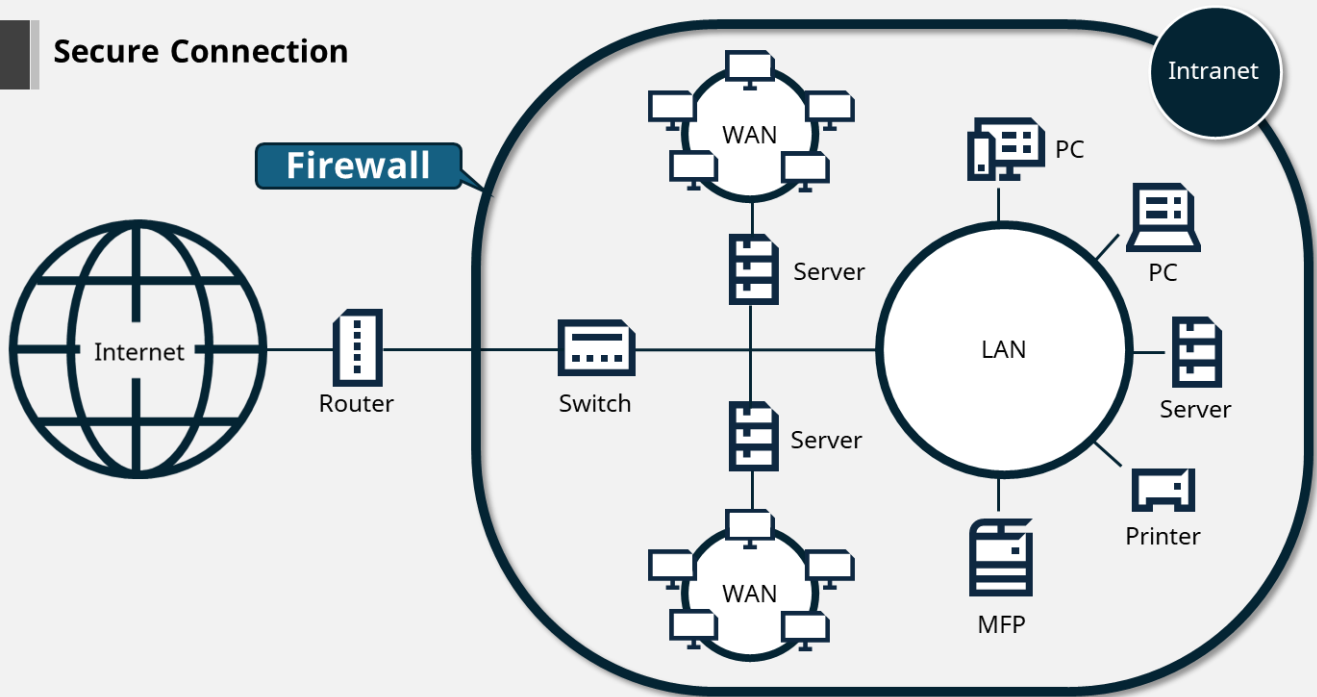
If the product is connected directly to the Internet without a firewall/router that enables to control access from the Internet, the product is directly exposed to attacks from the external network. In other words, the data stored on the product when copying, printing and faxing, and the personal data such as address book entries are exposed and can be viewed from the external network. This causes risks for unauthorised access to the product, resulting in alteration of security settings and send destination, and data leaks.



Accessible by unspecified number of users from the Internet (i.e., from the external network)



## Secure Connection



Accessible only by legitimated users on LAN (i.e., inhouse)

The following data should be protected:

- Data stored in HDD/SSD on the product
- Data stored in User Box/Job Box/FAX Box inside the product
- Destinations registered on the destination list such as address book and personally identifiable information
- Data stored in Shared Box
- Device settings
- Audit Logs

### **NOTE**

*Since the product is a network-connected device, it should restrict network access, the use of network protocols and ports, and deter malware.*

*Administrators should set enable/disable FTP, HTTP, IPP, SMTP, RAW, SNMP and other common protocols on a product basis to block unnecessary connections.*

*Also, the use of the product should be restricted by setting of IP address, allowing only the specified ranges of IP addresses (and subnet mask combinations) to be permitted/rejected access to the product and to send/receive documents.*

*In addition, the product should be able to use encryption protocols such as SSL/TLS and IPsec to protect data in transit over the network.*

*Finally, UTAH obtained Wi-Fi CERTIFIED WPA 3 certification. The products that support this feature offer more robust protection against unauthorised use. This helps prevent attacks like KRACKs and Brute-force.*

E.g.)

<From Web Connection>

## Configuring Protocol Settings

1. Click **Network Settings** > **Protocol**.
2. Specify the required settings to switch **Off/On** for any of the protocols as shown in the remote screen.
3. Click **Submit**.

Home

Device Information / Remote Operation

Job Status

Document Box

Address Book

Device Settings

Function Settings

**Network Settings**

General

TCP/IP

Protocol

Security Settings

Management Settings

Links

### Network Settings : Protocol

Print Protocols

\*NetBEUI :  Off

\*LPD :  Off

\*FTP Server (Reception) :  Off

\*IPP :  Off

\*IPP over TLS :  On

Note :  
To use these settings, enable TLS. [Network Security](#)

\*Port Number :  (1 - 32767)

\*IPP over TLS Certificate : Device Certificate 1

IPP Authentication :  Off

\*Raw :  Off

\*WSD Print :  Off

Note :  
This setting is used commonly with WSD Print and WSD Scan.

POP3 (E-mail RX) :  Off

Note :  
For more settings, click here. [E-mail Settings](#)

Note :  
E-mail printing is unavailable if remote printing is not enabled. [Printer Settings](#)

\* : For these settings to take effect, click Submit and then restart the device and network.  
Restart the device or network on this page: [Restart/Reset](#)

E.g.)

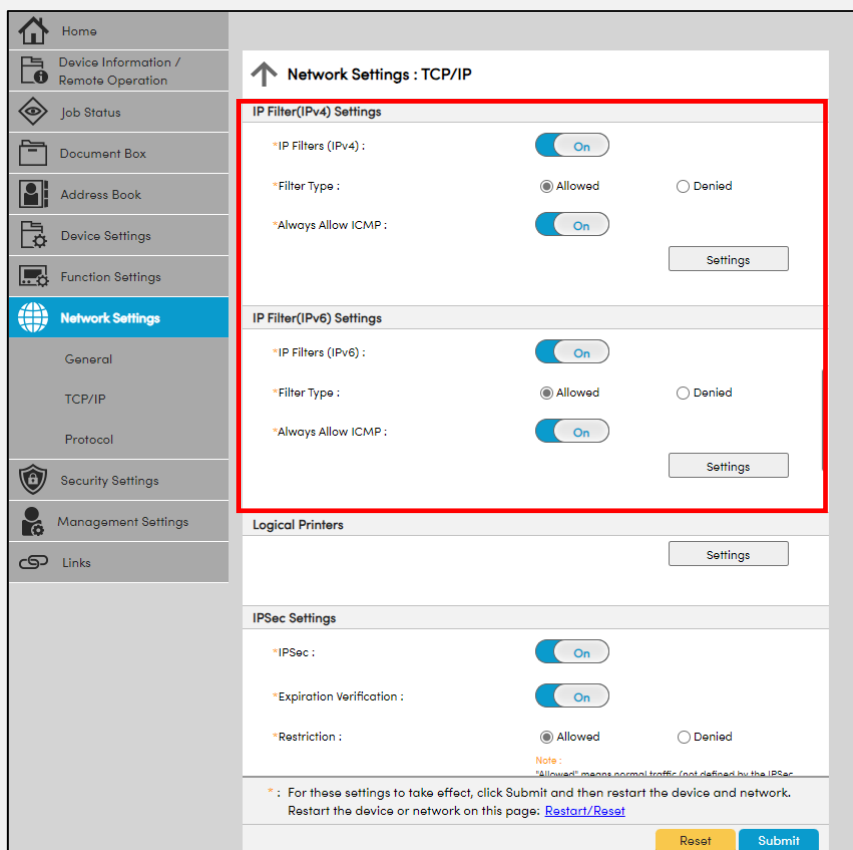
<From Web Connection>

### Configuring IP Filter(IPv4) Settings

1. Click **Network Settings** > **TCP/IP**.
2. Set IP Filters (IPv4) to **On**.
3. In Filter Type, select either **Allowed** or **Denied**.
4. If necessary, set Always Allow ICMP to **On**.
5. Click **Settings**.

### Configuring IP Filter(IPv6) Settings

1. Click **Network Settings** > **TCP/IP**.
2. Set IP Filters (IPv6) to **On**.
3. In Filter Type, select either **Allowed** or **Denied**.
4. If necessary, set Always Allow ICMP to **On**.
5. Click **Settings**.



E.g.)

<From Web Connection>

## Configuring Network Access Settings

1. Click **Security Settings > Network Security**.
2. Specify the required settings such as **Filtering/Firewall, SNMPv1/v2c, SNMPv3, TLS, IEEE802.1X, and IPSec**.
3. Click **Submit**.

**Security Settings : Network Security**

Effective Encryption :

ARCFOUR       DES  
 3DES       AES  
 AES-GCM       CHACHA20/POLY1305

Note:  
Automatically use the appropriate encryption when selecting more than one effective encryption.

Hash :

SHA1       SHA2(256/384)

**Network Access Settings**

**Filtering/Firewall :** Network access to the device can be restricted to allow only specific network addresses. Refer to this link: [IP Filter\(IPv4\) Settings](#) [IP Filter\(IPv6\) Settings](#)

**SNMPv1/v2c :** The SNMP Read and Write Community settings function as passwords to control read and write access to the device via SNMP. Refer to this link: [SNMP Settings](#)

**SNMPv3 :** The SNMPv3 communication settings are used to control authentication and encryption communication that occur via SNMP. Refer to this link: [SNMP Settings](#)

**TLS :** To use TLS communication, Secure Protocols must be enabled. See Secure Protocol Settings at the top of this page.

**IEEE802.1X :** To use IEEE802.1X communication, IEEE802.1X communication must be enabled. Refer to this link: [IEEE802.1X Settings](#)

**IPSec :** To use IPSec communication, IPSec must be enabled. Refer to this link: [TCP/IP](#)

\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)

E.g.)

<From Web Connection>

## Configuring IP Settings (Wired Network)

1. Click **Network Settings > TCP/IP**.
2. This screen includes the following items for configuration: **DHCP/BOOTP, Auto-IP, IP Address, Subnet Mask, Domain Name, DNS Server, DNS Search Suffix, DNS over TLS, Certificate Auto Verification, Hash, and WINS Server**.
3. Click **Submit**.

The screenshot shows the 'Network Settings : TCP/IP' configuration page. The left sidebar contains navigation links: Home, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings (highlighted), General, TCP/IP, Protocol, Security Settings, Management Settings, and Links. The main content area is titled 'IPv4 Settings (Wired Network)' and contains the following settings:

- \*DHCP/BOOTP:  On
- \*Auto-IP:  On
- \*IP Address: 192.168.11.66
- \*Subnet Mask: 255.255.255.0
- \*Domain Name: [Empty field]
- \*DNS Server:  Use DNS Server from DHCP,  Use following DNS Server
- \*DNS Server (Primary): [Empty field]
- \*DNS Server (Secondary): [Empty field]
- \*DNS Search Suffix:  Use DNS Search Suffix from DHCP,  Use following DNS Search Suffix
- \*DNS Search Suffix (Primary): [Empty field]
- \*DNS Search Suffix (Secondary): [Empty field]
- \*DNS over TLS: On
- Certificate Auto Verification:  Validity Period,  Server Identity,  Chain
- Hash:  SHA1,  SHA2(256/384)
- \*WINS Server:  Use WINS Server from DHCP,  Use following WINS Server
- \*WINS Server (Primary): [Empty field]

\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)

Buttons: Reset, Submit

E.g.)

<From Web Connection>

## Configuring IPsec Settings

1. Click **Network Settings > TCP/IP**.
2. Switch to **On** to use IPsec protocol.
3. Specify the required settings such as **Expiration Verification, Restriction,** and **Root Certificate**.
4. Click **Submit**.

Home

Device Information / Remote Operation

Job Status

Document Box

Address Book

Device Settings

Function Settings

**Network Settings**

General

TCP/IP

Protocol

Security Settings

Management Settings

Links

### Network Settings : TCP/IP

#### IPsec Settings

\*IPsec :  On

\*Expiration Verification :  On

\*Restriction :  Allowed  Denied

Note :  
"Allowed" means normal traffic (not defined by the IPsec rules) will be allowed to reach the device in addition to the IPsec traffic (as defined by the IPsec rules).  
"Denied" means only IPsec traffic (as defined by the IPsec rules) will be allowed to reach the device and all other traffic (not defined by the IPsec rules) will be denied to reach the device.

Root Certificate :

Root Certificate 1 Subject :

Root Certificate 2 Subject :

Root Certificate 3 Subject :

Root Certificate 4 Subject :

Root Certificate 5 Subject :

Note :  
Make settings for Device Certificates here: [Certificates](#)

\* : For these settings to take effect, click Submit and then restart the device and network.  
Restart the device or network on this page: [Restart/Reset](#)

Restart Submit

### NOTE

*At UTAX, we conduct our own vulnerability tests and penetration tests performed by a third party to ensure the security for our products without vulnerabilities. However, if the product is connected directly to the Internet, customers are facing security risks for the product.*

## TLS Encrypted Communication

When accessing a product through a web browser or network printing, the communication data in transit should be encrypted by enabling the TLS protocol. Communication destination should also be checked if it is a legitimate connection destination. TLS protocol helps prevent tapping and alteration and makes it difficult to analyse the data.

If TLS encrypted communication is not supported, this causes risks for alteration, leakage, tapping of settings information and print data, sending information to unauthorised destinations (i.e., devices), and unauthorised access to the product from the external network.

Depending on the security level corresponding to each organisation's environment, a stronger version of encryption protocol (e.g., TLS 1.3) or encryption algorithm (AES) can be set. Self-certificates and CSR certificates support secure and stronger level of TLS 1.3/SHA-2.

### NOTE

*Use available stronger encryption for communication.*

*UTAX products support TLS encryption protocols including TLS1.0, 1.1, 1.2, and 1.3. The availability of these features depends on the product model.*

E.g.)

<From Web Connection>

## Configuring TLS

1. Click **Security Settings > Network Security**.
2. Specify the required settings such as **TLS Version (TLS1.0/TLS1.1/TLS1.2/TLS1.3)**, **Effective Encryption (ARCFOUR/DES/3DES/AES/AES-GCM/CHACHA20/POLY1305)**, **Hash (SHA1/SHA2(256/384))**, **HTTP Security (Secure Only (HTTPS)/Not Secure (HTTPS & HTTP))**, **IPP Security (Secure Only (IPPS)/Not Secure (IPPS & IPP))**, **Enhanced WSD Security (Secure Only (Enhanced WSD over TLS)/Not Secure (Enhanced WSD over TLS & Enhanced WSD))**, **eSCL Security (Secure Only (eSCL over TLS)/Not Secure (eSCL over TLS & eSCL))**, **REST Security (Secure Only (REST over TLS)/Not Secure (REST over TLS & REST))**, and **Clientside Settings**.
3. Click **Submit**.

Home

Device Information / Remote Operation

Job Status

Document Box

Address Book

Device Settings

Function Settings

Network Settings

**Security Settings**

Device Security

Send Security

Network Security

Certificates

Management Settings

Links

### Security Settings : Network Security

Secure Protocol Settings

\*TLS :  On

Note:  
If you select Off, TLS cannot be used for communication.

Serverside Settings :

\*TLS Version :  TLS1.0  TLS1.1  
 TLS1.2  TLS1.3

\*Effective Encryption :  ARCFOUR  DES  
 3DES  AES  
 AES-GCM  CHACHA20/POLY1305

\*Hash :  SHA1  SHA2(256/384)

\*HTTP Security :  Secure Only (HTTPS)  
 Not Secure (HTTPS & HTTP)

\*IPP Security :  Secure Only (IPPS)  
 Not Secure (IPPS & IPP)

\*Enhanced WSD Security :  Secure Only (Enhanced WSD over TLS)  
 Not Secure (Enhanced WSD over TLS & Enhanced WSD)

\*eSCL Security :  Secure Only (eSCL over TLS)  
 Not Secure (eSCL over TLS & eSCL)

\*REST Security :  Secure Only (REST over TLS)  
 Not Secure (REST over TLS & REST)

Clientside Settings :

TLS Version :  TLS1.0  TLS1.1  
 TLS1.2  TLS1.3

Effective Encryption :  ARCFOUR  DES

\* : For these settings to take effect, click Submit and then restart the device and network.  
Restart the device or network on this page: [Restart/Reset](#)

Reset Submit



E.g.)

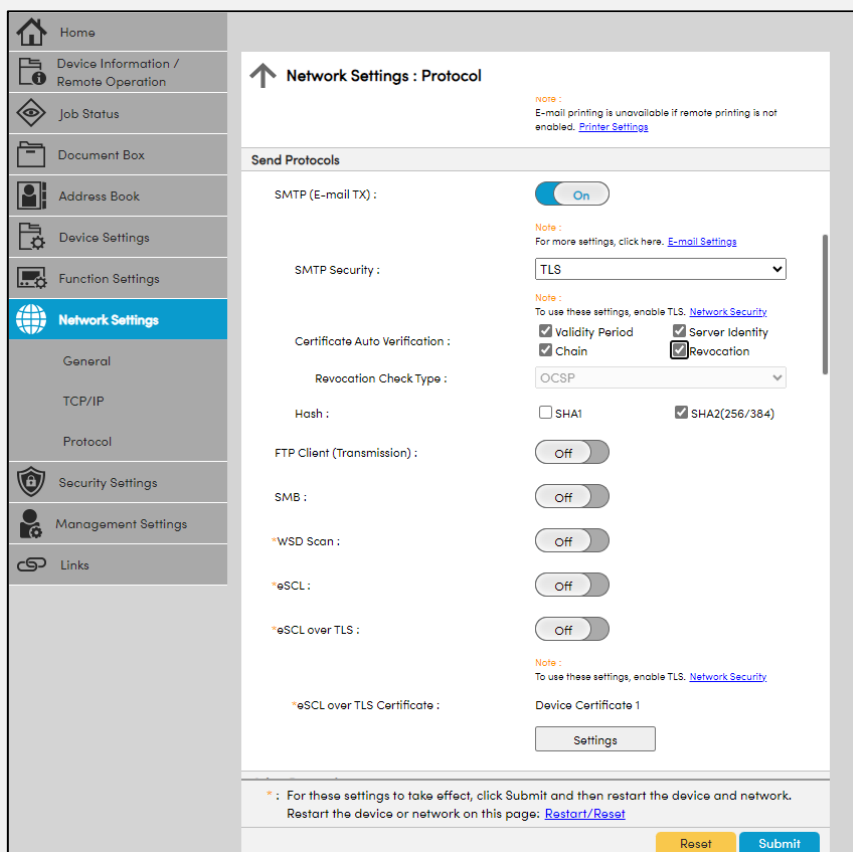
<From Web Connection>

## Configuring protocols for sending email

1. Click **Network Settings > Protocol**.
2. In SMTP (E-mail TX), switch to **On**.
3. In SMTP Security, select **TLS**.
4. In Certificate Auto Verification, select the check box for the following in sequence: **Validity Period, Server Identity, Chain, and Revocation**.
5. In Revocation Check Type, select from the following: **OCSP, CRL, CRL & OCSP**.
6. For Hash algorithm, select the box for either **SHA1** or **SHA2(256/384)**.

### NOTE

The remote screen shows an example to confirm a communication destination if it is a legitimate connection destination.



Home

Device Information / Remote Operation

Job Status

Document Box

Address Book

Device Settings

Function Settings

**Network Settings**

General

TCP/IP

Protocol

Security Settings

Management Settings

Links

### Network Settings : Protocol

Note :  
E-mail printing is unavailable if remote printing is not enabled. [Printer Settings](#)

#### Send Protocols

SMTP (E-mail TX) :  On

Note :  
For more settings, click here. [E-mail Settings](#)

SMTP Security :

Note :  
To use these settings, enable TLS. [Network Security](#)

Certificate Auto Verification :  
 Validity Period  Server Identity  
 Chain  Revocation

Revocation Check Type :

Hash :  SHA1  SHA2(256/384)

FTP Client (Transmission) :  Off

SMB :  Off

\*WSD Scan :  Off

\*eSCL :  Off

\*eSCL over TLS :  Off

Note :  
To use these settings, enable TLS. [Network Security](#)

\*eSCL over TLS Certificate :  
Device Certificate 1

\* : For these settings to take effect, click Submit and then restart the device and network.  
Restart the device or network on this page: [Restart/Reset](#)

E.g.)

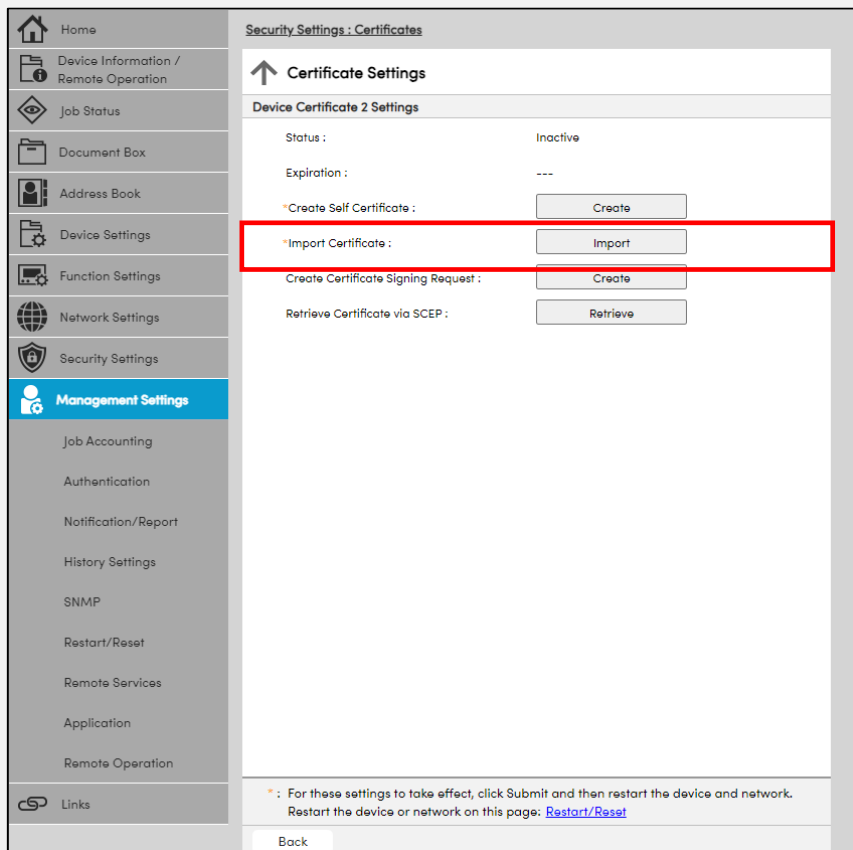
<From Web Connection>

## Importing a CA-Issued Certificate

1. Click **Security Settings > Certificate Settings**.
2. In Import Certificate, select **Import** on a root certificate.
3. Select **Choose File** to browse for the certificate file.
4. Select **Open**.
5. Click **Submit** after importing the root certificate.

### NOTE

The remote screen shows an example of management settings for the respective certificate settings. We recommend a CA-issued certificate be imported for a device certificate as indicated in the red box.



The screenshot displays the 'Security Settings: Certificates' configuration page. On the left is a navigation menu with 'Management Settings' selected. The main content area is titled 'Certificate Settings' and contains a section for 'Device Certificate 2 Settings'. The status is 'Inactive' and the expiration is '---'. A red box highlights the 'Import Certificate' option, which has an 'Import' button next to it. Other options include 'Create Self Certificate' (Create), 'Create Certificate Signing Request' (Create), and 'Retrieve Certificate via SCEP' (Retrieve). A note at the bottom states: '\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)'. A 'Back' button is located at the bottom left of the main content area.

## Stored Data Protection

### HDD/SSD Encryption

Any encryptions available for the product should be used and security features supported should be used to ensure the product is as secure/strong as possible.

Image data obtained when copying, printing, faxing and scanning is stored on an HDD/SSD inside the product. User registration, device settings, and address books are also stored on the drives. If the HDD/SSD is removed from the product by a malicious person, the data/information stored on the HDD/SSD may be leaked.

By enabling the HDD/SSD encryption feature, data to be stored on an HDD/SSD is encrypted for protection. The encryption algorithm and key length adopt AES (FIPS 197) and 256 bits, respectively, which are used for the government documents. Even if the HDD/SSD is removed from the product by a malicious person, the sensitive or confidential data stored on the HDD/SSD cannot be leaked. Because the data is protected by encryption, it will be impossible to analyse the data even if the drive is connected to a PC analysis tool.

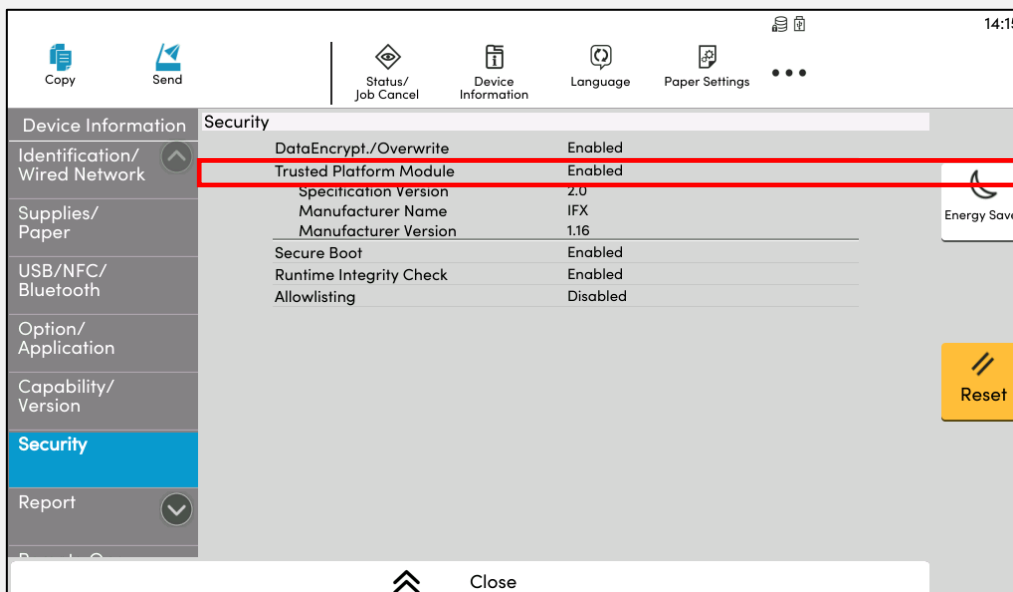
#### NOTE

*The product will have a cryptographic module, which meets **FIPS 140-3** level 2 requirements. The cryptographic module is designed and implemented by UTAX. FIPS140-3 certification for its cryptographic module is in the review phase.*

**NOTE**

The operational panel of the product shows an example of Security Settings for **Trusted Platform Module** setting as indicated in the red box.

Some UTAX products are equipped with the Trusted Platform Module. An encryption key used for encrypting the HDD is encrypting by a root encryption key contained in the Trusted Platform Module. Certificates are encrypted by the same root encryption key. The HDD encryption key and the root encryption key are saved separately. The root encryption key is rigorously protected within the Trusted Platform Module so that it cannot be disclosed outside of the security chip. Even if the HDD is removed from the product, data stored on the HDD cannot be leaked and is securely protected.



The screens may vary depending on the product model.

# Device Management

## Audit Logs

Audit logs for all activities (e.g., login logs, device logs, and security communication error logs) on the product are highly recommended to provide administrators with visible records such as when and how the product or document is accessed and handled. In other words, organisations should monitor security logs from the product via SIEM to detect any intrusion in real time. The product should seamlessly communicate with the SIEM using syslog protocol. Therefore, the SIEM server notifies clients of external attacks and threats based on the analysis results.

E.g.)

<From Web Connection>

### Configuring settings for Audit Log (Syslog) Setting

1. Click **Management Settings** > **History Settings**.
2. Displays the status for **Syslog**.
3. In **Destination Server**, enter the address for the destination server.
4. In **Port Number**, enter the port number for Syslog.
5. In **Facility**, select the number of facilities that obtains the log from the drop-down list.
6. In **Severity**, select the severity of obtained log from the drop-down list.

The screenshot shows a web interface for 'Management Settings : History Settings'. The left sidebar contains a navigation menu with 'Management Settings' highlighted. The main content area is titled 'Job Log History' and contains several configuration fields. A red box highlights the 'Audit Log (Syslog) Setting' section, which includes the following fields and options:

- Syslog**: On
- Destination Server**: [Empty text input field]
- Port Number**: 514 (1 - 65535)
- Facility**: 6 (dropdown menu)
- Severity**: 7 (dropdown menu)

Additional fields in the 'Job Log History' section include: Recipient E-mail Address, Subject, Auto Sending (Off), Number of Records (16), Personal Information (Include/Exclude), and Run once now (Send).

Notes in the highlighted section: 'Settings must be made in Remote Syslog: [Protocol](#)' and 'To specify the server name by domain name, set DNS server: [TCP/IP](#)'.

Buttons for 'Reset' and 'Submit' are located at the bottom right of the page.

E.g.)

<From Web Connection>

## Configuring Event Report/Scheduled Report settings

1. Click **Management Settings > Notification/Report.**
2. In **Syslog Records Kept Alert**, switch to **On.**
3. Click **Submit.**

The screenshot shows the 'Management Settings : Notification/Report' page. The left sidebar contains a menu with 'Management Settings' highlighted. The main content area is titled 'Event Report / Scheduled Report 1' and contains the following settings:

- Recipient 1 E-mail Address :
- Subject :   
Subject Conversion Strings  
%printer : Model  
%serial : Serial Number  
%etheraddr : MAC Address  
%host : Host Name  
%ip : IP Address
- Event Report :
  - Add Paper
  - Add Toner
  - Full Waste Toner Box
  - All other Errors
  - Time for Maintenance
  - Low Toner
  - Cover Open
  - Paper Jam
  - Time for Maintenance soon
- Event Report Interval :  minutes
- Notify when Data Sanitization Starts :  Off
- Syslog Records Kept Alert :  On** (highlighted with a red box)
- Notify when Malicious Program is Detected :  On
- Scheduled Report :
  - Counter Status
- Scheduled Report Interval :
- Run once now :

At the bottom right, there are 'Reset' and 'Submit' buttons.

## Log Status/Job Logs

Users (i.e., Administrators) should check the product is securely used and checked for unauthorised access, and should update the product settings to control who can access and use the product regularly. To confirm this, Log Status/Job Logs should be set.

These logs provide job information and fax transmission logs such as who has accessed the product, what errors have occurred, and how the functions have been used.

The job logs highly disincentivise unauthorised use of the product or data leaks by a malicious person and allow tracking unauthorised access to the product.

E.g.)

<From Web Connection>

### Configuring Job Status/Job Logs Settings

1. Click **Security Settings > Device Security**.
2. In **Display Jobs Details Status, Display Jobs Log**, select **Show All/My Jobs Only/Hide All** from the drop-down list. In **Display Fax Log**, switch to **Show All/Hide All**. In **Pause/Resume of All Print Jobs**, switch to **Prohibit/Permit**.
3. Click **Submit**.

The screenshot shows the 'Security Settings : Device Security' configuration page. The left sidebar contains navigation options: Home, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings, Security Settings (highlighted), Device Security, Send Security, Network Security, Certificates, Management Settings, and Links. The main content area is titled 'Security Settings : Device Security' and includes several sections: 'Interface Block' with settings for Network, USB Device, USB Host, USB Drive, and Optional Interface; 'Lock Operation Panel' with an 'Operation Panel' dropdown set to 'Unlock'; 'Job Status/Job Logs Settings' (highlighted with a red box) containing 'Display Jobs Detail Status' (dropdown set to 'Hide All'), 'Display Jobs Log' (dropdown set to 'Hide All'), 'Display FAX Log' (radio buttons for 'Show All' and 'Hide All', with 'Hide All' selected), and 'Pause/Resume of All Print Jobs' (radio buttons for 'Prohibit' and 'Permit', with 'Permit' selected); 'Edit Restriction' with 'Address Book' and 'One Touch Key' set to 'Administrator Only'; and 'Authentication Security Settings' with 'Password Policy' set to 'Off'. A note at the bottom states: '\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)'. At the bottom right are 'Reset' and 'Submit' buttons.

## Interface Block

Security features supported by the product should be used to ensure the product is as secure/strong as possible. According to the users' security policy, access through the product's interface such as USB Device, USB Host, Optional Interface should be blocked. Network interface should also be restricted on a protocol basis.

If these settings are not proper, risks for data leaks or unauthorised access to data on the product can exist.

These Interface Block settings prevent data leaks from the USB interface via USB memory as well as prevent the spread of viruses.

E.g.)

<From Web Connection>

### Configuring Interface Block setting

1. Click **Security Settings > Device Security**
2. In **USB Device, USB Host, USB Drive, and Optional Interface**, switch to Block/Unblock. To configure the detailed settings, go to **Network Settings > Protocol**.
3. Click **Submit**.

The screenshot shows the 'Security Settings : Device Security' web interface. The 'Interface Block' section is highlighted with a red box. It contains the following settings:

Setting	Block	Unblock
Network :	<input type="radio"/>	<input type="radio"/>
*USB Device :	<input checked="" type="radio"/>	<input type="radio"/>
*USB Host :	<input checked="" type="radio"/>	<input type="radio"/>
*USB Drive :	<input type="radio"/>	<input checked="" type="radio"/>
*Optional Interface :	<input checked="" type="radio"/>	<input type="radio"/>

Below the 'Interface Block' section, there are other settings:

- Lock Operation Panel**: Operation Panel: Unlock
- Job Status/Job Logs Settings**: Display Jobs Detail Status: Hide All; Display Jobs Log: Hide All; Display FAX Log: Hide All; Pause/Resume of All Print Jobs: Permit
- Edit Restriction**: Address Book: Administrator Only; One Touch Key: Administrator Only
- Authentication Security Settings**: Password Policy: Off

\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)

Buttons: [Reset](#) [Submit](#)



## Lock Operation Panel

Insiders have a relatively high likelihood of handling their organisations' critical data/information. If some insiders who do not have authorisation conduct unauthorised use of the product or its particular features, this may cause critical data/information leaks of data stored on the product.

Therefore, operations on the product panel should be restricted. The partial lock feature controls options in three areas: input/output, job execution, and paper. This feature has the ability to prohibit system menu and job cancellation operations. Only administrators can set these options.

The partial lock feature prevents unauthorised operations on the product.

E.g.)

<From Web Connection>

### Configuring Lock Operation Panel setting

1. Click **Security Settings > Device Security**.
2. In **Operational Panel**, select **Lock (Partial Lock 1/ Partial Lock 2/Partial Lock 3)/Unlock** from the drop-down list.
3. Click **Submit**.

The screenshot displays the 'Security Settings : Device Security' configuration page. The left sidebar contains navigation options: Home, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings, Security Settings (highlighted), Device Security, Send Security, Network Security, Certificates, Management Settings, and Links. The main content area is titled 'Security Settings : Device Security' and includes several sections: 'Interface Block' with settings for Network, USB Device, USB Host, USB Drive, and Optional Interface; 'Lock Operation Panel' where the 'Operation Panel' dropdown is set to 'Unlock' (highlighted with a red box); 'Job Status/Job Logs Settings' with options for Display Jobs Detail Status, Display Jobs Log, Display FAX Log, and Pause/Resume of All Print Jobs; 'Edit Restriction' for Address Book and One Touch Key; and 'Authentication Security Settings' with a Password Policy toggle set to 'Off'. A footer note states: '\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)'. At the bottom right are 'Reset' and 'Submit' buttons.

# **In the Operation Phase**

## **Device Management**

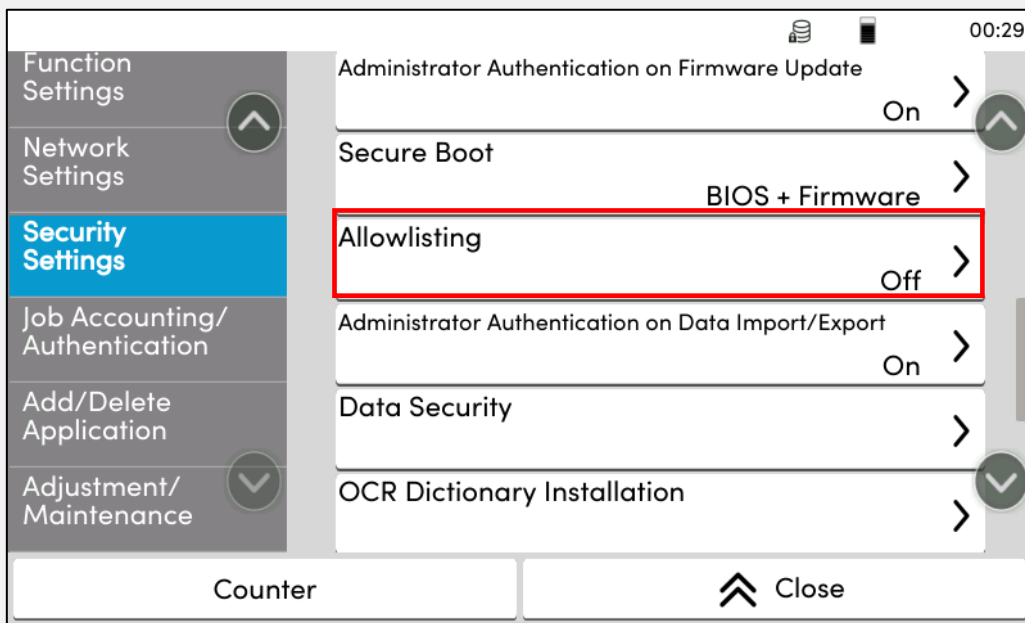
### **Product Software Management**

It is very important for your organisation to keep product software up to date on your UTAX product. To do this, please visit the UTAX global website regularly to check the latest security-related information.

If your device is still running an outdated software version, it could present an opportunity for exploiting the product with known vulnerabilities. Users should maintain the security and functionality of your product by running the latest software version.

**NOTE**

As for security level enhancement, **Allowlisting** can be enabled as a malware prevention measure. If an untrusted program file, which is not included in the allowlist, is found, Allowlisting automatically prevents the program from running. The operational panel of the product shows an example of Security Settings for Allowlisting setting as indicated in the red box. By default, Allowlisting is Off. For enablement, administrators can switch Allowlisting to On from the menu.



The screens may vary depending on the product model.

**NOTE**

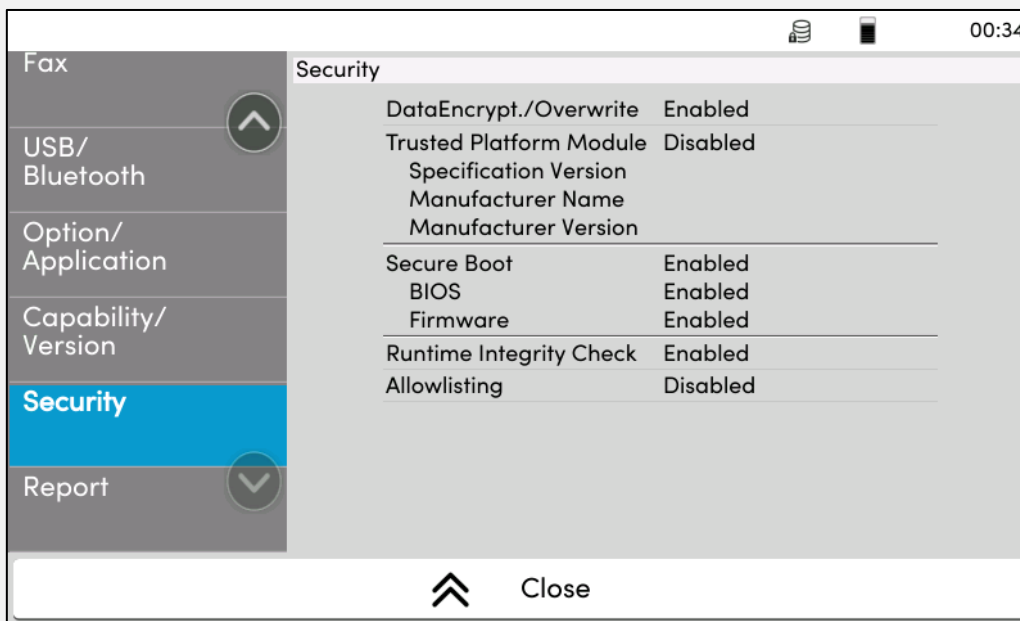
Users should always apply the latest security updates not only to the product but also PCs and servers that handle your valuable information assets to protect against attacks on these IoT devices used for your organisation in the office.

## Authenticity and Integrity of the Firmware

We strongly recommend Digitally-Signed Firmware, Secure Boot and Run Time Integrity Check (RTIC) be used for your UTAX product in order to verify integrity and authenticity of the firmware. Particularly, RTIC can be expected to be more effective as a security measure against firmware alteration when used with the Secure Boot feature.

The firmware validity can be verified by applying a digitally-signed signature to the firmware. When the product starts up, the Secure Boot verifies the firmware is authenticated/legitimate using the digital signature. Even if a firmware is altered by a malicious person, it can never be executed. RTIC regularly verifies if the validity of the firmware is maintained during the operation of the product without altering the firmware deployed on RAM after the product starts up. Even if the firmware is maliciously re-written, it can be detected by confirming the hash value of the firmware uploaded to the product and the hash value created from the signature and a warning is issued as a system error.

With these malware protection settings, the firmware is protected from being altered, damaging the product, and using the product as stepping stone by a malicious third person.



The screens may vary depending on the product model.

# Print Security

## Walk-Up and Authentication Print Job

A print job should be held in the product from a PC until a user enters their appropriate password through the product operational panel.

If printed documents are left on the product tray for a long time or until the owner of the documents walks up to the product to pick them up, the documents may be read or taken by third parties and the document data leaks may be noticed later.

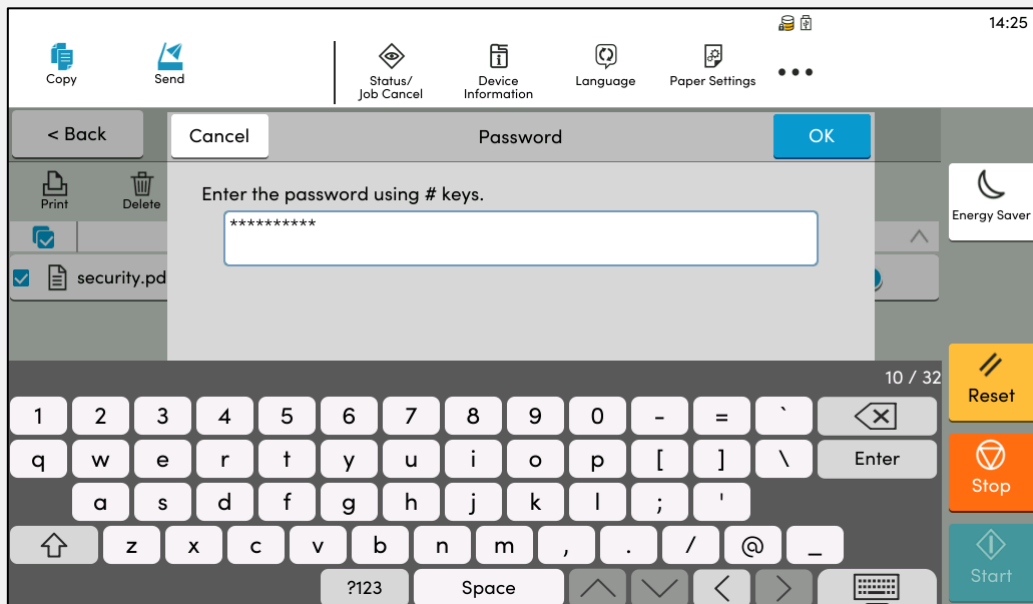
UTAX offers Private Print feature in the print driver. A password can be set for a print job. The print job sent from a PC is held in the product, and then the appropriate password is required to be entered from the panel of the product when printing a document. This prevents the printed documents from being read or taken by third parties.

E.g.)

<From the Operational Panel of the product>

### Configuring Print/Stored Job setting

1. Click **Job Box** > **Private Print**> **Stored Job**.
2. Enter a password in the password field.
3. Click **OK**.



The screens may vary depending on the product model.

# Send Security

## Send Security

The product offers various settings to confirm the send destination (i.e., address numbers) and subject on the screen before sending. This helps prevent sending to the wrong address and transmitting to the unintended destinations caused by unintentionally adding send destination to the group.

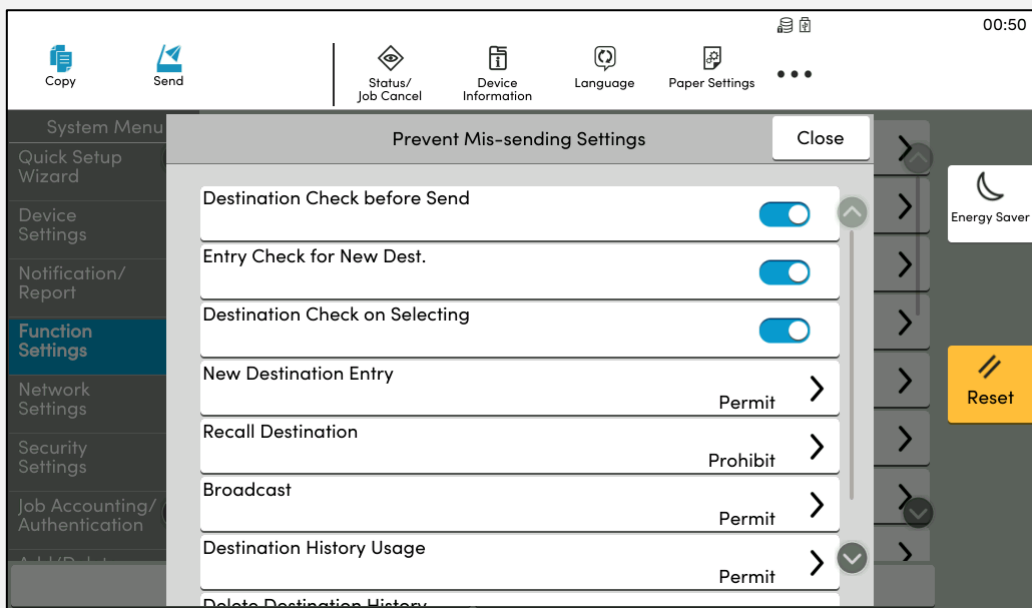
By configuring these correct settings, organisations can rest assured that documents can only be sent to the right owner and will not fall into the wrong hands. This effectively prevents unauthorised use or wrong sending caused by wrong number entry, even by mistakes or errors.

E.g.)

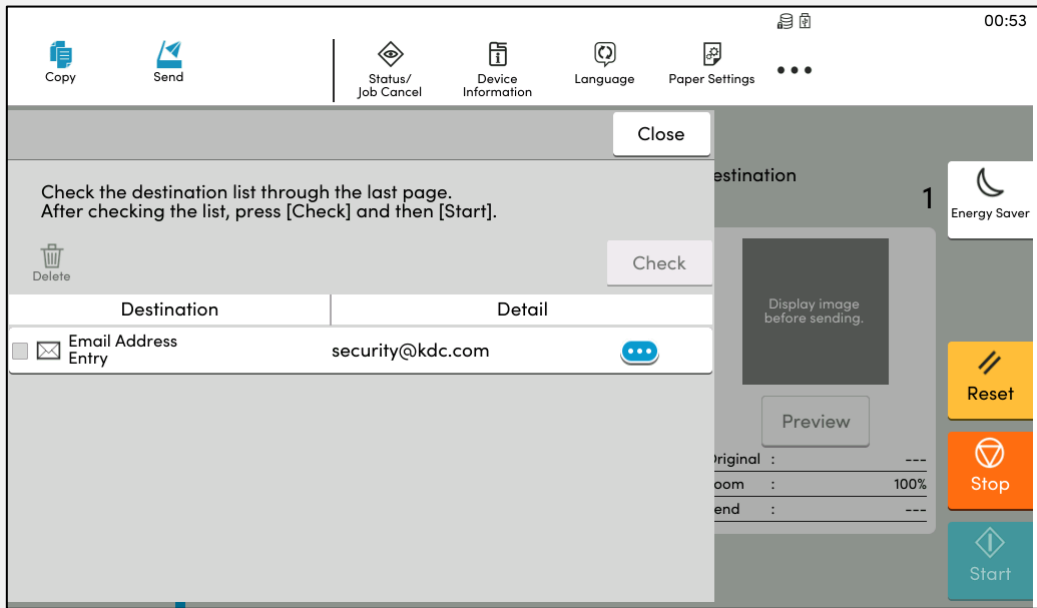
<From the Operational Panel of the product>

### Configuring Send Security setting

1. Click **Function Settings** > **Send/Store** > **Prevent Miss-sending Settings**
2. Switch to **On**.



The screens may vary depending on the product model.



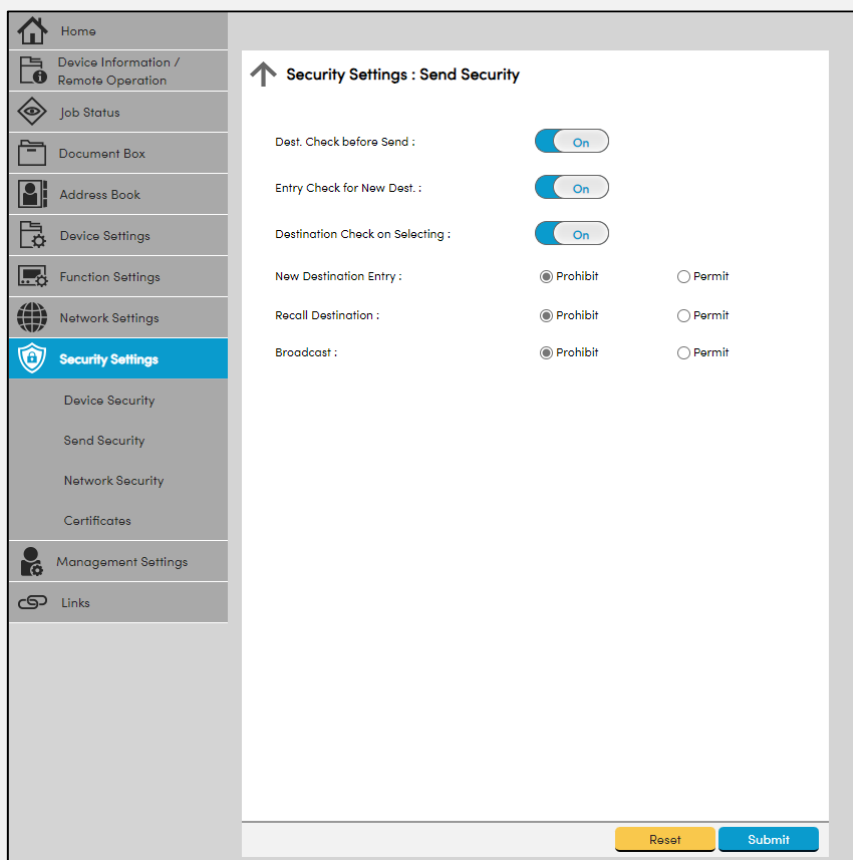
The screens may vary depending on the product model.

E.g.)

<From Web Connection>

### Configuring Send Security setting

1. Click **Security Settings > Send Security.**
2. In **Dest. Check before Send**, **Entry Check for New Dest.**, and **Destination Check on Selecting**, switch to **On/Off**. In **New Destination Entry**, **New Destination Entry (FAX)**, **Recall Destination**, and **Broadcast**, switch to **Prohibit/Permit**.
3. Click **Submit.**





# In the Decommission Phase

## Stored Data Protection

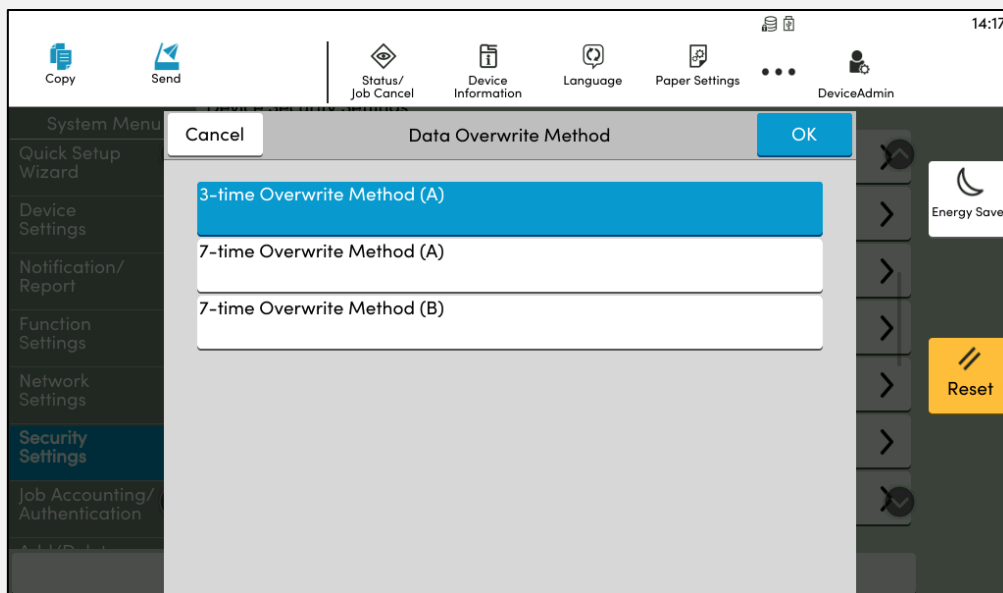
### Data Sanitisation

At the product's lease end or end of life, administrators set and execute sanitisation features to completely sanitise the data retained inside the product or any residual data, using the Data Overwrite Methods such as DoD5200.22-M, DoD 5220.22-M ECE, BSI/VSITR, and/or the SSD Secure Erase (depending on the product model). Product settings can revert to factory default settings.

This prevents critical data/information restoration and data/information leaks to the outside.

#### Note

The operational panel of the product shows an example of Data Overwrite Method: 3-time Overwrite Method (A) that conforms to **the U.S. Department of Defense, DoD 5220.22-M**, 7-time Overwrite Method (A) that conforms to **the U.S. Department of Defense, DoD 5220.22-M ECE**, and 7-time Overwrite Method (B) that conforms to **the German Federal Office for Information Security, BSI/VSITR**.



The screens may vary depending on the product model.

E.g.)

<From Web Connection>

## Configuring Reserve a Sanitisation Time setting

1. Click **Security Settings > Device Security**.
2. Specify the required settings such as **Reserve a Sanitisation Time** and **Device Use After Sanitisation**.
3. Click **Submit**.

The screenshot displays the 'Security Settings : Device Security' configuration page. The left sidebar contains navigation options: Home, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings, Security Settings (highlighted), Device Security, Send Security, Network Security, Certificates, Management Settings, and Links. The main content area is titled 'Security Settings : Device Security' and includes several sections: 'Unusable Time Settings' with 'Unusable Time' set to 'Off'; 'Data Security Settings' with a 'Settings' button; 'Data Sanitization' (highlighted with a red box) with 'Reserve a Sanitization Time' set to 'On', and dropdowns for Year (2024), Month (10), Day (25), and Hour (01). 'Device Use After Sanitization' is set to 'Prohibit' (radio button selected). Below this is the 'Firmware Update' section with 'Administrator Authentication on Firmware Update' set to 'On'. The 'Data Import/Export' section has 'Administrator Authentication on Data Import/Export' set to 'On'. The 'Secure Boot' section has 'Secure Boot' set to 'BIOS + Firmware' (radio button selected). At the bottom, a note states: '\* : For these settings to take effect, click Submit and then restart the device and network. Restart the device or network on this page: [Restart/Reset](#)'. There are 'Reset' and 'Submit' buttons at the bottom right.

---

© 2025 UTAX (UK) Limited

UTAX (UK) LIMITED

89 Shrivenham Hundred Business Park  
Watchfield, Swindon, SN6 8TY



UTAX does not warrant that any specifications mentioned will be error-free. Specifications are subject to change without notice. Information is correct at time of going to press. All other brand and product names may be registered trademarks or trademarks of their respective holders and are hereby acknowledged.