kyoceradocumentsolutions.com

Command Center RX User Guide

ECOSYS MA4000wifx
ECOSYS MA4000x
ECOSYS MA3500fx
ECOSYS PA4000x
ECOSYS MA4000wfx
ECOSYS MA3501wfx
ECOSYS MA3500x
ECOSYS PA3500wx
ECOSYS MA4000fx
ECOSYS MA3500wfx
ECOSYS PA4000wx
ECOSYS PA3500x

2025.11
C1DCCRXKDEN02

General Information

About This Guide

This user guide is intended to help you configure the settings using the Command Center RX correctly and take simple troubleshooting measures as needed so that the machine can always be used in the optimum condition.

The settings and screens described in this guide may be different according to the machine type or destination.

Legal Notes

Unauthorized reproduction of all or part of this guide is prohibited.

The information in this guide is subject to change without notice.

Examples of the operations given in this guide support the Windows 10 printing environment.

We cannot be held liable for any problems arising from the use of this product, regardless of the information herein.

Regarding Trademarks

Microsoft Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries. KPDL is a trademark of Kyocera Corporation. PCL is a trademark of Hewlett-Packard Company. Google and Google Chrome are trademarks of Google LLC.

All other brand and product names herein are registered trademarks or trademarks of their respective companies.

Table of Contents

Chapter 6 Device Settings

Chapter 7 Function Settings

Chapter 8 Network Settings

Chapter 9 Security Settings

Chapter 10 Management Settings

Chapter 11 Troubleshooting

1 Introduction

Command Center RX (Remote eXtension), which will hereafter be referred to as the embedded server, refers to the web server that is built into the printing device. It allows you to verify the operating status of the device and make settings related to security, network printing, and email transmission.

With the embedded server, the administrator can check paper, toner usage status, and the optional equipment. The embedded server also configures device settings, monitors jobs, and manages document boxes and address books in the same manner as using the machine operation panel.

System Requirements

The embedded server operates in the following environment. Check the following before use.

Protocol

- The TCP/IP protocol is configured in the computer.
- An IP address is assigned to the machine.

Web browser

- Microsoft Edge
- Mozilla Firefox 14 or later
- Safari 5 or later
- Google Chrome 21

Operating systems

- Windows 11
- Windows 10
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- macOS 13 Ventura
- macOS 12 Monterey
- macOS 11 Big Sur
- macOS 10.15 Catalina
- macOS 10.14 Mojave
- macOS 10.13 High Sierra
- macOS 10.12 Sierra

- OS X 10.11 El Capitan
- OS X 10.10 Yosemite
- OS X 10.9 Mavericks

Accessing the Embedded Server

Access the embedded server when you enter the host name or IP address of the machine in a web browser. Obtain the IP address from your network administrator. This example uses Microsoft Edge.

Do not access to other websites for security reasons while operating the Command Center RX.

1 Open a web browser.

2 Enter the host name or IP address of the device as the URL.

If you use the host name, you must first specify the DNS server information. For example, `https://192.168.10.1`.

If the screen *"There is a problem with this website's security certificate."* is displayed, configure the certificate. For details, see *Certificates*. You can also continue the operation without configuring the certificate.

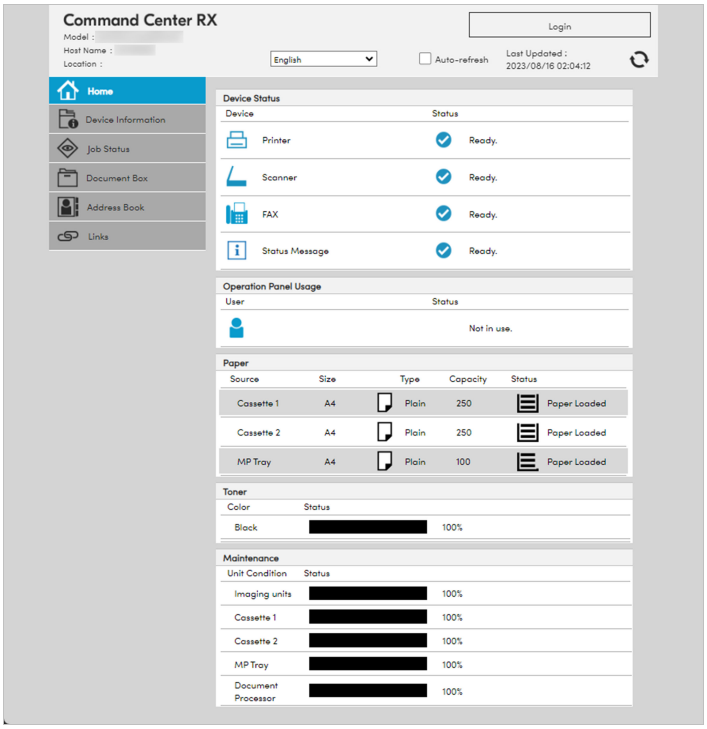
The embedded server's home page will be displayed.

Select **Login** or **Admin Login** in the upper right corner of the screen, then the Admin Login screen appears. Enter the user name and password, and then select **Login**.

At initial log in, enter the user name and password to access all the pages. For the user name and password, refer to the machine's *Operation Guide*.

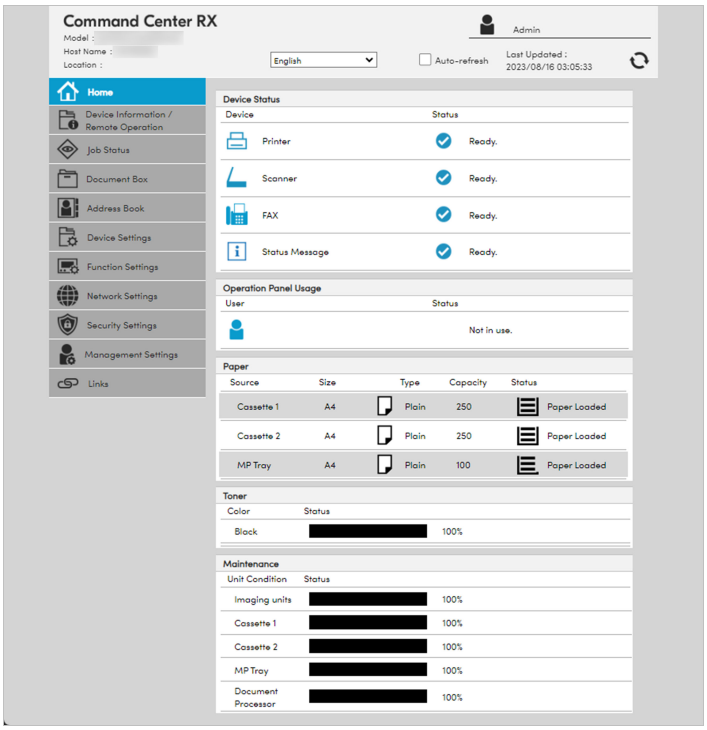
2 The Embedded Server Home Page

The embedded server home page allows you to select and set values for the category from the navigation menu on the left. You can also view information about the device, user, and supplies on the right, which changes according to the features selected in the navigation menu.



Login

To fully access the features of the embedded server pages, enter the user name and password to log in. By logging in using administrator rights, users can access all pages in the navigation menu including document box, address book, and device settings.



For embedded server access, user can be distinguished by using local authentication, network authentication, or job accounting. For details, see *Login Authentication Type*.

Top Bar

At the top of the home page, you can do the following:

Select language

Select your preferred display language from the drop-down list. If the selected language is different from that of the operation panel, then some characters may not display properly.

The embedded server supports multiple languages.

Auto-refresh

Select the **Auto-refresh** checkbox to automatically update the embedded server page to the most recent status.

If you select the **Auto-refresh** checkbox, the login state continues without the automatic logout.

For safe and secure connection, do not select the **Auto-refresh** checkbox.

Refresh

Click the circular arrow icon to refresh the embedded server page at any time.

Navigation Menu

To access the pages of the following features from the home page, select the navigation menu on the left side.

Device Information / Remote Operation

Shows the various information of the machine. You can access this menu when running Remote Operation. After selecting **Device Information / Remote Operation**, the following information is available:

Configuration

Shows the following device configuration information:

- Basic
- Identification information
- Capability
- Optional equipment installed
- Firmware
- Network parameters
- FAX parameters
- Security parameters

Counter

Shows the number of printed pages and scanned pages. To filter the count of specific printed pages, select an option from the Type drop-down list.

About Command Center RX

Displays the firmware version and the list of supported web browsers of the embedded server.

Remote Operation

Select **Start** button to run Remote Operation.

To run Remote Operation, Enhanced VNC(RFB) over TLS is set to **On** in **Network Settings** > **Protocol** and enter the port number, if necessary. Also, Remote Operation is set to **On** in **Management Settings** > **Remote Operation** and configure the settings, if necessary. For details, refer to *Protocol* and *Remote Operation*.

Job Status

Shows the details of the following:

Items may vary depending on the access level.

- Printing job status and log
- Sending job status and log
- Storing job status and log
- Scheduled jobs

Depending on the access level and the job, you can do any of the following:

- To filter the details, select an option from the Type drop-down list.
- Select Number or Job Name to view job details.
- Select the refresh button.
- If necessary, select **Cancel Job**.

Document Box

Allows you to add, edit, or delete a document box, and delete documents in a document box. Document Box includes Subaddress Box, Polling Box, FAX Memory RX Box, and Job Box Settings. For details, see *Document Box*.

Address Book

Allows you to add, edit, or delete a contact address or an address group. Address Book includes Machine Address Book, External Address Book Settings, and One Touch Key. For details, see *Address Book*.

Device Settings

Allows you to configure the advanced settings of the machine. Device Settings includes Paper/Feed/Output, Original Document, Energy Saver/Timer, Date/Time, and System. For details, see *Device Settings*.

Function Settings

Allows you to configure the advanced settings of the function. Function Settings includes Common/Job Defaults, Printer, E-mail, Scan to Folder, FAX, Send and Forward, Forwarding, and Operation Panel. For details, see *Function Settings*.

Network Settings

Allows you to configure the advanced settings for network. Network Settings includes General, TCP/IP, Protocol, and Wireless LAN. For details, see *Network Settings*.

Security Settings

Allows you to configure the advanced settings for security. Security Settings includes Device Security, Send Security, Network Security, and Certificates. For details, see *Security Settings*.

Management Settings

Allows you to configure the advanced management settings. This includes Job Accounting, Authentication, ID Card, Notification/Report, History Set-

tings, SNMP, Restart/Reset, Remote Services, Application, and Remote Operation. For details, see *Management Settings*.

Links

This page includes links of the company websites. Visit the following websites for more information and downloads.

Download Drivers and Software

For downloading printer drivers and software:

KYOCERA Document Solutions - Download

https://www.kyoceradocumentsolutions.com/download/

About KYOCERA Document Solutions

For more information about products:

KYOCERA Document Solutions Website

https://www.kyoceradocumentsolutions.com/

HyPAS Applications

The link information is displayed when the HyPAS applications are installed and configured.

Home

The home page displays information, such as device status, supplies, and operation panel usage. To return to the home page, select **Home**.

Device Status

Shows the operating status of the Printer, Scanner, or FAX.

Operation Panel Usage

Shows the user currently logged in to the device from the operation panel and its operating status.

Settings made using the operation panel may override those made using the embedded server.

Paper

Shows the size, type, maximum capacity, and the remaining quantity of paper source.

Toner

Shows the toner level and the waste toner box status.

Maintenance

Shows the usable state of each maintenance kit.

3 About Login

This section provides information to help the administrator manage domain and local users. The administrator can set embedded server access limit for a user and set a password depending on the authentication function.

For configuration, you need a user name and a password. For the user name and password, refer to the machine's *Operation Guide*.

Login Authentication Type

An administrator can configure the device to require a user login before it is accessed, in either of three different ways of authentication as described in this section.

If you select **Local Authentication** or **Network Authentication**, User Login must be enabled.

Local Authentication

Users are registered in the device and one-to-one authentication is done between a machine and a computer. If a local account user will access the embedded server, enter the user name and password, then select **Login**.

When a drop-down list shows, select **Local**.

If logged in with administrator rights, user can access User Properties, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings, Security Settings, Management Settings, and Links in the navigation menu.

If logged in with a general user account, user cannot add or delete document boxes, nor view the Address Book, Device Settings, Function Settings, Network Settings, Security Settings, and Management Settings.

For the local authenticated method of a user, see *Authentication*.

Network Authentication

When configuring the network authentication, the machine should be under the management of a Windows domain network. Select the domain from the drop-down list, enter the user name and password, and then select **Login**.

If logged in with administrator rights, user can access User Properties, Device Information / Remote Operation, Job Status, Document Box, Address Book, Device Settings, Function Settings, Network Settings, Security Settings, Management Settings, and Links in the navigation menu.

If logged in with a general user account, user cannot add or delete document boxes, nor view the Address Book, Device Settings, Function Settings, Network Settings, Security Settings, and Management Settings.

For the network authentication method of a user, see *Authentication*.

Job Accounting Authentication

If the Authentication Setting is Off and the Job Accounting is On, Account Login and Admin Login shows when you enter the job account ID. Enter the job account ID in Account Login and select **Login**. For details, see *Local Job Accounting List* and *Local User List*.

If a user is registered as an Administrator in the Local User List, select **Admin Login**. Enter the user name and password and select **Login**.

For access using a job account ID, User Properties, Device Information / Remote Operation, Job Status, Document Box, Address Book, and Links are displayed in the navigation menu.

4 Document Box

This page is accessible when you have logged in using a general user or administrator account. It allows you to add or delete a document box or documents in a document box.

A general user is not allowed to add or delete a document box.

These are the types of document boxes, which vary depending on models: Subaddress Box, Polling Box, FAX Memory RX Box, and Job Box Settings.

- Subaddress Box, Polling Box, and FAX Memory RX Box are available only if the device is equipped with a FAX function.
- Users with a general user account can delete the documents that were created and added in their own document boxes.

Subaddress Box

This feature stores received original documents on a machine where the FAX system is installed.

Adding a New Subaddress Box

1. In the navigation menu, select **Document Box** > **Subaddress Box**.
2. Select **Add**.
3. Review or modify the available box properties such as Name, Subaddress, and Permission.
4. Select **Submit**.

Editing a Subaddress Box

1. In the navigation menu, select **Document Box** > **Subaddress Box**.
2. To select a subaddress box, do the following:

   All Boxes and My Boxes are available only when either **Local Authentication** or **Network Authentication** is selected in **Management Settings** > **Authentication**.

   - Select **All Boxes** to view all subaddress boxes for all users.
   - Select **My Boxes** to view the subaddress boxes you created.
   - Search for a specific subaddress box number or name.

3 Select **Box Property**.

4 Review or modify the available box properties such as Name and Subaddress.

5 Select **Submit**.

Working with a Subaddress Box

1 In the navigation menu, select **Document Box** > **Subaddress Box**.

2 To select a subaddress box, do the following:

- If the box is password-protected, enter the correct password.
- All Boxes and My Boxes are available only when either **Local Authentication** or **Network Authentication** is selected in **Management Settings** > **Authentication**.

- Select **All Boxes** to view all subaddress boxes for all users.
- Select **My Boxes** to view the subaddress boxes you created.
- Search for a specific subaddress box number or name.

3 Do any of the following:

When viewing the documents, you can switch between list or thumbnail view.

- To view the details of the document, select the file name. You can then select **Change File Name** or **Preview**. In Preview, you can view the document contents and its properties.
- Select one or more documents, then select **Delete**, **Download**, or **Print**.

Deleting a Subaddress Box

1 In the navigation menu, select **Document Box** > **Subaddress Box**.

2 Select the **Delete** icon.

Selecting the **Delete** icon does not remove any subaddress box yet, but allows you to specify the subaddress boxes you want to remove.

3 In Sub Address Boxes, select the subaddress box you want to delete.

- You can delete only one Sub Address Box at a time.
- All Boxes and My Boxes are available only when either **Local Authentication** or **Network Authentication** is selected in **Management Settings** > **Authentication**.

- Select **All Boxes** to view all subaddress boxes for all users.
- Select **My Boxes** to view the subaddress boxes you created.

- Search for a specific subaddress box number or name.

4 Select the **Delete** icon once.

If necessary, enter the password, and then select **OK**.

Polling Box

This feature allows you to manage documents in polling boxes. You can determine whether documents are automatically deleted or retained after polling.

Polling Box Property

This determines after the document has been sent, whether you want the document to be automatically deleted or to be retained.

1 In the navigation menu, select **Document Box** > **Polling Box**.

2 Select **Box Property**.

3 Do any of the following:

- To configure the box so that the documents are overwritten at updating, set the Overwrite Setting to **Permit**.
- To configure the box so that the documents are automatically deleted after transmission, set the Delete after Transmitted to **On**.

4 Select **Submit**.

Deleting Documents in Polling Box

To delete documents in a polling box, do the following:

1 In the navigation menu, select **Document Box** > **Polling Box**.

2 Do any of the following:

When viewing the documents, you can switch between list or thumbnail view.

- To view the details of the document, select the file name. You can then select **Change File Name** or **Preview**. In Preview, you can view the document contents and its properties.
- Select one or more documents you want to delete.

3 Select the **Delete** icon once.

Printing Documents in Polling Box

To print documents in a polling box, do the following:

1 In the navigation menu, select **Document Box** > **Polling Box**.

2 Do any of the following:

When viewing the documents, you can switch between list or thumbnail view.

- To view the details of the document, select the file name. You can then select **Change File Name** or **Preview**. In Preview, you can view the document contents and its properties.
- Select one or more documents you want to print.

3 Select the **Print** icon.

4 In Selected Files, you can start printing the documents in the order shown.

- If you want to change the order of printing, select a document and click **Top**, **Up**, **Down**, or **Bottom**.
- If you want to remove a document from the list, select the **Delete** icon.

5 Select **Print** once.

FAX Memory RX Box

This feature allows you to receive faxes, check the contents, and print only the faxes that you need.

This feature is available only if you go to **Function Settings** > **FAX** and set FAX Memory RX to **On**.

Deleting Documents in FAX Memory RX Box

To delete documents in a FAX Memory RX Box, do the following:

1 In the navigation menu, select **Document Box** > **FAX Memory RX Box**.

2 Do any of the following:

When viewing the documents, you can switch between list or thumbnail view.

- To view the details of the document, select the file name. You can then select **Change File Name** or **Preview**. In Preview, you can view the document contents and its properties.
- Select one or more documents you want to delete.

3 Select the **Delete** icon once.

Printing Documents in FAX Memory RX Box

To print documents in a FAX Memory RX Box, do the following:

1. In the navigation menu, select **Document Box** > **FAX Memory RX Box**.
2. Do any of the following:

   When viewing the documents, you can switch between list or thumbnail view.

   - To view the details of the document, select the file name. You can then select **Change File Name** or **Preview**. In Preview, you can view the document contents and its properties.
   - Select one or more documents you want to print.
3. Select **Print** icon.
4. In Selected Files, you can start printing the documents in the order shown.

   - If you want to change the order of printing, select a document and click **Top**, **Up**, **Down**, or **Bottom**.
   - If you want to remove a document from the list, select the **Delete** icon.
5. Select **Print**.

Job Box Settings

This feature explains how to change the number of Quick Copy jobs and set automatic delete times for temporary jobs in Job Box. Also, you can determine whether documents are automatically deleted or retained after printing.

1. In the navigation menu, select **Document Box** > **Job Box Settings**.
2. Enter the value from 0 to 300 in Quick Copy Job Retention.
3. In Deletion of Job Retention, do any of the following:
   - To delete automatically the temporary retained jobs after printing, select **1 hour**, **4 hours**, **1 day**, or **1 week** in the drop-down list.
   - If you do not want to delete the jobs after printing, select **Off** in the drop-down list.
4. To delete a PIN print document when the power is turned off, set Deletion of PIN Print at Power Off to **On**.

   Deletion of PIN Print at Power Off is displayed when an SSD is installed in the machine.
5. Select **Submit**.

5 Address Book

This page is accessible when you have logged in using a general user or administrator account.

Address Book contains Machine Address Book and External Address Book Settings. You can also specify the address quickly by assigning it to the One Touch Key.

Machine Address Book

This section explains you to add, edit, or delete contacts in the machine address book.

Contacts

This subsection explains how to add, edit, or delete contacts in the machine address book.

In Machine Address Book, contacts and groups are listed together. Contacts are displayed as single person icon and groups in triple person icon. To filter and display only contacts or groups, select either **Contact** or **Group** from the Type drop-down list.

Adding a New Contact

1. In the navigation menu, select **Address Book** > **Machine Address Book**.
2. Select **Add**.
3. Enter the number, name, and email address of a contact.

   If necessary, you can also enter SMB and FTP access information for the contact including a shared folder accessible from Microsoft Windows Network. To configure the SMB and FTP information, do the following:

   a. Specify the host name, port number, and path to the shared folder, login user name, and login password for the contact.

   b. When you select **Test**, this machine tries to connect to the SMB or FTP server.

   c. If you use the host name, make sure that you have specified DNS server information.

   d. If the FAX system is installed and enabled in the system, you can include a FAX number.

4 Select **Submit**. To cancel, select **Back**.

If S/MIME is set to **On** when registering the email address, you can import the required certificate in Encryption Certificate, Root Certificate (S/MIME), and Intermediate Certificate (1 to 3). Do the following:

a. Select **Import** on the required S/MIME certificate.

b. Select **Open** to specify the Certificate.

c. Select **Submit** and click **OK** to register the certificate.

If a certificate is already registered, you may click **View** to check its details. You may also select **Delete** on a previously imported certificate to replace it with a new one.

Editing a Contact

These steps will help you modify the number, name, email address, SMB and FTP information, and FAX settings of a contact.

1 In the navigation menu, select **Address Book** > **Machine Address Book**.

2 Select the contact's **Number** or **Name** you want to edit.
Search for a specific address number or the address name in the corresponding search box.

3 Modify number, name, or email of the contact.

If S/MIME is set to **On**, do the following:

a. In S/MIME Certificate, select **Settings**.

b. To import the necessary encryption certificate file, select **Import**.

c. If the system installed with a FAX system is enabled, you can modify these settings.

4 Modify the settings for SMB and FTP accesses as necessary. When **Test** is selected, this machine tries to connect to the SMB or FTP server.

- To confirm that the settings are correct, test a connection with the SMB or FTP server, then select **Test**.
- For FTP servers, you can also select **Connection Test (Encrypted TX)** to test a connection.

5 Select **Submit**. To cancel, select **Back**.

Deleting a Contact

1. In the navigation menu, select **Address Book** > **Machine Address Book**.
2. Select the contacts you want to delete by selecting the checkbox to the left.
3. If you want all contacts displayed on the page deleted, select **Check All**. To clear all, select **None**.
4. Select **Delete** once.

Adding a New Group

1. In the navigation menu, select **Address Book** > **Machine Address Book**.
2. Select **Add Group**.
3. In New Group - Property, enter the following:
   - Number of the group

     You can use the automatically-generated number.
   - Name of the group
4. To add contacts to the group, select **Add**.
5. Select the contact to join the group by checking the **Select** checkbox to the left. You can select more than one contacts at once.

   You can only select contacts that are already registered in the Address Book.
6. Select **Submit**. To delete a contact, select a contact and click **Delete**.
7. Select **Submit**. To add more groups, repeat steps 2 to 7.

Edit Group

1. In the navigation menu, select **Address Book** > **Machine Address Book**.
2. Select the group **Number** or **Name** you want to edit.

   Alternatively, you can enter the group number or the group name in the corresponding search box.
3. Modify the group number and name.
4. Add contacts to the group by selecting **Add**.
5. To add a contact to the group, select the corresponding checkbox.

- You can select more than one group at once.
- To filter the contacts, select an option from the Type drop-down list.

6 To add the contacts, select **Submit**. To delete a contact, select a contact and click **Delete**.

7 Select **Submit**.

Delete group

1 In the navigation menu, select **Address Book** > **Machine Address Book**.

2 Do one or more of the following:

a. To filter the contact groups, select **Group** in Type drop-down list.

b. Select the checkbox on the left to delete the groups you want.

c. Select **Check All** if you want all groups deleted. If you want to clear all, select **None**.

Deleting a group does not delete the contacts added to the group.

3 Select **Delete**.

External Address Book Settings

This section explains how to use the external address book.

1 In the navigation menu, select **Address Book** > **External Address Book Settings**.

2 Confirm that LDAP is set to **On**. If the LDAP is Off, configure the settings in **Network Settings** > **Protocol**.

3 Select **On** of the preferred external address book, and then click **Settings**.

External Address Book (5 to 8) is used for sending a fax via FAX server.

4 If prompted, configure the following settings for External Address Book.

External Address Book Name

Enter the external address book name.

LDAP Server

Configure the LDAP server.

LDAP Server Name

Specify a name or an IP address for the LDAP server.

LDAP Port Number

Enter the port number used by LDAP. The default port number is 389.

Search Timeout

Enter your preferred timeout after which a search on the LDAP server expires.

Login User Name

Enter the login name of the user to access the LDAP server.

Login Password

Enter the password to log in the LDAP server.

Max Search Results

Enter the maximum value of the search results when using Search Settings.

Search Base

Enter the basic information of a search.

Entry example of Search Base is as follows.

To search through the "Users" container in the Active Directory "serv.example.com" domain, enter the following:

```
cn=Users,dc=serv,dc=example,dc=com
```

To search through the "Sales div" Organizational Unit (OU) in the Active Directory "serv.example.com" domain, enter the following:

```
ou="Sales div",dc=serv,dc=example,dc=com
```

To search through the user's container "Hanako Yamada" which belongs to "Sales2" Organizational Unit (OU) in the Active Directory "serv.example.com" domain, enter the following:

```
cn="Hanako
Yamada",ou=Sales2,dc=serv,dc=example,dc=com
```

If there are one or more blank spaces in each of value, you have to enclose the value in double quotation marks (").

LDAP Security

Configure this setting in **Network Settings** > **Protocol**.

Authentication Type

Select an authentication type from the drop-down list.

Connection Test

To confirm communication between the machine and LDAP server, select **Test**.

Display Sequence Settings

Select your preferred option from the Display Mode drop-down list.

Search Settings (1 to 2)

You can configure the following settings.

Search Criteria

Enter a display name and an LDAP attribute as search criteria.

Return Value

Enter an LDAP attribute as a return value and select an option from the Job Type drop-down list.

Optional Return Value

Enter a display name and LDAP attribute as an optional return value.

5 If prompted, configure the following settings for External Address Book (FAX Server).

External Address Book Name

Enter the external address book name.

LDAP Server Settings

Configure the LDAP server.

LDAP Server Name

Specify a name or an IP address for the LDAP server.

LDAP Port Number

Enter the port number used by LDAP. The default port number is 389.

Search Timeout

Enter your preferred timeout after which a search on the LDAP server expires.

Login User Name

Enter the login name of the user to access the LDAP server.

Login Password

Enter the password to log in the LDAP server.

Max Search Results

Enter the maximum value of the search results when using Search Settings.

Search Base

Enter the basic information of a search.

Entry example of Search Base is as follows.

To search through the "Users" container in the Active Directory "serv.example.com" domain, enter the following:

```
cn=Users,dc=serv,dc=example,dc=com
```

To search through the "Sales div" Organizational Unit (OU) in the Active Directory "serv.example.com" domain, enter the following:

```
ou="Sales div",dc=serv,dc=example,dc=com
```

To search through the user's container "Hanako Yamada" which belongs to "Sales2" Organizational Unit (OU) in the Active Directory "serv.example.com" domain, enter the following:

```
cn="Hanako
Yamada",ou=Sales2,dc=serv,dc=example,dc=com
```

If there are one or more blank spaces in each of value, you have to enclose the value in double quotation marks (").

LDAP Security

Configure this setting in **Network Settings** > **Protocol**.

Authentication Type

Select an authentication type from the drop-down list.

Connection Test

To confirm communication between the machine and LDAP server, select **Test**.

Display Sequence Settings

Select your preferred option from the Display Mode drop-down list.

Search Settings

You can configure the following settings.

Search Criteria

Enter a display name and an LDAP attribute as search criteria.

Return Value

Enter an LDAP Attribute.

Optional Return Value

Enter a display name and an LDAP attribute as an optional return value.

6 Review the settings and select **Submit**.

One Touch Key

This section explains how to register the address to the One Touch Key.

Registering a new One Touch Key

1 In the navigation menu, select **Address Book** > **One Touch Key**.

2 Select **Settings** of the One Touch Key that you want to register.

3 Select **Address Book** to call a registered address from the address book. To filter and display a type of address, select an option from the Type drop-down list. You can also enter the address name in the corresponding search box.

4 Select either **No.** or **Name** of the address you want to register, and then select **Submit**.

5 Review the address details and select **Back**.

6 Select the contact you want to register. You can assign only one contact in One Touch Key at a time.

7 Review the settings and select **Submit**.

Edit one touch key

1 In the navigation menu, select **Address Book** > **One Touch Key**.

2 Search for a specific key number. You can also enter the key number in the corresponding search box.

3 Make the necessary changes to the display name and destination. To remove a destination, select **Delete**.

4 Review the settings and select **Submit**.

Delete One Touch Key

1 In the navigation menu, select **Address Book** > **One Touch Key**.

2 To remove an assigned One Touch Key, select **Delete**.

6 Device Settings

This page is accessible when you have logged in the embedded server with administrator rights, while network authentication or local authentication is enabled.

If prompted, configure the following settings. See the sections below for detailed information.

- Paper/Feed/Output
- Original Document
- Energy Saver/Timer
- Date/Time
- System

Paper/Feed/Output

This section includes settings that apply to paper size and media type for the paper loaded in the MP tray and the cassettes, configuring cassette group, paper output, and the other detailed properties.

Cassette Settings

1. In the navigation menu, select **Device Settings** > **Paper/Feed/Output**.
2. Configure the paper size and media type for each cassette.
3. Review the settings and select **Submit**.

MP Tray Settings

1. In the navigation menu, select **Device Settings** > **Paper/Feed/Output**.
2. Configure the paper size and media type for MP Tray.
3. Review the settings and select **Submit**.

Group Settings

Group Settings is available only when an optional cassette is installed.

1. In the navigation menu, select **Device Settings** > **Paper/Feed/Output**.
2. Select the cassettes corresponding to your preferred group arrangement.

3 Review the settings and select **Submit**.

Other Settings

1 In the navigation menu, select **Device Settings** > **Paper/Feed/Output**.

2 You can configure the following settings.

Default Paper Source

Select the cassette or MP Tray to feed the paper with priority.

Paper Selection

Select either **Auto** or **Default Paper Source** from the drop-down list.

Auto Paper Selection

Select either **Most Suitable Size** or **Same as Original Size** from the drop-down list.

Special Paper Action

Select either **Adjust Print Direction** or **Speed Priority** from the drop-down list.

Media for Auto (B&W)

You can select the media type when **Auto** is selected in Paper Selection for black and white printing.

Show Paper Setup Message

To display a paper setup message when loading the paper in the paper source, select **On**.

This message will be displayed at the confirmation screen.

3 Review the settings and select **Submit**.

Paper Detail Settings

1 In the navigation menu, select **Device Settings** > **Paper/Feed/Output**.

2 In Paper Detail Settings, select **Settings**.

You can configure the following settings.

Custom Paper Size Settings

Set the paper size for the cassette and MP tray. If necessary, you can enter the length and width of the custom paper.

Media Type Settings

Select the paper weight for each media type from the drop-down list.

If you configure the Custom (1 to 8) setting, you can allow duplex printing and enter your preferred name for the setting. Duplex feature is available only in some machines.

3 Review the settings and select **Submit**.

Original Document

This section explains how to configure the original size of the document.

Auto Detect Original Size

1 In the navigation menu, select **Device Settings** > **Original Document**.

2 You can configure the following settings.

Auto Detect

To use automatic detection, select **On**.

System of Units

To automatically detect the unit of measurement of the original document, select either **Metric** or **Inch**.

If you select **Inch**, you can also specify the original paper size from the drop-down list.

Default Original Size

- If Auto Detect is set to **On**, this setting is displayed as Default Original Size (Platen).
- If Auto Detect is set to **Off**, this setting is displayed as Default Original Size.

If **On** is selected, then specify the default size of the original placed on the platen. Select from the following:

- A4
- A5
- A6
- B5
- B6
- Letter
- 216×340mm
- Statement

- Legal
- Executive
- 16K
- OficioII
- Folio
- ISO B5
- Envelope #10
- Envelope #9
- Envelope #6
- Envelope Monarch
- Envelope DL
- Envelope C5
- Hagaki
- Oufukuhagaki
- Youkei 4
- Youkei 2
- Nagagata 3
- Nagagata 4
- Younaga 3

3 Review the settings and select **Submit**.

Custom Original Size

1 In the navigation menu, select **Device Settings** > **Original Document**.

2 Configure the custom original size. Enter the length and width of the custom paper.

3 Review the settings and select **Submit**.

Energy Saver/Timer

This section explains how to configure the Energy Saver Settings and Timer Settings.

Energy Saver Settings

1 In the navigation menu, select **Device Settings** > **Energy Saver/Timer**.

2 You can configure the following settings:

Sleep Level

When you select a sleep level, the machine can recover from sleep mode when you press any key on the operation panel or, if the machine receives a print or fax job. Select either of the following:

Quick Recovery

The machine recovers from the sleep mode faster compared to the Energy Saver mode.

Energy Saver

The machine reduces power consumption compared to the Quick Recovery mode, allows sleep mode to be set separately for each function, and takes longer time for the machine to wake up from the sleep mode and resume normal operation.

The Sleeping page appears on the embedded server while the system is in Energy Saver mode. You can select **Start** on the Sleeping page.

Sleep Rule

This feature is available only if you select **Energy Saver** as a sleep level. You can also set Card Reader and Application to **On**.

Card Reader is available only when a Card Authentication kit is enabled.

Sleep Timer

Specify the time period for the system to enter Auto Sleep Mode.

Power Off Timer

Specify the time after which the system enters power off mode, where the device automatically turns off after a certain amount of time elapses that the device is idle.

Power Off Rule

Select **On** for the corresponding interface or application you want to set in power off mode.

Energy Saver Recovery Level

In Energy Saver Recovery Level, select any of the following:

- **Full Recovery**
- **Normal Recovery**
- **Power Saving Recovery**

3 Review the settings and select **Submit**.

Timer Settings

1 In the navigation menu, select **Device Settings** > **Energy Saver/Timer**.

2 Do any of the following settings:

Auto Panel Reset

This setting allows you to automatically reset the panel. Enable this setting to open Panel Reset Timer and specify the time between 5 and 495 seconds.

WSD Scan Timer

When enabled, this setting determines the time period before the machine reverts to normal mode. The range is 10 to 495 seconds.

3 Review the settings and select **Submit**.

Date/Time

This section includes advanced settings on date and time.

Date/Time

1 In the navigation menu, select **Device Settings** > **Date/Time**.

The following items are displayed:

Current Local Time

Displays the time that is currently set in the machine.

Current Universal Time (UTC/GMT)

Displays the Greenwich Mean Time that is currently set in the machine.

2 If necessary, specify the following:

- **Date**
- **Time**
- **Date Format**
- **Time Zone**
- **Summer Time/Daylight Saving Time**

This setting is available only if certain time zones are selected.

3 Review the settings and select **Submit**.

Synchronization

1 In the navigation menu, select **Device Settings** > **Date/Time**.

2 If necessary, enter the host name or IP address of the time server, and select **Submit**.

If you use the host name, make sure to specify the DNS server information.

3 Select **Synchronize**.

Time information is required when you receive reports from this machine via email. It is recommended that you set the time when the report mail function is enabled.

4 Select **Submit**

System

This section includes advanced settings that apply to the system.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the machine or the network. To restart the machine, go to **Management Settings** > **Restart/Reset**.

Device Information

1 In the navigation menu, select **Device Settings** > **System**.

2 If necessary, enter the host name, asset number, and location.

If you use the host name, make sure to specify the DNS server information.

3 Select **Submit**.

General

1 In the navigation menu, select **Device Settings** > **System**.

2 If necessary, modify the following settings:

Language
Select the language.

RAM Disk Mode
When you use RAM disk mode, select **On**.

RAM Disk Size
Set the RAM disk size.

This feature is available only if an optional RAM disk is installed.

Software Keyboard Layout
Select an appropriate type of keyboard layout.

USB Keyboard Type

Select an appropriate type of USB keyboard.

Keyboard Language

Select either **English** or **Follow Displayed Language** as of USB keyboard language.

Override A4/Letter

Specify whether you want to interchange A4 and Letter paper size during printing.

- When set to **On**, for example, if A4 is not in the tray, Letter is selected for printing.
- When set to **Off**, Letter is not used for printing documents in place of A4 even if the A4 tray is empty.

Measurement

Select the unit of measurement for entry.

Preset Limit

Specify the number of copies limited to print.

Default Screen

To set a default screen, select from the drop-down list.

Default Screen (Send/FAX)

To set a default screen for Send/FAX, select from the drop-down list.

- For printers without fax function installed, this setting is displayed as Default Screen (Send).
- This setting is available only if an External Address Book (FAX Server) is set to **On**.

Default Address Book

Select either **Machine Address Book** or your preferred external address book as the default address book.

For information on how to set the machine address book, refer to *Machine Address Book*.

For information on how to set the external address book, refer to *External Address Book Settings*.

Destination History Usage

To enable destination history usage, select **Permit**.

Reset Destination History

To reset the destination history, select **Reset**.

Altitude Adjustment

Select an altitude from the drop-down list according to your operating environment.

Device Managed by Administrator

Select whether the administrator manages the device.

Bluetooth

Select whether to use the Bluetooth keyboard.

This setting is available only when a Bluetooth USB adapter is installed.

Clear Set. after Job Started

Set whether to clear the function settings to the default after finishing a job.

Card Position on Platen

To set the card position on the platen, select either **Free** or **Upper Left**.

Layout for ID Card Copy

To set the alignment of the layout for ID card copy, select either **Align Upper Right** or **Align Center**.

Time for Maintenance Alert

Do either of the following:

Notify via Operation Panel

Select either **Display Status** or **Display Status and Error** to notify the user for periodic inspection in the operation panel.

Notify Externally (for administration use)

To notify the administrator, select **On**. Once enabled, the notification timing is set within a time period until the periodic inspection. The setting range is 5% to 100%.

3 Select **Submit**.

Error Settings

1 In the navigation menu, select **Device Settings** > **System**.

2 If necessary, modify the following settings:

MP Tray Empty

To enable the alert when the MP tray is empty, select **On**.

Auto Error Clear

To automatically clear errors, select **On**. If enabled, printing resumes after the specified time period. You can enter a value from 5 to 495 seconds.

Low Toner Alert

Set the level of remaining toner to notify the administrator when to order a toner when the toner is running low. This notification is used for event report, status monitor, and SNMP trap.

If you select **Off**, the administrator is notified when the toner level is at 5%.

If you select **On**, set the level of remaining toner that triggers the low toner alert to the administrator. The setting range is 5% to 100%.

Continue or Cancel Err. job

Select either **All Users** or **Job Owner Only** as the target users who can cancel or continue operations on jobs paused due to error.

Administrator can cancel all jobs regardless of this setting.

3 Select **Submit**.

7 Function Settings

This page is accessible when you have logged in the embedded server with administrator rights, while network authentication or local authentication is enabled. If needed, make the following settings:

- Common/Job Defaults
- Printer
- E-mail
- Scan to Folder
- FAX
- Send and Forward
- Forwarding
- Operation Panel
- Cloud Access

Common/Job Defaults

In this section, you can make settings for the following items:

Common Settings

1. In the navigation menu, select **Function Settings** > **Common/Job Defaults**.
2. To enable automatic zooming with priority, set Auto % Priority to **On**.
3. Select **Submit**.

Job Default Settings

1. In the navigation menu, select **Function Settings** > **Common/Job Defaults**.
2. If necessary, modify the following settings:

File Name

Enter the default name for the document used in the print job.

Additional Information

In Additional Information, select from the following:

- **None**
- **Date and Time**

- **Job No.**
- **Job No. + Date and Time**
- **Date and Time + Job No.**

3 Select **Submit**.

Scan Default Settings

1 In the navigation menu, select **Function Settings** > **Common/Job Defaults**.

2 If necessary, modify the following settings:

Original Orientation

Select either **Top Edge on Top** or **Top Edge on Left** as the original orientation.

Color Selection (Send/Store)

Select the color mode for scanning or storing.

- **Auto Color(Color/Grayscale)**
- **Auto Color(Color/B & W)**
- **Full Color**
- **Grayscale**
- **Black & White**

- Auto Color(Color/Grayscale) and Auto Color(Color/B & W) allow you to identify color for the original document to scan.
- You can manually select Black & White to forcibly switch color mode.

Scan Resolution

Specify the resolution for scanning.

- The resolutions available differ depending on the model, current color mode, and the saving format of files.
- To scan in full color or grayscale with a solution of 400 dpi or greater, the internal memory must be expanded for some models.

Original Image (Copy)

The original quality for copying must be selected according to the type of the original. Select from the following:

- **Text+Photo**
- **Photo**
- **Text**
- **Graphic/Map**

Original Image (Send/Store)

The original quality for scanning or storing must be selected according to the type of the original. Select from the following:

- **Text+Photo**
- **Photo**
- **Text**
- **Light Text/Fine Line**

Zoom

This switches the zoom ratio between Auto and 100%. The default setting is 100%.

Background Density (Copy)

This removes dark background from originals, such as newspapers, when copying.

Background Density (Send/Store)

This removes dark background from originals, such as newspapers, when sending or storing a job.

Continuous Scan (Copy)

To enable continuous scan for copy, select **On**.

Continuous Scan (Send/Store)

To enable continuous scan for send or store, select **On**.

Some printers display Continuous Scan (Except FAX). Activates or deactivates Continuous Scan except fax.

Continuous Scan (FAX)

To enable continuous scan for fax, select **On**.

Border Erase (Copy)

Select the type of border erase for copying from the drop-down list.

In Border Erase, set the width of the outer and inner borders to erase in 0 to 50mm. You can also set border erase for the reverse side.

Border Erase/Full Scan (Send/Store)

Select the type of border erase from the drop-down list when sending or storing. You can also select **Full Scan** which scans all area of original as image.

In Border Erase, set the width of the outer and inner borders to erase in 0 to 50mm. You can also set border erase for the reverse side.

Border Erase/Full Scan (FAX)

Select the type of border erase from the drop-down menu when sending fax. You can also select **Full Scan** which scans all area of original as image.

In Border Erase, set the width of the outer and inner borders to erase in 0 to 50mm. You can also set border erase for the reverse side.

Prevent Bleed-through (Copy)

To enable Prevent Bleed-through for copying, select **On**.

Prevent Bleed-through (Send/Store)

To enable Prevent Bleed-through for sending and storing, select **On**.

Skip Blank Page (Copy)

To enable Skip Blank Page for copying, select **On**.

Skip Blank Page (Send/Store)

To enable Skip Blank Page for sending and storing, select **On**.

Detect Folded Corner Originals

Select whether to detect an original with bent corners when reading an original from the document processor.

Detect Non-standard Size (Copy)

Select whether to detect a size outside the standard sizes during copying.

Detect Non-standard Size (Send/Store)

Select whether to detect a size outside the standard sizes during sending or storing.

Clarify Text (Noise Removal)

Set the default state of Clarify Text (noise removal).

Clarify Text Level

Set the text reproduction level from the drop-down list.

Noise Removal

Set noise removal from the drop-down list.

Original Type (Copy)

Select original types when copying. You can also select the binding direction when copying 2-sided documents.

Original Type (Send/Store)

Select original types when sending or storing. You can also select the binding direction when sending or storing 2-sided documents.

3 Select **Submit**.

Output Default Settings

1 In the navigation menu, select **Function Settings** > **Common/Job Defaults**.

2 If necessary, modify the following settings:

EcoPrint

To control toner consumption for saving the printing costs, set Eco-Print to **On**. The default setting is Off. If this setting is set to **On**, you can select **Toner Save Level** from 1 (Low) to 5 (High), according to the machine.

JPEG/TIFF Print

This determines the physical size of JPEG images when printing them from a USB drive. Select from the following:

- **Fit to Paper Size**
- **Image Resolution**
- **Fit to Print Resolution**

XPS Fit to Page

This determines the page size for printing XPS data. To fit print data over the page size, set XPS Fit to Page to **On**. To print in the original size, set to **Off**.

Print Mode

To set how many sides of copy are in the output, select either **1-sided** or **2-sided** as print mode.

Collate

Select the default collate settings.

FAX TX Resolution

This selects the document resolution when sending a document through fax.

E-mail Template

Create a template for emails sent from this machine.

3 Select **Submit**.

Copy Default Settings

1 In the navigation menu, select **Function Settings** > **Common/Job Defaults**.

2 In DP Read Action, you can select either faster scanning or better quality scanning when using the document processor.

3 Select **Submit**.

File Default Settings

1 In the navigation menu, select **Function Settings** > **Common/Job Defaults**.

2 If necessary, review and modify the following settings:

File Format

In File Format, select from the following:

- **PDF**
- **TIFF**
- **JPEG**
- **XPS**
- **High Compression PDF**
- **Open XPS**

Image Quality

This determines the quality of the image when saved, from 1 Low Quality (High Comp.) to 5 High Quality (Low Comp.).

PDF/A

PDF/A is an electronic file format for long-term preservation of documents as addressed in the ISO 19005-1 specification. Set the PDF/A-compliant format of the document. Select from the following:

- **PDF/A-1a**
- **PDF/A-1b**
- **PDF/A-2a**
- **PDF/A-2b**
- **PDF/A-2u**
- **Off**

Color TIFF Compression

Select either **TIFF V6** or **TTN2** format for compression of color TIFF images.

File Separation

To extract pages as separate files from an output file, set File Separation to **On**.

Digital Signature

In Digital Signature, select from the following:

- **Off**

- **Specify Each Job**
- **On**

Signing Certificate

a. In Signing Certificate, select **Settings**.

b. Select a certificate from the list.

c. Select **Submit**.

Configure the certificate setting in **Security Settings** > **Certificates**.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **KeyUsage**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Revocation Check Type

In Revocation Check Type, select either of the following as your revocation digital certificate.

- **OCSP**
- **CRL**
- **CRL & OCSP**

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

Password Confirmation on Signature Permission

Enable password confirmation then set up a password to use when selecting the digital signature.

This feature is available only if you select **Specify Each Job** in Digital Signature.

Password

Enter the password to confirm the digital signature.

3 Select **Submit**.

Printer

This section includes advanced settings for printing.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the machine or the network. To restart the machine, go to **Management Settings** > **Restart/Reset**.

General

1. In the navigation menu, select **Function Settings** > **Printer**.
2. If necessary, review and modify the following settings:

Emulation

Set the Emulation Mode.

- **PCL6**
- **KPDL**
- **KPDL(Auto)**

Alternate Emulation appears when **KPDL(Auto)** is selected from Emulation.

Paper Feed Mode

Determines the behavior of paper feed selection when the paper you requested of size or type is not available in the current paper source. To let the machine search for the matching paper in all the paper sources, select **Auto**. The machine does not search in the other paper sources when **Fixed** is selected.

Form Feed Timeout

Adjusts the form feed timeout between 5 and 495 seconds in 5-second increments. A form feed will occur in the absence of data during this time period.

Job Name

In Job Name, select from the following:

- **Job Name**
- **Job No. & Job Name**
- **Job Name & Job No.**
- **Off**

User Name

To display the user name associated to the print job, select **On**.

Wide A4

To enable Wide A4 size during printing, select **On**.

Auto Cassette Change

You can select the action of the machine when the paper runs out in the paper source while printing.

When selecting **Off**, the machine displays message to load paper in the paper cassette and stops printing. Load the paper according to the paper source displayed to resume printing. You can also select your preferred paper source.

When selecting **On**, the machine continues printing automatically if the other paper cassette contains the same paper as the currently used paper cassette.

Printing Job Terminator

You can select the condition which determines a job termination if the print job could not be finished due to your environment or other reasons.

EOJ (End of Job)

The termination of the job data (`!R!RES;EXIT;`) is regarded as one job until it is detected.

End of Network Session

The data included in a network session at a network connection is considered as one job.

UEL (Universal Exit Language)

The UEL included in the termination of the job data is regarded as one job until it is detected.

Remote Printing

To enable remote printing, select **Permit**.

Direct Printing from Web

When you run direct printing from Command Center RX, select **Allowed**.

3 Select **Submit**.

Running Direct Printing from Command Center RX

To run direct printing from Command Center RX, do the following:

To run direct printing from Command Center RX, go to **Function Settings** > **Printer** and select **Allowed**.

1 Start up the browser.

2 Enter `https://` and host name of the machine to start up the Command Center RX.

3 Select **Home** to display the home page.

4 In Device Status, select **Direct Printing** next to the Printer icon.

5 In Direct Printing File, select the document to print.

6 Configure the job settings.

a. In Paper Selection, select an option if you want to change the paper source.

b. Select the number of copies to print in Copies.

c. Select **1-sided**, **2-sided(Bind Long Edge)**, or **2-sided(Bind Short Edge)** as duplex mode.

These features are available only in some machines.

d. To control toner consumption for saving the printing costs, set EcoPrint **On**.

e. If the PDF is encrypted, enter the password in Encrypted PDF Password.

f. Specify the page size for printing XPS data. To fit the print data over the page size, set to **On**. To print in the original size, set to **Off**.

g. Set Collate to either **On** or **Off**.

7 Select **Print**. The selected file will be printed without a printer driver.

AirPrint Settings

1 In the navigation menu, select **Function Settings** > **Printer**.

2 Select **Settings**.

If necessary, modify the following settings:

AirPrint

The default setting is On.

Bonjour Name

Enter the Bonjour name.

Location

Enter the location of the machine on Location in **Device Settings** > **System**.

When you enter Location, the location appears under the printing device name appears on the printer selection screen using the mobile device. The location also appears on the title of Command Center RX.

Geolocation

Specifies whether to set the geolocation information of the machine. If this setting is **On**, you can configure the latitude, longitude, and altitude of the machine location.

Even if Geolocation is set to **Off**, AirPrint works properly.

Latitude

Enter the latitude of the machine location.

Longitude

Enter the longitude of the machine location.

Altitude

Enter the altitude of the machine location.

Universal Print Settings

Universal Print is a service that allows users to share printers via the cloud. You can use the printer shared in advance from LAN or an external network. You can send a print job to a shared printer via Universal Print.

To use Universal Print, the following conditions are required.

- The license of Universal Printer has been granted.
- All administrators have Printer Administrator or Global Administrator rights.
- Microsoft Authenticator is installed on your mobile device.

Preparation before setting

1. In the navigation menu, go to **Network Settings** > **Protocol**.
2. In Other Protocols, go to Universal Print Settings and do either of the following:
   - To confirm Certificate Auto Verification and Hash, set Use Default Settings to **Off**.
   - To retain the configuration, set Use Default Settings to **On**.
3. Select **Submit**.
4. In the navigation menu, go to **Function Settings** > **Printer**.
5. In Universal Print Settings, select **Settings**.
6. Configure the following settings:

Printer Name

Displays the device name. You can modify the name as necessary.

Proxy

Select **Settings**.

If you do not use a proxy server, set Proxy to **Off**.

If you configure the proxy, set Proxy to **On**, and specify the following items as necessary. For details, see *Proxy settings*.

After configuring settings, return to the Universal Print Settings page.

Proxy Authentication

Enter the user name and password for proxy authentication.

Registering a printer with Universal Print

The operation from registering the printer to adding it to the computer should be completed within 15 minutes.

1. Launch the Microsoft Authenticator installed on your mobile device.
2. You can configure settings for Universal Print. Select **Register**.
3. Select the URL. Enter an access code and select **Next**.

   If you do not install the Microsoft Authenticator yet, follow the on-screen instructions to install it on your mobile device.

4. Log in using your Azure administrator account name and password.

   Permission is required only when registering for the first time.

5. Select **Accept** for the accept request from Microsoft Authenticator.
6. Close the Microsoft web page and return to the Command Center RX.
7. Select **OK**.

   When pressing the **OK** button, the Register button on the Universal Print Setting page changes to the Unregister button, and the Certificate Expiration is displayed. If it is not displayed, click the refresh button.

8. Select **Edit** in Universal Print Preferences and drag and copy the Unregistration URL.
9. Open the new tab on the browser and paste the copied URL.
10. Select **Printers**. The printer list is displayed.
11. Select the name of the printer you want to share and select **Share**.
12. Select the users with whom you want to share the printer and select **Share Printer**.

    Set Allow access to everyone in my organization to **On** to all users in your organization to share the printer.

13 Close the Universal Print web page.

Adding a printer to your computer

To add a shared printer using a proxy network connection, do the following:

If you are not using a proxy network connection, then proceed to step 3.

1 Start the command prompt as an administrator.

2 Enter the following command on the command line.

```
netsh winhttp set proxy proxy-server="<Proxy server
IP>:<Port number>" bypasslist="
```

For example, if the Proxy server IP is 10.184.212.160, the port number is 8080, and the bypass list is * .local, enter the following:

```
netsh winhttp set proxy proxy-
server="10.184.212.160:8080" bypass-list="*.local"
```

3 Select the **Window** icon, and then click **Settings** icon.

4 Select the **Accounts** icon.

5 Select **Access Work or School**.

6 Confirm that the Azure administrator account name appears in the work or school account.

If you do not see your Azure administrator account name, select **Connect** and log in using your Azure administrator account name and password.

7 Return to the Windows settings screen and select the **Devices** icon.

8 Select **Printers & scanners**.

9 To search for the printer and scanner, select the **Add Device** icon.

10 Select the shared printer (Cloud printer) from the list and click **Add device**. The shared printer is added to your computer.

Unregistering shared printer

Follow the steps to unregister a shared printer.

1 In the navigation menu, go to **Function Settings** > **Printer**.

2 In Universal Print Settings, select **Settings**.

3 Select **Unregister**.

4 Select the URL.

5 Select the **Printer Shares** icon.

6 Select the printer name you do not want to share, then click **Remove** > **OK**.

7 Select the **Printers** icon.

8 Select the printer name you want to unregister and click **Unregister** > **OK**.

9 Close the web page and return to the Command Center RX.

If successfully unregistered, the Unregister button on the Universal Print settings page will change to Register button. If it is not displayed, select the refresh icon.

Network Authentication

Network Authentication is available only when **Network Authentication** is selected in **Management Settings** > **Authentication**.

1 In the navigation menu, go to **Function Settings** > **Printer**.

2 In Universal Print Settings, select **Settings**.

3 In Network Authentication, select **Enable**.

4 Select the URL to open the Microsoft web page in a new tab.

5 Enter the code shown in Command Center RX, then select **Next**.

6 Log in using your Azure administrator account name and password.

7 Select **Continue**.

8 Close the Microsoft web page and return to the Command Center RX.

9 Select **OK**, and then close the embedded server.

- If authentication is successful, then the status of Universal Print Network Authentication is displayed as On.
- If authentication fails, then the status of Universal Print Network Authentication remains Off and displays an error status message.

Page Control Settings

1 In the navigation menu, go to **Function Settings** > **Printer**.

2 You can make changes for the following items as required.

Duplex

Select **1-sided**, **2-sided(Bind Long Edge)**, or **2-sided(Bind Short Edge)** as duplex mode.

This feature is available only in some machines.

Copies

Select the number of copies to print.

Page Orientation

Switches **Portrait** or **Landscape** page orientation.

LF Action

Sets line feed (LF) and carriage return (CR).

CR Action

Sets line feed (LF) and carriage return (CR).

3 Select **Submit**.

Print Quality Settings

1 In the navigation menu, go to **Function Settings** > **Printer**.

2 You can make changes for the following items as required.

KIR

To enable KIR smoothing, set to **On**.

EcoPrint

To control toner consumption for saving the printing costs, set Eco-Print **On**. The default setting is Off. If the setting is On, you can select Toner Save Level from 1 (Low) to 5 (High) according to the machine.

Resolution

Select the preferred resolution from the drop-down list.

3 Select **Submit**.

E-mail

This section includes advanced settings for email.

SMTP

1 In the navigation menu, go to **Function Settings** > **E-mail**.

2 You can make changes for the following items as required.

SMTP Protocol

Displays whether an SMTP connection is available or not. Configure SMTP in SMTP (E-mail TX) in **Network Settings** > **Protocol**.

SMTP Server Name

Enter the SMTP Server Name or its IP address.

If you entered the SMTP server name, instead of the IP address, a DNS server address must also be configured. To configure the DNS server address, go to **Network Settings** > **TCP/IP**.

SMTP Port Number

Enter the port number that SMTP will use. The default is 25. Normally, use port 25, but you can change the port number to match the email server's application and operation. For example, the default port number for SMTP connections over TLS is 465. The default port number for SMTP authentication is 587.

SMTP Server Timeout

Sets the timeout in seconds during which this device tries to connect to the SMTP server.

Authentication Protocol

In Authentication Protocol, set your preferred authentication type.

On

This option enables authentication protocol.

a. Select **On**.

b. In Authentication as, select either **POP before SMTP (FAX Server)** or **Other**.

POP before SMTP

This is an authentication mode that allows you to send an email from any location and also fetch your email from the same place.

a. Select **POP before SMTP**.

b. In Authentication as, select **POP before SMTP (FAX Server)**.

c. In POP before SMTP Timeout, enter your preferred timeout during which this device tries to connect to the POP3 server.

This setting is enabled when **POP before SMTP** is selected as the authentication protocol.

Off

Select this option to disable authentication protocol.

OAuth2

To set up OAuth2 for Microsoft 365, make sure to do the following:

a. Log in as an Administrator.

b. In the navigation menu, go to **Network Settings** > **Protocol** and set the following:

1. In Send Protocols, set SMTP (E-mail TX) to **On**.

2. In SMTP Security, select **STARTTLS**.

3. Select **Submit**.

In the navigation menu, go to **Function Settings** > **E-mail** > **SMTP** > **Authentication Protocol**, then select this option to enable OAuth2.0 as an authentication protocol. After selecting **OAuth2**, do the following:

a. To save the settings, select **Submit**.

b. In OAuth2 Status, select **Authorize**.

c. In Microsoft Exchange Server Authorization, copy the code, and then select the URL.

d. Paste the code and select **Next**.

e. In Microsoft 365, do either of the following:

- Select a saved account.
- Select **Use another account** and enter the necessary information.

For Exchange Online accounts with two-factor authentication (2FA) enabled, make sure to have access to your preferred authentication app. Log in to your Exchange Online account, and then follow the instructions to complete 2FA. For more information, contact your Exchange Online server administrator.

f. Enter the multi-factor authentication (MFA) code.

g. To confirm the account selected for signing in, select **Consent on behalf of your organization** > **Accept**.

h. Once the permission request has been approved, select **Continue**.

i. Close the Exchange Online Client for Device window.

j. In Command Center RX, go back to Microsoft Exchange Server Authorization, then select the refresh icon to check the Authorization Status.

k. Once authorization is complete, select **OK** > **Submit**, and then check the OAuth2 Status.

l. To save the settings, select **Submit**.

Proxy Authentication for OAuth2

For added security in OAuth2 Authentication, before selecting **Authorize** in OAuth2 Status, you can set up OAuth2 with Proxy Authentication by doing the following:

a. Go to **Network Settings** > **TCP/IP** and in Proxy Settings, set Proxy to **On**.

b. In Proxy Server (HTTP), enter the required IP address and port number.
   - The IP address and port number may vary depending on the proxy server configuration.
   - If you set Use the Same Proxy Server for All Protocols to **On**, the same IP address and port number is used for Proxy Server (HTTPS).

c. Select **Submit** > **OK**.

After successfully setting up Proxy Settings, you can proceed with the OAuth2 authentication.

In the navigation menu, go to **Function Settings** > **E-mail** > **SMTP**. When **OAuth2** is selected in Authentication Protocol, do the following:

When Authentication Protocol is set to **OAuth2**, you do not have to enter the login user name and password since the credentials used for OAuth2 authentication are the same.

a. In Proxy Authentication for OAuth2, enter the user name and password.

b. In OAuth2 Status, check whether you have access. You can do either of the following:
   - Select **Authorize** to enable access to OAuth2.
   - Select **Unauthorize** to revoke access to OAuth2.

c. Select **Submit** > **OK**.

SMTP Security

The name of the item that is set will be displayed if SMTP Security is enabled. It is enabled only when either **TLS** or **STARTTLS** is selected. If you select **OAuth2** as an authentication protocol, select **STARTTLS**. Configure the settings in the **Network Settings** > **Protocol**.

POP before SMTP Timeout

Set the timeout in seconds during which this device tries to connect to the POP3 server. You can configure this item when you select **POP before SMTP** as Authentication Protocol.

Connection Test

To confirm that the settings are correct, select **Test** for the machine to try to connect to the SMTP server.

Domain Restriction

If necessary, activate whether configured domain names in the Domain List are permitted or restricted domains.

This setting is enabled when a domain name is listed in the SMTP Domain Restriction List. To configure a domain name, do the following:

a. Select **Domain List**.

b. Enter a domain name that is either permitted or rejected. You can also specify email addresses.

c. Select **Submit** > **Back**.

3 Select **Submit**.

POP3

1 In the navigation menu, go to **Function Settings** > **E-mail**.

2 You can make changes for the following items as required.

POP3 Protocol

Displays whether a POP3 connection is available or not.

- Set POP3 (Email RX) to **On** in **Network Settings** > **Protocol**.
- If Remote Printing is prohibited, email printing is disabled. Configure Remote Printing in **Function Settings** > **Printer**.

Check Interval

Set the check interval for connecting to the POP3 server to check for incoming emails. The default is 15 minutes.

Run once now

To immediately receive email from the POP3 server, select **Receive**.

If Remote Printing is allowed, the machine prints the received email.

Domain Restriction

If necessary, activate whether configured domain names in the Domain List are permitted or restricted domains.

This setting is enabled when a domain name is listed in the POP3 Domain Restriction List. To configure a domain name, do the following:

a. Select **Domain List**.

b. Enter a domain name that is either permitted or rejected. You can also specify email addresses.

c. Select **Submit** > **Back**.

POP3 User Settings

To configure the following user settings, select **Settings**. Up to three users can be set.

User Profile (1 to 3)

Enables or disables the user.

E-mail Address

Enter the email address.

POP3 Server Name

Enter the POP3 server host name or IP address.

If you entered the host name, make sure that the DNS server information is specified.

POP3 Port Number

Enter the port number. The default port number is 110.

POP3 Server Timeout

Enter your preferred timeout during which this device tries to connect to the POP3 server.

Login User Name

Enter the login user name of your POP3 account.

Login Password

Enter the login password of your POP3 account.

Use APOP

If necessary, set Use APOP to **On**.

- APOP is an encryption mechanism used for encrypting the Login Password during communication with the POP3 server.
- When enabled, the login password is encrypted.
- When disabled, the login password is sent using plain ASCII text.
- To use this feature, the POP3 server must support and enable configuration for APOP.

Authentication

To set up OAuth2 for Microsoft 365, make sure to do the following:

a. Log in as an Administrator.

b. In the navigation menu, go to **Network Settings** > **Protocol** and set the following:

1. In Print Protocols, set POP3 (E-mail RX) to **On**.

2. In POP3 Security (User 1 to 3), select **TLS**.

3. Select **Submit**.

In the navigation menu, go to **Function Settings** > **E-mail** > **POP3**, then in POP3 User Settings, select **Settings**. In User (1 to 3), select either **Basic** or **OAuth2** as an authentication. For **OAuth2**, do the following:

a. To save the settings, select **Submit**.

b. In OAuth2 Status, select **Authorize**.

c. In Microsoft Exchange Server Authorization, copy the code, and then select the URL.

d. Paste the code and select **Next**.

e. In Microsoft 365, do either of the following:

- Select a saved account.
- Select **Use another account** and enter the necessary information.

For Exchange Online accounts with two-factor authentication (2FA) enabled, make sure to have access to your preferred authentication app. Log in to your Exchange Online account, and then follow the instructions to complete 2FA. For more information, contact your Exchange Online server administrator.

f. Enter the multi-factor authentication (MFA) code.

g. To confirm the account selected for signing in, select **Consent on behalf of your organization** > **Accept**.

h. Once the permission request has been approved, select **Continue**.

i. Close the Exchange Online Client for Device window.

j. In Command Center RX, go back to Microsoft Exchange Server Authorization, then select the refresh icon to check the Authorization Status.

k. Once authorization is complete, select **OK** > **Submit**, and then check the OAuth2 Status.

l. To save the settings, select **Submit**.

Proxy Authentication for OAuth2

For added security in OAuth2 Authentication, before selecting **Authorize** in OAuth2 Status, you can set up OAuth2 with Proxy Authentication by doing the following:

a. Go to **Network Settings** > **TCP/IP** and in Proxy Settings, set Proxy to **On**.

b. In Proxy Server (HTTP), enter the required IP address and port number.
- The IP address and port number may vary depending on the proxy server configuration.
- If you set Use the Same Proxy Server for All Protocols to **On**, the same IP address and port number is used for Proxy Server (HTTPS).

c. Select **Submit** > **OK**.

After successfully setting up Proxy Settings, you can proceed with the OAuth2 authentication.

In the navigation menu, go to **Function Settings** > **E-mail** > **POP3**, then in POP3 User Settings, select **Settings**. In User (1 to 3), when **OAuth2** is selected in Authentication, do the following:

When Authentication is set to **OAuth2**, you do not have to enter the login user name and password since the credentials used for OAuth2 authentication are the same.

a. In Proxy Authentication for OAuth2, enter the user name and password.

b. In OAuth2 Status, check whether you have access. You can do either of the following:

- Select **Authorize** to enable access to OAuth2.
- Select **Unauthorize** to revoke access to OAuth2.

c. Select **Submit** > **OK**.

POP3 Security

Enables or disables POP3 Security. When this protocol is enabled, either **TLS** or **STARTTLS** must be selected. If you select **OAuth2** as an authentication, select **TLS**. To enable POP3 Security, the POP3 port may have to be changed according to the server settings. Configure settings in the **Network Settings** > **Protocol**.

Connection Test

To confirm that the settings are correct, select **Test** for the machine to try to connect to the POP3 server.

Delete e-mail after retrieval

Enables or disables the Delete e-mail after retrieval function. When this item is set to **On**, the retrieved email is deleted from the POP3 server. When this setting is Off, the email will not be deleted after retrieved from the POP3 server.

E-mail Size Limit

Set a size limit for outgoing email messages.

- An error will occur and the email will not be sent if the email size is larger than the specified size.
- If you set the value to 0, then it disables the email size limit.

Cover Page

Specifies whether to print the body of an email in addition to the attached files. When this setting is On, the attached files and the body of an email are printed. When no attached files exist, only the body of an email is printed. When this item is set to **Off**, only the attached files are printed. When no attached files exist, nothing is printed.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. Validity Period

b. Server Identity

c. **Chain**

d. **Revocation**

- You can use more than one option at a time.
- This feature is displayed when you select **Basic** in Authentication.

Revocation Check Type

In Revocation Check Type, select a method to confirm the revocation of digital certificate.

- **OCSP**
- **CRL**
- **CRL & OCSP**

This feature is displayed when you select **Basic** in Authentication.

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

- You can use more than one algorithm at a time.
- This feature is displayed when you select **Basic** in Authentication.

3 Select **Submit**.

E-mail Send Settings

1 In the navigation menu, go to **Function Settings** > **E-mail**.

2 If necessary, modify the following settings:

E-mail Size Limit

Set a size limit for outgoing email messages in the SMTP server.

- An error will occur and the email will not be sent if the email size is larger than the specified size.
- If you set the value to 0, then it disables the email size limit.

Sender Address

Enter the sender address for emails sent from this machine.

Signature

In Signature, create an email signature you want to reflect in outgoing messages.

SMTP Authentication and Sender Address

Select the information source (cites destination) of login user name, password, and email address used for SMTP authentication and email sender address.

When you select **Use Device Setting**, the login user name and login password configured in **Function Settings** > **E-mail** are used as SMTP authentication user information.

When you select **Use Login User Information**, the login user name and password for log in to this machine are used as SMTP authentication user information. This information also applies when you configure local authentication and network authentication. An email address included in user information (property) which was used to log in to the machine is used as the sender address information.

If necessary, configure the default settings. To change the default settings for the fax function, go to **Function Settings** > **Common/Job Defaults**.

3 Select **Submit**.

S/MIME Settings

To enable this setting, do the following in sequence:

1. Go to **Network Settings** > **Protocol**.
2. In Send Protocols, set SMTP (E-mail TX) to **On**.
3. In S/MIME, select **On**.
4. Select **Submit**.

1 In the navigation menu, go to **Function Settings** > **E-mail**.

2 Select any of the following as your encryption method:

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

3 Configure the Encryption Certificate. You can make changes for the following items as required.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **KeyUsage**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Revocation Check Type

In Revocation Check Type, select either of the following as your revocation digital certificate.

- **OCSP**
- **CRL**
- **CRL & OCSP**

Digital Signature

In Digital Signature, select from the following:

- **On**
- **Select at Sending**
- **Off**

Digital Signature Format

Select the digital signature format from the drop-down list.

Signing Certificate

a. In Signing Certificate, select **Settings**.

b. Select a certificate from the list.

c. Select **Submit**.

Configure the certificate setting in **Security Settings** > **Certificates**.

4 Configure the Signing Certificate. You can make changes for the following items as required.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **KeyUsage**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Revocation Check Type

In Revocation Check Type, select either of the following as your revocation digital certificate.

- **OCSP**
- **CRL**
- **CRL & OCSP**

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

5 Select **Submit**.

OAuth2 (Microsoft Exchange) Settings

You can configure your preferred OAuth 2.0 settings for Command Center RX.

1 In the navigation menu, go to **Function Settings** > **E-mail**.

2 In OAuth2 (Microsoft Exchange) Settings, select **Settings**.

3 Go to the authentication endpoint URL to configure your Microsoft account.

4 Select **Submit**.

Scan to Folder

This section includes advanced settings for copying.

FTP Settings

1 In the navigation menu, go to **Function Settings** > **Scan to Folder**.

2 Review the following settings:

FTP

Display whether an FTP connection is available or not. Set FTP Client (Transmission) to **On** in **Network Settings** > **Protocol**.

FTP Port Number

Display the FTP port number. Enter the port number in **Network Settings** > **Protocol**.

SMB Settings

1 In the navigation menu, go to **Function Settings** > **Scan to Folder**.

2 Review the following settings:

SMB

Display whether an SMB connection is available or not. Set SMB to **On** in **Network Settings** > **Protocol**.

SMB Port Number

Display the SMB port number. Enter Port Number in **Network Settings** > **Protocol**.

Function Default

1. In the navigation menu, go to **Function Settings** > **Scan to Folder**.
2. The default settings can be changed in **Function Settings** > **Common/Job Defaults**.

FAX

This section includes advanced settings for FAX.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the machine or the network. To restart the machine, go to **Management Settings** > **Restart/Reset**.

Common Settings

1. In the navigation menu, go to **Function Settings** > **FAX**.
2. In Transmission, configure the following settings:

Local FAX Name

Specifies your FAX system name.

TTI

Selects **On** or **Off** whether to send the TTI (Transmit Terminal Identifier) information to the other party.

TTI Position

Selects the position of the TTI to be printed on the transmitted documents.

Account as Local FAX Name

Set to **On** to use the account name as the local FAX name. The account name appears in place of the local FAX name.

Retry Times

Specify the retry times from 0 to 14 times.

3. In Reception, configure the following settings:

Media Type

Sets the media type to print the received documents.

FAX Exclusive Paper Source

Selects the exclusive paper source (cassette) when printing received faxes.

Receive Date/Time

Selects **On** or **Off** whether to print the reception information such as the received date, the received time, the transmitting party's information and the number of transmitted pages on the top of the received documents.

Duplex Printing

Selects **On** or **Off** whether to use Duplex mode.

This feature is available only in some machines.

2in1 Printing

Selects **On** or **Off** whether to use 2-in-1 reception.

Batch Print

Selects **On** or **Off** whether to do batch printing for the received documents.

4 Select **Submit**.

Fax Settings

1 In the navigation menu, go to **Function Settings** > **FAX**.

2 Specify required settings for any of the following:

General

a. Enter the local FAX number and ID.

b. In Speaker Volume, select your preferred volume of the internal speaker.

If you press the On-Hook key on a fax, the speaker volume allows you to listen to the other party or to verify the conditions on the telephone line.

c. In Monitor Volume, select your preferred volume of the internal speaker.

This setting allows you to verify the fax tones during fax communication.

Transmission

a. In Dialing Mode, depending on the type of telephone line you are contracted with, select from the following:

- **Tone (DTMF)**
- **Pulse (10PPS)**
- **Pulse (20PPS)**

b. In TX Start Speed, select from the following speed rate when starting fax transmission:

Once communication is established, the speed rate that is slower than the other is employed.

- **33600 bps**
- **14400 bps**
- **9600 bps**

c. Set ECM TX to **On**.

- This setting turns error correction mode on which corrects errors that may happen during communication.
- For ECM feature to take effect, you must first enable error correction mode in both parties.

d. If necessary, select Always Continuous Scan with Platen to **On**.

This setting allows you to continuously scan your documents from the platen only.

Reception

a. In RX Setting, select from the following FAX reception modes:

- **Auto (Normal)**
- **Auto (FAX/TEL)**
- **Auto (TAD)**
- **Manual**

b. Specify the number of rings.

This setting is available only if you select **Auto (Normal)** or **Auto (TAD)** in RX Setting.

c. In Remote Switching Dial Number, specify the FAX remote switching dial number.

This setting allows you to initiate FAX reception from a telephone connected to the machine.

d. Set your preferred encryption key.

> This setting is available only if an encryption key is registered.

e. In F-Net Silent Reception, select **On** to connect to the provided FAX transmission network (F-Net) and allow FAX transmission.

f. To use Dial-in Service, select **On**. When using a number as a telephone number, you can enter from `0000` to `9999` in Dial-in Number.

g. In RX Start Speed, select from the following speed rate when starting fax reception:

- **33600 bps**
- **14400 bps**
- **9600 bps**

h. Set ECM RX to **On**.

> - This setting turns error correction mode on which corrects errors that may happen during communication.
> - For ECM feature to take effect, you must first enable error correction mode in both parties.

i. In FAX Memory RX, select **On**.

Encryption Key

a. In Encryption Key Registration, select **Settings**.

b. Enter a 16-digit encryption key with a hexadecimal value from 0 to F.

c. Select **Submit**.

TX/RX Restriction

a. In Transmit Restriction, select either **Off** or **Permit List + Address Book**.

b. In Receive Restriction, select from the following reception restrictions:

- **Off**
- **Permit List + Address Book**
- **Reject List**

c. In Unknown Number Reception, select either **Reject** or **Permit**.

> This setting is available only if you select **Reject List** in Receive Restriction.

d. In Permit No. List, do the following:

1. Select **List**.
2. Add or delete permitted fax numbers.
3. Select **Submit**.

e. In Permit ID List, do the following:

1. Select **List**.
2. Add or delete permitted fax IDs.
3. Select **Submit**.

f. In Reject No. List, do the following:

1. Select **List**.
2. Add or delete prohibited fax numbers.
3. Select **Submit**.

FAX Server Settings

Configure the following settings:

a. Set FAX Server to **On**.

b. Select **Settings** and do the following:

Address Settings

1. Enter the fax server information for the following:
   - Prefix
   - Suffix
   - Domain name
2. In File Format, select from the following:
   - **PDF**
   - **TIFF**
   - **XPS**

SMTP

1. Set Use E-mail SMTP Settings to **On**, and then select **Submit**. When this setting is Off, proceed to step 2.

   - Configure the SMTP settings if you want to send the fax via SMTP server.
   - When this setting is On, the fax server uses the email SMTP settings configured in **Function Settings** > **E-mail**.

2. Enter the SMTP server name or its IP address.

If you entered the SMTP server name, instead of the IP address, a DNS server address must also be configured. To configure the DNS server address, go to **Network Settings** > **TCP/IP**.

3. Enter the port number. The default port number is 25.
4. Enter your preferred timeout during which this device tries to connect to the SMTP server.
5. In Authentication Protocol, set your preferred authentication type.

On

This option enables authentication protocol.

a. Select **On**.

b. In Authentication as, select either **POP before SMTP (FAX Server)** or **Other**.

POP before SMTP

This is an authentication mode that allows you to send an email from any location and also fetch your email from the same place.

a. Select **POP before SMTP**.

b. In Authentication as, select **POP before SMTP (FAX Server)**.

c. In POP before SMTP Timeout, enter your preferred timeout during which this device tries to connect to the POP3 server.

This setting is enabled when **POP before SMTP** is selected as the authentication protocol.

Off

Select this option to disable authentication protocol.

OAuth2

Select this option to enable OAuth 2.0 as an authentication protocol.

When Authentication Protocol is set to **OAuth2**, you do not have to enter the login user name and password since the credentials used for OAuth2 authentication are the same.

a. Select **OAuth2**.

b. In Proxy Authentication for OAuth2, enter a user name and password.

c. To confirm that the information for OAuth 2.0 is correct, select **Authorize**.

6. In SMTP Security, the status is displayed.

   This setting is enabled when **TLS** or **STARTTLS** is selected in **Network Settings** > **Protocol**.

7. To confirm that the settings are correct, select **Test** for the machine to try to connect to the SMTP server.

   Review the test results. If you encounter any errors, review and modify the settings.

8. If necessary, activate whether configured domain names in the Domain List are permitted or restricted domains.

   This setting is enabled when a domain name is listed in the SMTP Domain Restriction List. To configure a domain name, do the following:

   a. Select **Domain List**.

   b. Enter a domain name that is either permitted or rejected. You can also specify email addresses.

   c. Select **Submit** > **Back**.

For more details about OAuth2 in SMTP configuration, refer to *SMTP*.

POP3 User Settings

1. Enter the POP3 server host name or IP address.

If you entered the host name, make sure that the DNS server information is specified.

2. Enter the port number. The default port number is 110.
3. Enter your preferred timeout during which this device tries to connect to the POP3 server.
4. Enter the login user name and login password of your POP3 account.
5. If necessary, set Use APOP to **On**.

- APOP is an encryption mechanism used for encrypting the Login Password during communication with the POP3 server.
- When enabled, the login password is encrypted.
- When disabled, the login password is sent using plain ASCII text.
- To use this feature, the POP3 server must support and enable configuration for APOP.

6. To confirm that the settings are correct, select **Test** for the machine to try to connect to the POP3 server.

E-mail Send Settings

1. Set a size limit for outgoing email messages.

- An error will occur and the email will not be sent if the email size is larger than the specified size.
- If you set the value to 0, then it disables the email size limit.

2. Enter the sender address for emails sent from this machine.
3. In Signature, create an email signature you want to reflect in outgoing messages.

c. In Default Address Book, select your preferred external address book. For details, see *External Address Book Settings*.

d. If necessary, configure the default settings. To change the default settings for the fax function, go to **Function Settings** > **Common/Job Defaults**.

Send and Forward

When sending a FAX, FTP, SMB or an email job, Send and Forward automatically forwards the same job to a destination specified.

General

1. In the navigation menu, go to **Function Settings** > **Send and Forward**.
2. This section includes the following items for configuration.

Send and Forward

Set Send and Forward to **On** or **Off**.

Rule

Select **E-mail**, **Folder(SMB)**, **Folder(FTP)**, or **FAX**.

3. Select **Submit**.

Destination

1. In the navigation menu, go to **Function Settings** > **Send and Forward**.
2. This section includes the following items for configuration.

Address Book

Select **Address Book** and select a type and a name of the address on the address page.

E-mail

E-mail forwards the email to the email address entered.

a. Select **E-mail** to specify an email address.
b. If necessary, select **Address Book** to change the address.
c. To finish the settings, select **Submit**.

Folder

Forwards and saves a job in a folder (SMB or FTP).

a. Enter the host name, port number, path to a folder, login user name, and the login password.

If you entered the host name, make sure you specify the DNS server information.

b. To confirm that the settings entered are correct, select **Test**.
c. If necessary, select **Address Book** to change the address.
d. To finish the settings, select **Submit**.

Delete

Removes the address selected.

3 Select **Submit**.

Forward Job Settings

1 In the navigation menu, go to **Function Settings** > **Send and Forward**.

2 In S/MIME, set E-mail Encrypted TX to **On** to send the encrypted e-mail using S/MIME. Set Digital Signature to E-Mail to **On** to send email with digital signature.

3 Select **Submit**.

Forwarding

Forwarding is a function for automatically forwarding documents received by FAX to other FAX machines, sending them as attachments to email.

For example, you can forward faxes from particular customers received during business hours to the email addresses of the people responsible for those customers, and forward faxes from outside of your business area to the business office nearest to the sender's fax number.

For models that do not support Forward Requirements, the documents received are forwarded to a forward destination or printed.

Enabling Forwarding Settings

1 In the navigation menu, select **Function Settings** > **Forwarding**.

2 In Forward Settings, select **On**.

3 In Schedule, select either **All Day** or **Preset Time**.
If you select Preset Time, specify the start and end time.

4 Enter the name of the document in File Name. If necessary, select additional information from the drop-down list.

5 Select from the following destinations, and then specify the required settings for any of the following:

To remove a previously set destination, select **Delete**.

Address Book

Select address names from the address book for your forward destination.

E-mail

Enter a valid email address.

Folder

Configure the settings of your folder.

a. Select either **SMB** or **FTP**.

b. Enter the host name, port number, path of the folder, login user name, and login password.

If you use the host name, make sure you specify the DNS server information.

c. To confirm if the settings are correct, select **Test**.

FAX

Configure the settings for your fax server.

a. Enter the fax number, subaddress, and the password for the subaddress.

b. Select **33600 bps**, **14400 bps**, or **9600 bps**.

c. To enable ECM communication, select **On**.

d. In Encryption, select **Off** or your preferred encryption key.

When using Key (1 to 20), you must create the encryption key in advance in **Function Settings** > **Fax Settings**.

e. To enable the encryption box, select **On**. You can configure this setting when the encryption key is selected in Encryption.

f. Enter the four-digit box number. You can configure this setting when the encryption key is selected in Encryption and Encryption Box is set to **On**.

File Format

Select your preferred file format from the following:

- **PDF**
- **TIFF**
- **XPS**
- **Open XPS**

PDF Encryption

Select **On** to use PDF encryption function. Configure the following settings as necessary:

Compatibility

Select **Acrobat 3.0 and later** or **Acrobat 5.0 and later**.

Password to Open Document

Select **On** to set the password to open the document, enter the password, and enter the password again for confirmation.

Password to Edit/Print Document

Select **On** to set the password to edit or print the document, enter the password, and enter the password again for confirmation. In Printing Allowed and Changes Allowed, select from the following:

- Not Allowed
- Allowed (Low Resolution Only)
- Allowed

Select **Enable** to permit to copying of text or images on Copying of Text/Images/Others.

PDF/A

PDF/A is an electronic file format for long-term preservation of documents as addressed in the ISO 19005-1 specification. Set the PDF/A-compliant format of the document. Select from the following:

- **PDF/A-1a**
- **PDF/A-1b**
- **PDF/A-2a**
- **PDF/A-2b**
- **PDF/A-2u**
- **Off**

File Separation

To enable file separation, select **Each Page**.

E-mail Subject Additional Info.

If necessary, select additional information for the email subject.

FTP Encryption TX

To enable the FTP encryption transmission function, select **On**.

This feature is available only if you go to **Security Settings** > **Network Security** and set TLS to **On**.

S/MIME

To enable S/MIME, do the following:

a. Go to **Network Settings** > **Protocol**.

b. In Send Protocols, set SMTP (E-mail TX) to **On**.

c. In S/MIME, select **On**.

d. Select **Submit**.

Do the following:

- To send the encrypted email using S/MIME, set E-mail Encrypted TX to **On**.
- To send the email using a digital signature, set Digital Signature to E-mail to **On**.

> To enable Digital Signature to E-mail, set an external address book (1 to 4) to **On**. Refer to *External Address Book Settings*. Do the following in sequence:
>
> **a.** Go to **Function Settings** > **E-mail**.
>
> **b.** In S/MIME Settings, set Digital Signature to **Select at Sending**.
>
> **c.** In Signing Certificate, select **Settings**.
>
> **d.** Select your preferred device certificate, then click **Submit**.

6 Select **Submit**.

Operation Panel

This section explains how to customize the operation panel.

Home

1 In the navigation menu, go to **Function Settings** > **Operation Panel**.

2 This section includes the following items for configuration.

Customize Desktop

a. To add an item in the home screen of the operation panel, select either from the following:

- **Add Function**
- **Add Favorites**
- **Add Application**

b. You can also use **Up** and **Down** to change the order of the items.

c. To finish the settings, select **Submit**. To delete items that are not needed, select an item, then click **Delete**.

Customize Taskbar

Specifies the items to show in the task bar. You can enable each of the following items:

- **None**
- **Status/Job Cancel**

- **Device Information**
- **Language**
- **Paper Settings**
- **Help**
- **User Property**
- **Incoming FAX Log**
- **Outgoing FAX Log**
- **System Menu**
- **Favorites**
- **Network Settings**

Incoming FAX Log and Outgoing FAX Log appear when FAX functions are available in the model.

Background

Allows you to change the background image of the home screen. Select an image.

3 Select **Submit**.

Quick Setup Registration

1 In the navigation menu, go to **Function Settings** > **Operation Panel**.

2 This section includes the following items for configuration. By default, each function is assigned with its standard items.

Copy

Each of Key (1 to 6) is assigned with one of the copying functions. Select an item from the drop-down list.

Send

Each of Key (1 to 6) is assigned with one of the sending functions. Select an item from the drop-down list.

FAX

Each of Key (1 to 6) is assigned with one of the fax functions. Select an item from the drop-down list.

Store Document in Box

Each of Key (1 to 6) is assigned with one of the Store Document in Box functions. Select an item from the drop-down list.

Print Document in Box

Each of Key (1 to 6) is assigned with one of the Print Document in Box functions.

3 Select **Submit**.

Cloud Access

Cloud Access is a utility application that is installed on a computer. You can configure this application to connect to any supported cloud service, and link one or more user accounts.

In Command Center RX, you can configure the settings for Cloud Access connection between a computer and a device.

1. In the navigation menu, select **Function Settings** > **Cloud Access**.
2. Select **Settings**, then set Connect to Cloud Access to **On**.
3. In Edit Restriction, select either **Off** or **Administrator Only**.
4. If necessary, set Use Device Login Information to **On**.

   This setting is displayed if User Authentication is On.

5. Select **Submit** > **Back**.

   To set a connection in the connection list, see *Adding a connection*, *Editing a connection*, and *Deleting a connection*.

Adding a connection

1. In Connection List, select **Add**.
2. If necessary, set the assigned connection ID.
3. Enter the connection name.
4. Enter the host name and port number.
5. To confirm that the settings are correct, select **Test**.
6. Select **Submit**.

Editing a connection

1. In Connection List, do either of the following:
   - Select the connection ID or name you want to edit.
   - Enter the connection ID or connection name in the corresponding search box. If you use the connection name for searching, then select the connection name you want to edit.
2. Modify any of the following:
   - Connection ID
   - Connection Name
   - Host Name

- Port Number

3. To confirm that the settings are correct, select **Test**.
4. Select **Submit**.

Deleting a connection

1. In Connection List, do either of the following:
   - Select the checkbox of the connection you want to delete.
   - Select the **Check All** icon to delete all items. To clear all selections, select the **None** icon.
2. Select the **Delete** icon.

8 Network Settings

This page is accessible when you have logged in the embedded server with administrator rights, while network authentication or local authentication is enabled.

If needed, make the following settings:

- General
- TCP/IP
- Protocol
- Wireless LAN

General

This section includes basic settings for networking.

1. In the navigation menu, go to **Network Settings** > **General**.
2. Select **Wired Network** or **Wi-Fi** from the Primary Network (Client) drop-down list.
3. The current communication status is shown in Host Name. Configure the host name on the System Settings page of Device Settings.
4. The host name is shown in NetBIOS Name. You can modify the name as necessary.
5. Select an option from the LAN Interface drop-down list.
   - **Auto**
   - **10BASE-Half**
   - **10BASE-Full**
   - **100BASE-Half**
   - **100BASE-Full**
   - **1000BASE-T**
6. The current status is shown in Client Certificate. Do the following:
   a. To make advanced settings, select **Settings**.
   b. In Certificate Settings, select the appropriate certificate.
   c. Select **Submit**.

TCP/IP

This section includes advanced settings for the TCP/IP protocol.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the machine or the network. To restart the machine, go to **Management Settings** > **Restart/Reset**.

General Settings (Wired Network)

1. In the navigation menu, go to **Network Settings** > **TCP/IP**.
2. To enable TCP/IP on the Wired Network, select **On**.
3. Select **Submit**.

General Settings (Wireless Network)

1. In the navigation menu, go to **Network Settings** > **TCP/IP**.
2. To enable TCP/IP on the Wireless Network, select **On**.
3. Select **Submit**.

General Settings (Common)

1. In the navigation menu, go to **Network Settings** > **TCP/IP**.
2. When an IP address that was mapped by the DNS server has been changed, Dynamic DNS automatically remaps the host name to the IP address. To enable the Dynamic DNS Settings, set Dynamic DNS to **On**. In addition, specifies the timeout in seconds after which a search on the DNS server expires.
3. Select **Submit**.

Proxy Settings

1. In the navigation menu, go to **Network Settings** > **TCP/IP**.
2. To configure the proxy, set Proxy to **On**, and specify the following items as required.

Automatically Detect

Select **On** to detect the proxy server automatically.

Use Automatic Configuration Script

Select **On** and enter the address when you use the automatic configuration script.

Proxy Server (HTTP)

Enter the host name or IP address for the proxy server (HTTP).

If you use the host name, you must first specify the DNS server information.

Port Number

Enter the port number for the proxy server (HTTP).

Use the Same Proxy Server for All Protocols

Select **On** when you use the same proxy server for all protocols.

Proxy Server (HTTPS)

Enter the host name or IP address for the proxy server (HTTPS).

If you use the host name, you must first specify the DNS server information.

Port Number

Enter the port number for the proxy server (HTTPS).

Do Not Use Proxy for Following Domains

Enter the domain address that do not use the proxy. Use a semicolon (;) between multiple addresses.

3 Select **Submit**.

IPv4 Settings (Wired Network)

1 In the navigation menu, go to **Network Settings** > **TCP/IP**.

2 This section includes the following items for configuration.

DHCP/BOOTP

To automatically obtain an IP address using DHCP or BOOTP, enable this setting.

Auto-IP

To automatically generate an IP address, set Auto-IP to **On** and restart the network.

- The generated IP address is from 169.254.0.1 through 169.254.255.254. However, if the IP address is using the DHCP server or manual settings are configured, the Auto-IP address is not generated even when Auto-IP is set to **On**.
- If the IP address has already been manually entered in IP Address, delete the address.
- The automatically generated IP address appears in **Device Information** > **Configuration** of the navigation menu.

IP Address

Enter a static IPv4 address as part of the system network settings.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.
- For example: 192.168.110.171

Subnet Mask

Specify the subnet mask.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.

Domain Name

Specify the domain name of the domain to which the machine belongs.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- The domain name should not contain the host printer name.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.

DNS Server

Specify the IP addresses of the primary and secondary DNS (Domain Name System) servers.

- If DHCP/BOOTP is set to **On** and **Use DNS Server from DHCP** is selected, the DNS server is obtained via DHCP.
- If DHCP/BOOTP is set to **On** and **Use following DNS Server** is selected, enter the static DNS server information.

DNS Server (Primary)

Specify the IP address of primary DNS server.

DNS Server (Secondary)

Specify the IP address of secondary DNS server.

DNS Search Suffix

Specify the primary and secondary DNS (Domain Name System) search suffix.

- This setting is enabled when DHCP/BOOTP is set to **On**.
- When DHCP/BOOTP is set to **On** and **Use following DNS Search Suffix** is selected, enter the static DNS search suffix.

DNS Search Suffix (Primary)

Specify the suffix for DNS Search Suffix (Primary).

DNS Search Suffix (Secondary)

Specify the suffix for DNS Search Suffix (Secondary).

DNS over TLS

In DNS over TLS, do one of the following options:

- To automatically configure DNS over TLS, select **Auto**.
- To enable DNS over TLS, select **On**.
- To disable DNS over TLS, select **Off**.

DNS over TLS is a protocol developed for DNS name resolution using the Transport Layer Security (TLS) protocol.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**
b. **Server Identity**
c. **Chain**
d. **Revocation**

You can use more than one option at a time.

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

WINS Server

Specify the IP addresses of the primary and secondary WINS (Windows Internet Name Service) servers.

- If DHCP/BOOTP is set to **On** and **Use WINS Server from DHCP** is selected, the WINS server is obtained via DHCP.
- If DHCP/BOOTP is set to **On** and **Use following WINS Server** is selected, enter the static WINS server information.

WINS Server (Primary)

Specify the IP address of primary WINS server.

WINS Server (Secondary)

Specify the IP address of secondary WINS server.

3 Select **Submit**.

IPv4 Settings (Wireless Network)

1 In the navigation menu, go to **Network Settings** > **TCP/IP**.

2 This section includes the following items for configuration.

DHCP/BOOTP

To automatically obtain an IP address using DHCP or BOOTP, enable this setting.

Auto-IP

To automatically generate an IP address, set Auto-IP to **On** and restart the network.

- The generated IP address is from 169.254.0.1 through 169.254.255.254. However, if the IP address is using the DHCP server or manual settings are configured, the Auto-IP address is not generated even when Auto-IP is set to **On**.
- If the IP address has already been manually entered in IP Address, delete the address.
- The automatically generated IP address appears in **Device Information** > **Configuration** of the navigation menu.

IP Address

Enter a static IPv4 address as part of the system network settings.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.
- For example: 192.168.110.171

Subnet Mask

Specify the subnet mask.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.

Domain Name

Specify the domain name of the domain to which the machine belongs.

- This setting is enabled when DHCP/BOOTP is set to **Off**.
- The domain name should not contain the host printer name.
- If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device, and the field is grayed out.

DNS Server

Specify the IP addresses of the primary and secondary DNS (Domain Name System) servers.

- If DHCP/BOOTP is set to **On** and **Use DNS Server from DHCP** is selected, the DNS server is obtained via DHCP.
- If DHCP/BOOTP is set to **On** and **Use following DNS Server** is selected, enter the static DNS server information.

DNS Server (Primary)

Specify the IP address of primary DNS server.

DNS Server (Secondary)

Specify the IP address of secondary DNS server.

DNS Search Suffix

Specify the primary and secondary DNS (Domain Name System) search suffix.

- This setting is enabled when DHCP/BOOTP is set to **On**.
- When DHCP/BOOTP is set to **On** and **Use following DNS Search Suffix** is selected, enter the static DNS search suffix.

DNS Search Suffix (Primary)

Specify the suffix for DNS Search Suffix (Primary).

DNS Search Suffix (Secondary)

Specify the suffix for DNS Search Suffix (Secondary).

DNS over TLS

In DNS over TLS, do one of the following options:

- To automatically configure DNS over TLS, select **Auto**.
- To enable DNS over TLS, select **On**.
- To disable DNS over TLS, select **Off**.

DNS over TLS is a protocol developed for DNS name resolution using the Transport Layer Security (TLS) protocol.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **Server Identity**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

WINS Server

Specify the IP addresses of the primary and secondary WINS (Windows Internet Name Service) servers.

- If DHCP/BOOTP is set to **On** and **Use WINS Server from DHCP** is selected, the WINS server is obtained via DHCP.
- If DHCP/BOOTP is set to **On** and **Use following WINS Server** is selected, enter the static WINS server information.

WINS Server (Primary)

Specify the IP address of primary WINS server.

WINS Server (Secondary)

Specify the IP address of secondary WINS server.

3 Select **Submit**.

IPv4 Settings (Common)

1 In the navigation menu, go to **Network Settings** > **TCP/IP**.

2 This section includes the following items for configuration.

Default Gateway

Specify the IP address of the default gateway.

If DHCP/BOOTP is set to **On**, a dynamic IPv4 address is assigned to the device.

Host Name

In Host Name, do either of the following:

- To get a host name from the DHCP server, select **Use Host Name from DHCP**.
- To get a host name from the device settings, select **Use Host Name from Device Setting**.

3 Select **Submit**.

IPv6 Settings (Wired Network)

1 In the navigation menu, go to **Network Settings** > **TCP/IP**.

2 This section includes the following items for configuration.

IPv6

To enable IPv6 protocol, select **On**.

IP Address

TA static IPv6 address can be entered in this field for the device as part of the system network settings. Assigns an IPv6 address to the machine network component. Enter a static IPv6 address.

For example: 2001:db8:3c4d:15::1a2c:1a1f

Prefix Length

Specify the IPv6 prefix length.

It can be a decimal value between 0 and 128.

RA (Stateless)

To generate the IPv6 stateless address on the machine, set RA (Stateless) to **On**.

Make sure the network provides the IPv6 address prefix in the router advertise information.

DHCPv6 (Stateful)

To assign an IPv6 stateful address (128-bit length) to the machine by the DHCPv6 server, set DHCPv6 (Stateful) to **On**.

Make sure the network provides the "Managed Address Configuration."

Domain Name

Specify the domain name of the domain to which the machine belongs.

This setting is enabled when DHCPv6 (Stateful) is set to **Off**.

DNS Server

Specify the IP addresses of the primary and secondary DNS (Domain Name System) servers.

- If DHCP/BOOTP is set to **On** and **Use DNS Server from DHCP** is selected, the DNS server is obtained via DHCP.
- If DHCP/BOOTP is set to **On** and **Use following DNS Server** is selected, enter the static DNS server information.

DNS Server (Primary)

Specify the IP address of primary DNS server.

DNS Server (Secondary)

Specify the IP address of secondary DNS server.

DNS Search Suffix

Specify the primary and secondary DNS (Domain Name System) search suffix.

- This setting is enabled when DHCP/BOOTP is set to **On**.
- When DHCP/BOOTP is set to **On** and **Use following DNS Search Suffix** is selected, enter the static DNS search suffix.

DNS Search Suffix (Primary)

Specify the suffix for DNS Search Suffix (Primary).

DNS Search Suffix (Secondary)

Specify the suffix for DNS Search Suffix (Secondary).

DNS over TLS

In DNS over TLS, do one of the following options:

- To automatically configure DNS over TLS, select **Auto**.
- To enable DNS over TLS, select **On**.
- To disable DNS over TLS, select **Off**.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **Server Identity**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

3 Select **Submit**.

IPv6 Settings (Wireless Network)

1 In the navigation menu, go to **Network Settings** > **TCP/IP**.

2 This section includes the following items for configuration.

IPv6

To enable IPv6 protocol, select **On**.

IP Address

TA static IPv6 address can be entered in this field for the device as part of the system network settings. Assigns an IPv6 address to the machine network component. Enter a static IPv6 address as part of the system network settings.

For example: 2001:db8:3c4d:15::1a2c:1a1f

Prefix Length

Specify the IPv6 prefix length.

It can be a decimal value between 0 and 128.

RA (Stateless)

To generate the IPv6 stateless address on the machine, set RA (Stateless) to **On**.

Make sure the network provides the IPv6 address prefix in the router advertise information.

DHCPv6 (Stateful)

To assign an IPv6 stateful address (128-bit length) to the machine by the DHCPv6 server, set DHCPv6 (Stateful) to **On**.

Make sure the network provides the "Managed Address Configuration."

Domain Name

Specify the domain name of the domain to which the machine belongs.

This setting is enabled when DHCPv6 (Stateful) is set to **Off**.

DNS Server

Specify the IP addresses of the primary and secondary DNS (Domain Name System) servers.

- If DHCPv6 (Stateful) is set to **On** and **Use DNS Server from DHCP** is selected, the DNS server is obtained via DHCP.
- If DHCPv6 (Stateful) is set to **On** and **Use following DNS Server** is selected, enter the static DNS server information.

DNS Server (Primary)

Specify the IP address of primary DNS server.

DNS Server (Secondary)

Specify the IP address of secondary DNS server.

DNS Search Suffix

Specify the primary and secondary DNS (Domain Name System) search suffix.

- This setting is enabled when DHCP/BOOTP is set to **On**.
- When DHCP/BOOTP is set to **On** and **Use following DNS Search Suffix** is selected, enter the static DNS search suffix.

DNS Search Suffix (Primary)

Specify the suffix for DNS Search Suffix (Primary).

DNS Search Suffix (Secondary)

Specify the suffix for DNS Search Suffix (Secondary).

DNS over TLS

In DNS over TLS, do any of the following options:

- To automatically configure DNS over TLS, select **Auto**.
- To enable DNS over TLS, select **On**.
- To disable DNS over TLS, select **Off**.

Certificate Auto Verification

In Certificate Auto Verification, select the following in sequence:

a. **Validity Period**

b. **Server Identity**

c. **Chain**

d. **Revocation**

You can use more than one option at a time.

Hash

In Hash, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

3 Select **Submit**.

IPv6 Settings (Common)

1 In the navigation menu, select **Network Settings** > **TCP/IP**.

2 In Default Gateway, specify the IPv6 address.

3 Select **Submit**.

Bonjour Settings

1 In the navigation menu, select **Network Settings** > **TCP/IP**.

2 Specify the required settings for any of the following:

Bonjour

a. In Bonjour, select **On**.

b. Select an available network for Bonjour.

Bonjour Name

Review or modify the name as necessary.

Bonjour Name is displayed when Bonjour is set to **On**.

3 Select **Submit**.

IP Filter(IPv4) Settings

This section allows you to configure IP filters. IP filters restrict access to the machine based on the IP addresses and protocols.

Specify the IP addresses or network addresses of the hosts to allow. If there are no entries, then all access is allowed. Do the following:

1 In the navigation menu, select **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 To make advanced settings, select **Settings**. Specify the required settings for any of the following:

You can set multiple filters.

Network Interface

Select an available network for IP Filter (IPv4).

IP Address(IPv4)

Specify the IP address or network address to allow.

Subnet Mask

Specify the subnet mask to allow. If there are no entries, then all access is allowed.

To allow access to the network, enter the IPv4 address and the subnet mask. For example, to allow access from all hosts on network 192, enter `192.0.0.0` for the IP address and `255.0.0.0` for the subnet mask.

To allow access to a single IP address, enter the IPv4 address and `255.255.255.255` for the subnet mask.

Protocols

Specify one or more protocols to allow.

ThinPrint is an optional protocol and is available only when installed.

6 Select **Submit**.

IP Filter(IPv6) Settings

This section allows you to configure IP filters. IP filters restrict access to the machine based on the IP addresses and protocols.

Specify the IP addresses or network addresses of the hosts to allow. If there are no entries, then all access is allowed.

1 In the navigation menu, select **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 To make advanced settings, select **Settings**. Specify the required settings for any of the following:

You can set multiple filters.

Network Interface

Select an available network for IP Filter (IPv6).

IP Address(IPv6)

Specify the IP addresses to allow. If there are no entries, then all access is allowed.

The number of addresses you can specify depends on the prefix length setting and the IPv6 address.

To filter a single IPv6 address, enter the IPv6 address with a maximum prefix length of 128.

Prefix Length

Enter the IPv6 prefix length. It can be a decimal value from 0 to 128.

Protocols

Specify one or more protocols to allow.

ThinPrint is an optional protocol and is available only when installed.

6 Select **Submit**.

Logical Printers

You can use logical printers as virtual printers to convert ASCII print data to PostScript data, or to add and replace character strings at the start or end of job string.

You can set up to four logical printers.

A logical printer can be any of the following print protocols:

- FTP
- LPD
- IPP
- IPPS
- SMB Server Protocol
- Raw

If no port is specified for printing, enter the port number. The default port number is 9100.

To configure the logical printers, do the following:

1. In the navigation menu, select **Network Settings** > **TCP/IP**.
2. Go to logical printers then select **Settings**. Specify the required settings for any of the following:

   You can set multiple logical printers.

   TCP/IP Port Number

   Enter a logical printer port value that is the same with TCP Raw port number, for example, 9100. The TCP Raw port changes depending on the value entered for the logical printer port.

   If you assigned the same port number to other ports, such as FTP or LPD, then the port is disabled.

   Bi-directional Printing

   When printing to a TCP/IP Raw port, do the following:

   - To remove all Send data, select **Off**.
   - To return the data received from the printer to the client when printing with PostScript or PJL commands, select **On**.

   Start of Job String

   Specify the character string to send to the printer before printing directly to the output port or logical port. If necessary, send the control code before sending the print data for the string specification.

End of Job String

Specify the character string to send to the printer before printing directly to the output port or logical port. If necessary, send the control code after sending the print data for the string specification.

3 Select **Submit**.

IPSec Settings

This section allows you to set access restrictions for IPSec protocol-based communication.

1 In the navigation menu, select **Network Settings** > **TCP/IP**.

Specify whether to enable the IPSec protocol. Select **On** to use the IPSec protocol. Select **Off** when encryption is not used.

2 Specify the required settings for any of the following:

Expiration Verification

Set Expiration Verification to **On**.

- When enabled, the expiration of the server certificate is verified.
- If the certificate is expired then Command Center RX cannot communicate with the printing system.

Restriction

Specifies the default policy for non-IPSec packets. Select **Allowed** to allow communication with all hosts and networks including those not permitted by the rules. Select **Denied** to allow communication only with the hosts and networks permitted by the rules.

- Allowed means normal traffic (not defined by the IPSec rules) will be allowed to reach the device.
- 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

Displays whether the certificate is active for Root Certificate (1 to 5) Subject.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

IPSec Rules

Allows to validate the rule used for communication using the IPSec protocol. Rule (1 to 10) are displayed. To configure this item, select **Settings**. For details, see *Configuring IPSec Rules*.

3 Select **Submit**.

Configuring IPSec Rules

1 In the navigation menu, select **Network Settings** > **TCP/IP**.

2 In IPSec Settings, set IPSec to **On**. Then in IPSec Rules, select **Settings**.

3 Do one or more of the following:

Policy

Set the policy for using IPSec protocol-based communication.

a. In Rule, select **On**.

b. In Key Management Type, select from the following:

- **IKEv1**
- **IKEv2**
- **Manual**

c. For Encapsulation Mode, select either **Transport** or **Tunnel**.

- Transport encapsulates an encrypted data and transmits along with an IP header. This is the simplest method when both the transmitting host and receiving host have the IPSec protocol supported.
- Tunnel uses a gateway provided in the network. The gateway receives the IP packets sent by the transmitting host, encrypt the entire IP packet which is then encapsulated by IPSec, then transmits along with a new IP header.

IP Address

Specify the IP addresses of the hosts or network with which the machine is connecting via IPSec.

a. For IP Version, select either **IPv4** or **IPv6**.

b. If **IPv4** is selected, enter the IP address and subnet mask.

- When you are restricting the scope of IPSec, be sure to specify the IP addresses. If the IP Address (IPv4) field is blank, all IPv4 addresses will be allowed to connect to the machine.
- When **IPv4** is selected for IP Version, specify the subnet mask. If the Subnet Mask field is blank, the specified addresses are considered to be host addresses.

c. If **IPv6** is selected, enter the IP address and prefix length.

- When you are restricting the scope of IPSec, be sure to specify the IP addresses. If the IP Address (IPv6) field is blank, all IPv6 addresses will be allowed to connect to the machine.
- When **IPv6** is selected for IP Version, specify the prefix length. If the Prefix Length field is blank, the specified addresses are considered to be host addresses.

d. If necessary, enter the remote peer address.

Remote Peer Address is available only when **Tunnel** is selected in Encapsulation Mode.

Authentication

Configure the local side or remote side authentication when using IPSec protocol.

If **IKEv1** is selected as the Key Management Type, configure the following for Local Side:

a. In Authentication Type, select either **Certificates** or **Pre-shared Key**.

b. If **Certificates** is selected, the device certificate status is displayed.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

c. If **Pre-shared Key** is selected, enter the pre-shared key.

If **IKEv2** is selected as the Key Management Type, configure the following for Local Side and Remote Side:

a. In Authentication Type, select either **Certificates** or **Pre-shared Key**.

b. In Local or Remote ID Type, select from the following:

- **Distinguished Name**

- **IP Address**
- **FQDN**
- **E-mail Address**
- **Key ID**

c. Enter the local or remote ID.

d. If **Certificates** is selected in Authentication Type, the device certificate status is displayed in Local Side.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

e. If **Pre-shared Key** is selected in Authentication Type, enter the pre-shared key for local or remote side.

Key Exchange (IKE phase1)

Key Exchange (IKE phase1) is available only when either **IKEv1** or **IKEv2** is selected in Key Management Type.

When using IKE phase1, a secure connection with the other end is established by generating ISAKMP SAs. Configure the following items so that they meet the requirement of the other end:

a. For Mode, select either **Main Mode** or **Aggressive Mode**.

- Mode is available when **IKEv1** is selected in Key Management Type.
- Main Mode protects identifications but requires more messages to be exchanged with the other end.
- Aggressive Mode requires fewer messages to be exchanged with the other end but restricts identification protection and narrows the extent of the parameter negotiations.
- When **Aggressive Mode** is selected and **Pre-shared Key** is selected for Authentication Type, only host addresses can be specified for IP addresses of the rule.

b. Select the hash algorithm.

You can use more than one algorithm at a time.

c. Select the encryption algorithm.

You can use more than one algorithm at a time.

d. Select a Diffie-Hellman group from the drop-down list.

The Diffie-Hellman Group key-sharing algorithm allows two hosts on an unsecured network to share a private key securely.

e. In Lifetime (Time), enter the ISAKMP SA lifetime in seconds.

Data Protection (IKE phase2)

Data Protection (IKE phase2) is available only when either **IKEv1** or **IKEv2** is selected in Key Management Type.

In IKE phase2, IPSec SAs such as ESP or AH are established by using SAs established in IKE phase1. Configure the following items so that they meet the requirement of the other end:

a. For Protocol, select either **ESP** or **AH**.

- ESP protects the privacy and integrity of packet contents.
- AH protects the integrity of the packet contents using encryption checksum. When **AH** is selected, you cannot use the AES-GCM-128, AES-GCM-192, or AES-GCM-256.

b. Select the hash algorithm.

You can use more than one algorithm at a time.

c. Select the encryption algorithm.

- You can use more than one algorithm at a time.
- Encryption is available only when **ESP** is selected in Protocol.
- If you select **AES-GCM-128** or **AES-GMAC-128** in Hash, you must also select **AES-GCM-128** in Encryption.
- If you select **AES-GCM-192** or **AES-GMAC-192** in Hash, you must also select **AES-GCM-192** in Encryption.
- If you select **AES-GCM-256** or **AES-GMAC-256** in Hash, you must also select **AES-GCM-256** in Encryption.
- If no encryption algorithm is selected, the device will authenticate without encryption.

d. If necessary, set PFS to **On**.

When PFS is enabled, even if a key is decrypted, the decrypted key cannot be used to decrypt the other keys generated after the decryption. This improves the safety, but imposes a heavy burden because of more key-generation processes.

e. Select a Diffie-Hellman group from the drop-down list.

Diffie-Hellman Group is available only when PFS is set to **On**.

f. For Lifetime Measurement, select either **Time** or **Time & Data Size**.

g. In Lifetime (Time), enter the IPSec SA lifetime in seconds.

h. In Lifetime (Data Size), enter the IPSec SA lifetime in kilobytes.

Lifetime (Data Size) is available only when **Time & Data Size** is selected in Lifetime Measurement.

i. If necessary, set Extended Sequence Number to **On**.

Manual Key Settings

Manual Key Settings is available only when **Manual** is selected in Key Management Type.

Configure the following items for manual key settings:

a. For Protocol, select either **ESP** or **AH**.

b. Select a hash algorithm from the drop-down list.

c. Select an encryption algorithm from the drop-down list.

Encryption is available only when **ESP** is selected in Protocol.

d. For SPI Format, select either **DEC** or **HEX**.

e. In SPI for Inbound and SPI for Outbound, enter a value.

- If **DEC** is selected in SPI Format, enter a decimal value.
- If **HEX** is selected in SPI Format, enter a hexadecimal value.

f. For Key Format, select either **ASCII** or **HEX**.

g. In Authentication Key for Inbound and Authentication Key for Outbound, enter a value.

- If **ASCII** is selected in Key Format, enter an alphanumeric value.
- If **HEX** is selected in Key Format, enter a hexadecimal value.

h. In Encryption Key for Inbound and Encryption Key for Outbound, enter a value.

- Encryption Key for Inbound and Encryption Key for Outbound features are available only when **ESP** is selected in Protocol.
- Encryption Key for Inbound and Encryption Key for Outbound features are not available when **None** is selected in Encryption.
- If **ASCII** is selected in Key Format, enter an alphanumeric value.
- If **HEX** is selected in Key Format, enter a hexadecimal value.

4 Select **Submit**.

Protocol

This section includes advanced settings for various protocols used as the communication procedures and communication protocols.

You can set the following protocols:

- Print protocols
- Send protocols
- Other protocols

If the settings for the item marked with an asterisk (*) has been changed, you must restart the device or network. In the navigation menu, go to **Management Settings** > **Restart/Reset**.

Configuring protocol settings

1 In the navigation menu, select **Network Settings** > **Protocol**.

2 Specify the required settings for any of the following:

Print Protocols

This setting allows you to configure protocols for printing. For details, see *Configuring protocols for printing*.

Send Protocols

This setting allows you to configure protocols for sending email. For details, see *Configuring protocols for sending email*.

Other Protocols

This setting allows you to configure other network protocols. For details, see *Configuring other protocols*.

3 Select **Submit**.

Print Protocols

SMB Server Protocol

The SMB Server protocol allows peer-to-peer printing (SMB Print). With this protocol enabled, the machine is created in Windows Network Neighborhood. SMB Server protocol is an enhanced version of the NetBIOS protocol, which is used for the transport of SMB protocol. If the SMB Server protocol is set to **On**, the name resolution by NetBIOS (NMB) becomes available.

LPD

LPD is a protocol used to submit print jobs to a remote printer or a server.

FTP Server (Reception)

FTP is a communications protocol for transferring files over a network.

IPP

IPP is a protocol that sends and receives printed data and controls the printing device through TCP/IP networks of the internet and the like.

IPP over TLS

A certificate can be added for communication using the IPP protocol.

IPP Authentication

If IPP Authentication is set to **On**, the machine authenticates the user during printing to avoid unauthorized use.

Raw

Raw employs another method of printing over the network like LPR. Typically, Raw uses port 9100 to remotely administer the printer via using SNMP or MIB.

ThinPrint

Configure this setting whether to use ThinPrint.

ThinPrint over TLS

ThinPrint over TLS establishes secured communication between the printing systems and other devices.

WSD Print

WSD is a new networking protocol provided with Windows Vista for discovery of the machines and data exchange for printing.

POP3 (E-mail RX)

POP3 is a standard protocol used by local email clients to retrieve email from a remote server over a TCP/IP connection.

Configuring protocols for printing

1. In the navigation menu, select **Network Settings** > **Protocol**.
2. Do one or more of the following:

SMB Server Protocol

a. In SMB Server Protocol, select **On**.

b. Select an available network for SMB Server Protocol.

c. Specify the workgroup that you want to appear in **Windows Network Neighborhood** > **Entire Network**.

d. If necessary, set SMBv1 (Server) to **On**.

LPD

a. In LPD, select **On**.

b. Select an available network for LPD.

FTP Server (Reception)

a. In FTP Server (Reception), select **On**.

b. Select an available network for FTP Server (Reception).

IPP

a. In IPP, select **On**.

b. Select an available network for IPP.

c. Enter the port number. The default port number is 631.

IPP over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In IPP over TLS, select **On**.

b. Select an available network for IPP over TLS.

c. Enter the port number. The default port number is 443.

d. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

IPP Authentication

To enable this setting, go to **Management Settings** > **Authentication** > **Settings**. In Authentication, select **Local Authentication** or **Network Authentication**.

a. In IPP Authentication, select **On**.

b. Enter the default user name.

Raw

a. In Raw, select **On**.

b. Select an available network for Raw.

ThinPrint

ThinPrint is an optional protocol and is available only when installed.

a. In ThinPrint, select **On**.

b. Select an available network for ThinPrint.

c. Enter the port number. The default port number is 4000.

ThinPrint over TLS

- ThinPrint is an optional protocol and is available only when installed.
- To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In ThinPrint over TLS, select **On**.

b. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

WSD Print

a. In WSD Print, select **On**.

b. Select an available network for WSD Print.

POP3 (E-mail RX)

- To configure the POP3 protocol, go to **Function Settings** > **E-mail**.
- To use email printing, go to **Function Settings** > **Printer**. In Remote Printing, select **Permit**.

a. In POP3 (E-mail RX), select **On**.

b. In POP3 Security (User 1 to 3), select from the following:

- **STARTTLS**
- **TLS**
- **Off**

3 Select **Submit**.

Send Protocols

SMTP (E-mail TX)

SMTP is an Internet standard for email transmission across IP networks.

SMTP (FAX Server)

SMTP allows email transmission using the FAX server.

FTP Client (Transmission)

FTP is a standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

SMB

SMB is a network protocol applied to share access to files, printers, or serial ports.

WSD Scan

WSD is a new network protocol provided with Windows Vista for discovery of the machines and data exchange for printing.

eSCL

eSCL is a network protocol used for remote scanning from Mac OS X computer.

eSCL over TLS

A certificate can be added for communication using the eSCL protocol.

Configuring protocols for sending email

1 In the navigation menu, select **Network Settings** > **Protocol**.

2 Do one or more of the following:

SMTP (E-mail TX)

- To use these settings, enable TLS in **Security Settings** > **Network Security**.
- To configure the detailed settings, go to **Function Settings** > **E-mail**.

a. In SMTP (E-mail TX), select **On**.

b. In SMTP Security, select from the following:

- **STARTTLS**
- **TLS**
- **Off**

c. In Certificate Auto Verification, select the following in sequence:

1. **Validity Period**
2. **Server Identity**
3. **Chain**
4. **Revocation**

You can use more than one option at a time.

d. In Revocation Check Type, select from the following:

- **OCSP**
- **CRL**
- **CRL & OCSP**

e. For Hash algorithm, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

f. If necessary, set S/MIME to **On**.

SMTP (FAX Server)

- This feature is available only when FAX Server is set to **On** in **Function Settings** > **FAX**.
- To use these settings, enable TLS in **Security Settings** > **Network Security**.
- To configure the detailed settings, go to **Function Settings** > **E-mail**.

In SMTP Security, select from the following:

- **STARTTLS**
- **TLS**
- **Off**

FTP Client (Transmission)

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In FTP Client (Transmission), select **On**.

b. Enter the port number. The default port number is 21.

c. If necessary, set FTP Encryption TX to **On**.

d. In Certificate Auto Verification, select the following in sequence:

1. **Validity Period**
2. **Server Identity**
3. **Chain**
4. **Revocation**

You can use more than one option at a time.

e. In Revocation Check Type, select from the following:

- **OCSP**
- **CRL**
- **CRL & OCSP**

f. For Hash algorithm, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

SMB

a. In SMB, select **On**.

b. Enter the port number. The default port number is 445.

c. If necessary, do the following:

- Set SMBv1 to **On**.
- Set Use Temporary File Name to **On**.

WSD Scan

In WSD Scan, select **On**.

To use these settings, enable Available Network in WSD Print.

eSCL

a. In eSCL, select **On**.

b. Select an available network for eSCL.

eSCL over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In eSCL over TLS, select **On**.

b. Select an available network for eSCL over TLS.

c. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

3 Select **Submit**.

Other Protocols

SNMPv1/v2c

The SNMP protocol provides and transfers management information within the network environment. Should an error occur such as Add Paper, the machine automatically generates a trap, an error message sent to up to two predetermined trap recipients.

SNMPv3

The SNMP protocol provides and transfers management information within the network environment.

HTTP

HTTP is the protocol used to exchange or transfer hypertext between the World Wide Web and web browsers.

HTTPS

HTTPS is a widely used communications protocol for secure communication over the Internet. It provides bidirectional encryption of communications between a client web browser and a web server.

HTTP (Clientside)

You can configure HTTP for the client side.

Enhanced WSD

Enhanced WSD is an API that simplifies connections to web service-enabled devices, such as Printers, Scanners, and File Shares.

Enhanced WSD over TLS

Enhanced WSD over TLS is a communication security protocol that provides encryption, authentication, and anti-tampering integrity over the Internet.

LDAP

The machine can refer to the address book which is on the LDAP server as an external address book and assign a FAX number and email address to the destination.

IEEE802.1X

IEEE802.1X is a security protocol that allows login to the secured networks based on a client certificate.

LLTD

LLTD is a protocol that provides network topology discovery and quality of service diagnostics.

REST

REST is an architecture for the web application suitable for the multiple software linkage in the distributed network system.

REST over TLS

A certificate can be added for communication using the REST protocol.

VNC (RFB)

VNC (RFB) is set when starting a VNC Viewer, for example RealVNC, and using the Remote Operation.

VNC(RFB) over TLS

VNC (RFB) is set when starting a VNC Viewer, for example RealVNC, and using the Remote Operation protected by TLS.

Enhanced VNC(RFB) over TLS

Enhanced VNC(RFB) over TLS is a communication security protocol that provides encryption, authentication, and anti-tampering integrity over the Internet. This protocol is set when starting up Command Center RX, and using the Remote Operation protected by TLS.

OCSP/CRL Settings

You can configure the validity of certificates and specify the available CRL server address.

Syslog

When Syslog is set to **On**, you can communicate between client and SIEM server. By linking with the SIEM server, the security logs generated by security devices and network devices are collected and centrally managed by the SIEM server. The server analyzes the contents of multiple logs across the log and automatically detects correlated activities, and notifies clients of external attacks and threats based on the analysis results.

Configuring other protocols

1. In the navigation menu, select **Network Settings** > **Protocol**.
2. Do one or more of the following:

SNMPv1/v2c

To configure the detailed settings, go to **Management Settings** > **SNMP**.

a. In SNMPv1/v2c, select **On**.

b. Select an available network for SNMPv1/v2c.

This setting is commonly used with SNMPv1/v2c and SNMPv3.

SNMPv3

- To configure the detailed settings, go to **Management Settings** > **SNMP**.
- To use these settings, enable Available Network in SNMPv1/v2c.

In SNMPv3, select **On**.

HTTP

a. In HTTP, select **On**.

b. Select an available network for HTTP.

HTTPS

To use these settings, enable TLS in **Security Settings** > **Network Security**, and Available Network in IPP over TLS.

a. In HTTPS, select **On**.

b. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

HTTP (Clientside)

a. In Certificate Auto Verification, select the following in sequence:

1. **Validity Period**
2. **Server Identity**
3. **Chain**
4. **Revocation**

You can use more than one option at a time.

b. In Revocation Check Type, select from the following:

- **OCSP**
- **CRL**
- **CRL & OCSP**

c. For Hash algorithm, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

d. Set Use Default Settings to **On** to use default machine settings for the following:

If Use Default Settings is set to **Off**, you need to configure the settings manually.

- Remote Services
- Universal Print
- OAuth2 (Exchange online(Reception))
- OAuth2 (Exchange online(Transmission))
- SOAP
- Cloud Access

Enhanced WSD

a. In Enhanced WSD, select **On**.

b. Select an available network for Enhanced WSD.

Enhanced WSD over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In Enhanced WSD over TLS, select **On**.

b. Select an available network for Enhanced WSD over TLS.

c. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

LDAP

- To configure the External Address Book, go to **Address Book** > **External Address Book Settings**.
- To configure advanced settings, go to **Management Settings** > **Authentication**.

a. In LDAP, select **On**.

b. In External Address Book (1 to 8) and Network Authentication, select from the following:

- **STARTTLS**
- **TLS**
- **Off**

To use these settings, enable TLS in **Security Settings** > **Network Security**.

c. In Certificate Auto Verification, select the following in sequence:

1. **Validity Period**
2. **Server Identity**
3. **Chain**
4. **Revocation**

You can use more than one option at a time.

d. In Revocation Check Type, select from the following:

- **OCSP**
- **CRL**
- **CRL & OCSP**

e. For Hash algorithm, select either **SHA1** or **SHA2(256/384)**.

You can use more than one algorithm at a time.

IEEE802.1X

a. In IEEE802.1X, select **On**.

b. In IEEE802.1X Settings, select **Settings**.

To configure the detailed settings, see *IEEE802.1X* and *Certificate Status*.

LLTD

a. In LLTD, select **On**.

b. Select an available network for LLTD.

REST

a. In REST, select **On**.

b. Select an available network for REST.

c. Enter the port number. The default port number is 9080.

REST over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In REST over TLS, select **On**.

b. Select an available network for REST over TLS.

c. Enter the port number. The default port number is 9081.

d. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

VNC (RFB)

a. In VNC (RFB), select **On**.

b. Select an available network for VNC (RFB).

c. Enter the port number. The default port number is 9062.

VNC(RFB) over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In VNC(RFB) over TLS, select **On**.

b. Select an available network for VNC(RFB) over TLS.

c. Enter the port number. The default port number is 9063.

d. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

Enhanced VNC(RFB) over TLS

To use these settings, enable TLS in **Security Settings** > **Network Security**.

a. In Enhanced VNC(RFB) over TLS, select **On**.

b. Select an available network for Enhanced VNC(RFB) over TLS.

c. Enter the port number. The default port number is 9061.

d. To make advanced settings, select **Settings**, then select a certificate.

If necessary, review or modify the device certificate in **Security Settings** > **Certificates**.

OCSP/CRL Settings

a. In OCSP/CRL Settings, select **Settings**.

b. In General, enter the revocation information cache period.

c. In OCSP, do the following:

1. Set Auto Server Selection with AIA Information to **On**.

   You can use this setting to select the server automatically using AIA.

2. Enter the specific information for the following:
   - Number of available OCSP URL
   - Server address
   - Timeout
3. In Proxy, select **Settings**.
4. In Proxy Authentication, enter the user name and password.
5. In NONCE Extension, select **On**.

   You can use this setting to communicate to the server using a one-time token.

6. Set Response Signing Check to **On** to check signing of certificates.
7. Set Validity Period Check to **On** to check the validity of certificates.
8. Enter your preferred retry period and retry count.
9. In Unknown Certificate, select either **Reject** or **Permit**.

d. In CRL, do the following:

1. Set Auto Server Selection with CDP to **On**.

   This setting is used to select the server automatically using CDP.

2. Enter the specific information for the following:
   - Number of Available CRL URL
   - Server Address
   - Timeout
3. In Proxy, select **Settings**.
4. In Proxy Authentication, enter the user name and password.

When using LDAP server, enter the user name (LDAP) and password (LDAP).

5. Enter your preferred retry period and retry count.

Syslog

To configure the detailed settings, go to **Management Settings** > **History Settings**.

a. In Syslog, select **On**.

b. In Connection Type, select either **UDP** or **TCP**.

If you select **TCP**, you can set Syslog Security to **On**.

3 Select **Submit**.

Wireless LAN

This section includes advanced settings for Wi-Fi and Wi-Fi Direct.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the device or network. In the navigation menu, go to **Management Settings** > **Restart/Reset**.

Wi-Fi Settings

1 In the navigation menu, select **Network Settings** > **Wireless LAN**.

2 Specify the required settings for any of the following:

Wi-Fi

Select **On** to use Wi-Fi for wireless LAN communication.

Network Name (SSID)

Enter the SSID of the wireless LAN.

Network Authentication

Select a network authentication method from the drop-down list.

Encryption

To configure the encryption method, do any of the following:

- If you select **Open** in Network Authentication, select **Disable** or **WEP**.
- If you select **WPA2/WPA-PSK** or **WPA2/WPA-EAP** in Network Authentication, select **AES** or **Auto**.
- If you select **WPA2-PSK**, **WPA2-EAP**, **WPA3-SAE/WPA2-PSK**, **WPA3-SAE**, **WPA3/WPA2-EAP**, or **WPA3-EAP** in Network Authentication, AES is applied as Encryption.

WEP Key Index

Select the WEP Key Index when you select **Open** in Network Authentication and **WEP** in Encryption.

WEP Key

Enter the WEP Key when you select **Open** in Network Authentication and **WEP** in Encryption.

Pre-shared Key

Enter the Pre-shared Key when you select **WPA2/WPA-PSK** or **WPA2-PSK** in Network Authentication.

Automatic Channel Control

Select **On** to use automatic channel control.

3 Select **Submit**.

IEEE802.1X

This setting shows if you select **WPA2/WPA-EAP**, **WPA2-EAP**, **WPA3/WPA2-EAP**, or **WPA3-EAP** in Network Authentication.

1 In the navigation menu, select **Network Settings** > **Wireless LAN**.

2 Specify the required settings for any of the following:

Effective Encryption

Select an encryption method from the following:

- **EAP-TLS**
- **EAP-TTLS**
- **EAP-FAST**
- **PEAP(EAP-MS-CHAPv2)**

Tunneled Authentication Protocol

Select a method of authentication from **MSCHAPV2**, **MSCHAP**, **CHAP**, and **PAP** on the drop-down list.

This protocol is available only when **EAP-TTLS** is selected for encryption.

Login User Name

Enter the name of the user to access the machine.

The IEEE802.1X Client Certificate of this user must be valid.

Password

Enter the password.

This protocol is available only when **EAP-TTLS**, **EAP-FAST**, or **PEAP(EAP-MSCHAPv2)** is selected for encryption.

Common Name

Specify the common name of the server certificate if the server is required to be authenticated.

This protocol is available only when **EAP-TTLS**, **EAP-FAST**, or **PEAP(EAP-MSCHAPv2)** is selected for encryption.

Match Rule of Common Name

When the server certificate is verified, the common name specified under Common Name is compared with the common name on the server certificate. This item allows you to specify whether the common names are considered to be matched if they exactly or partially match.

This protocol is enabled when **EAP-TTLS**, **EAP-FAST**, or **PEAP (EAP-MSCHAPv2)** has been selected for encryption.

Expiration Verification

Set Expiration Verification to **On**.

- When enabled, the expiration of the server certificate is verified.
- If the certificate is expired then Command Center RX cannot communicate with the printing system.

IEEE802.1X Client Certificate

The current status is shown in IEEE802.1X Client Certificate. To make advanced settings, select **Settings** and select a device certificate. Select **Submit** to finish settings. Configure the Device Certificate on the Certificates page under Security Settings.

3 Select **Submit**.

Certificate Status

1 In the navigation menu, select **Network Settings** > **Wireless LAN**.

2 Specify the required settings for any of the following:

Root Certificate (1 to 5)

Displays the current status of the root certificates.

To configure the detailed settings, go to **Security Settings** > **Certificates**.

IEEE802.1X Client Certificate

Displays the current status of the IEEE802.1X client certificate.

To configure the detailed settings, go to **Security Settings** > **Certificates**.

Wi-Fi Direct Settings

1. In the navigation menu, select **Network Settings** > **Wireless LAN**.
2. Specify the required settings for any of the following:

Wi-Fi Direct

Select **On** when using Wi-Fi Direct for wireless LAN communication.

Frequency Band

Select either **2.4 GHz** or **5 GHz** as the frequency band.

This feature is available only in some machines.

Device Name

Enter the device name.

IP Address

Displays the IP address of the device.

Persistent Group

Do either of the following:

- To use persistent group, select **On**.
- To reset the password for Wi-Fi Direct connection, select **Reset**.

- This option is available only when Auto Generation is selected in Password.
- To confirm the password, do either of the following:
  - Go to **Device Information / Remote Operation** > **Configuration** > **Network (Wireless LAN)**.
  - Go to the network status in the control panel of the machine.

Password

Do any of the following:

- Select **Auto Generation** to generate the Wi-Fi Direct password automatically.
- Select **Manual Creation** to create the password manually.

Restart the device or network to apply the changes to the setting.

Auto Disconnect

Do the following:

a. To automatically disconnect the handheld device connected using Wi-Fi Direct, select **On**

b. Specify the value for the following:

- Day
- Hour
- Minute

3 Select **Submit**.

9 Security Settings

This page is accessible when you have logged in the embedded server with administrator rights while network authentication or local authentication is enabled.

If necessary, make the following settings:

- Device Security
- Send Security
- Network Security
- Certificates

Device Security

This section includes settings for device security.

Quick Setup

This section allows you to configure the security level for the device.

1. In the navigation menu, select **Security Settings** > **Device Security**.
2. Specify the required settings for any of the following:

Status of Security Settings

Displays the security level configured in Security Quick Setup.

Security Quick Setup

Select **Settings** to open Quick Setup. Then, select from the following:

Level 1

This is the factory default setting.

Level 2

The network security functions are changed.

Level 3

All functions that protect the device are enabled, while functions that do not protect the device are disabled.

For more details on each security level, refer to the machine's *Operation Guide*.

Allowlisting

Select **On** to prevent unauthorized software execution and software tampering and to maintain system reliability.

Make sure to restart the device after setting this function to **On**. Enabling this function will slow down device startup.

To make it easier to understand the contents when a malicious program is detected, enable Notify when Malicious Program is Detected. For details, see *Notification/Report Settings*.

3 Select **Submit**.

Interface Block

This section allows you to restrict access from each interface.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Network

Access cannot be restricted from the network interface. Access should be restricted depending on the protocol.

To configure the detailed settings, go to **Network Settings** > **Protocol**.

USB Device

Select **Block** to block access from devices connected to the USB port.

USB Host

Select **Block** to block access from USB host devices.

USB Drive

Select **Block** to block access from storage drives connected to the USB port.

3 Select **Submit**.

Lock Operation Panel

This section allows you to restrict access from the operation panel.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 As necessary, set the following from the Operation Panel drop-down list:

Lock

Settings related to input/output, jobs, and paper are prohibited. To set partial locks, select from the following:

Partial Lock 1

Settings related to input/output such as network settings, system settings, and document settings are prohibited. These include registering and editing the address book and document box.

Partial Lock 2

In addition to the Partial Lock 1 restrictions, settings related to run jobs such as panel settings and printer settings are prohibited. These include using stop keys and canceling jobs.

Partial Lock 3

In addition to the Partial Lock 2 restrictions, settings related to paper are prohibited. These include cassette settings and MP Tray settings.

Unlock

All keys and settings are allowed.

3 Select **Submit**.

Job Status/Job Logs Settings

This section allows you to restrict access to job status, job logs, and FAX history.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Display Jobs Detail Status

You can set restrictions for viewing the progress of all jobs in detail. Select **Hide All** to restrict viewing of jobs status to administrators only. Select **Show All** to allow all users to view the jobs status. Select **My Jobs Only** to filter jobs status for the current user only.

Display Jobs Log

You can set restrictions for viewing the job history. Select **Hide All** to restrict viewing of jobs log to administrators only. Select **Show All** to allow all users to view the jobs log. Select **My Jobs Only** to filter jobs log for the current user only.

Display FAX Log

You can set restrictions for viewing the FAX history. Select **Hide All** to restrict viewing of FAX logs to administrators only. Select **Show All** to allow all users to view the FAX logs.

Pause/Resume of All Print Jobs

Select **Permit** to pause all jobs including jobs that are currently printing. Printing will resume when selecting the option again.

Remaining Print Jobs on Logging out

Select either **Cancel** or **Continue**.

3 Select **Submit**.

Edit Restriction

This section allows you to set restrictions for adding, editing, and deleting the address book and one touch key.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Address Book

Select **Off** to allow all users to edit the address book. Select **Administrator Only** to allow only users with administrator rights to edit the address book.

One Touch Key

Select **Off** to allow all users to edit the one touch key. Select **Administrator Only** to allow only users with administrator rights to edit the one touch key.

3 Select **Submit**.

Authentication Security Settings

This section allows you to configure passwords and user accounts for security.

These settings can be made when local authentication is enabled.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Password Policy Settings

You can configure settings for password policy.

Password Policy

Select **On** to enable settings for password policy.

Maximum password age

Select **On** to set the password validity period. Select a value from 1 to 180 days.

Minimum password length

Select **On** to set the minimum number of characters required for the password. Select a value from 1 to 64 characters.

Password complexity

To set rules for password complexity, select from the following:

- **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

Select **User List** to display a list of users in violation of the password policy.

User Account Lockout Settings

You can configure settings to exclude specific user accounts.

Lockout Policy

Select **On** to enable settings for lockout policy.

Number of Retries until Locked

Set the number of password retries until a user account is locked. Select a value from 1 to 10 times.

Lockout Duration

Set the time period during which a user account is locked. Select a value from 1 to 60 minutes.

Lockout Target

Set the target users for lockout. Select either **All** or **Remote Login Only**.

Locked out Users List

Select **User List** to display a list of users that are currently locked.

3 Select **Submit**.

Unusable Time Settings

This section allows you to set the time period during which the machine is restricted for use.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Unusable Time

Select **On**. When Unusable Time is set to **On**, the machine is restricted for the duration specified in Start Time and End Time. To use the machine during this time period, an unlock code must be entered.

Start Time

Set the start time for restricting machine use.

End Time

Set the end time for restricting machine use.

Unlock Code

Enter a decimal value from 0000 to 9999. You can use this unlock code to temporarily deactivate unusable time.

3 Select **Submit**.

Data Sanitization

This section allows you to reset data registered in the machine to factory default settings.

The data may vary depending on the device model.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Reserve a Sanitization Time

Select **On** and set the schedule for data sanitization. When this is enabled, all address information and image data stored in the machine will be deleted during the specified schedule.

Device Use After Sanitization

Select either **Prohibit** or **Permit** to restrict machine use after data sanitization.

3 Select **Submit**.

Firmware Update

This section allows you to configure the firmware update settings.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 Specify the required settings for any of the following:

Administrator Authentication on Firmware Update

To enable, select **On**.

Firmware Update Tool

To enable, select **On**.

3 Select **Submit**.

Data Import/Export

This section allows you to configure the data import/export settings.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 In Administrator Authentication on Data Import/Export, select **On**.

3 Select **Submit**.

Secure Boot

This section allows you to configure the secure boot settings.

1 In the navigation menu, select **Security Settings** > **Device Security**.

2 In Secure Boot, select either **BIOS + Firmware** or **BIOS**.

3 Select **Submit**.

Send Security

This section includes security settings for sending.

1 In the navigation menu, select **Security Settings** > **Send Security**.

2 Specify the required settings for any of the following:

Dest. Check before Send

To enable the front panel message which prompts you to confirm the destination to forward the scan data, select **On**. The message is displayed when you press the **Start** key of the machine to start scanning.

Entry Check for New Dest.

To determine whether re-entry of a destination for confirmation is required when adding a new destination, select **On**.

Destination Check on Selecting

To enable, select **On**.

New Destination Entry

To determine whether an entry of a new destination is allowed, do the following:

- To enable the entry of a new destination, select **Permit**.
- To disable the entry of a new destination, select **Prohibit**.

New Destination Entry (FAX)

If New Destination Entry is enabled, do the following:

- To enable the entry of a new fax destination, select **Permit**.
- To disable the entry of a new fax destination, select **Prohibit**.

Recall Destination

To permit or prohibit using recall destination, do the following:

- To enable the entry of a destination to recall, select **Permit**.
- To disable the entry of a destination to recall, select **Prohibit**.

Broadcast

To permit or prohibit broadcast, do the following:

- To enable the broadcast transmission, select **Permit**.
- To disable the broadcast transmission, select **Prohibit**.

3 Select **Submit**.

Network Security

This section includes settings for network security.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the device or network. In the navigation menu, go to **Management Settings** > **Restart/Reset**.

Secure Protocol Settings

1 In the navigation menu, select **Security Settings** > **Network Security**.

2 Specify the required settings for any of the following:

TLS

TLS is a cryptographic protocol that provides communication security between a computer and the machine. This setting allows you to enable TLS protocol for communication. For details, see *Configuring TLS*.

Serverside Settings

This setting allows you to configure settings on the server side. For details, see *Configuring serverside settings*.

Clientside Settings

This setting allows you to configure settings on the client side. For details, see *Configuring clientside settings*.

3 Select **Submit**.

Configuring TLS

1 In the navigation menu, select **Security Settings** > **Network Security**.

2 To enable the TLS protocol, set TLS to **On**.

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

3 Select **Submit**.

Configuring serverside settings

1 In the navigation menu, select **Security Settings** > **Network Security**.

2 Specify the required settings for any of the following:

TLS Version

TLS is a cryptographic protocol that provides communication security between a computer and the machine. Select the TLS version from the following:

- **TLS1.0**
- **TLS1.1**
- **TLS1.2**
- **TLS1.3**

You can use more than one version at a time.

Effective Encryption

Select an encryption algorithm from the following:

- **ARCFOUR**
- **DES**
- **3DES**
- **AES**
- **AES-GCM**
- **CHACHA20/POLY1305**

You can use more than one algorithm at a time.

Hash

Select either **SHA1** or **SHA2(256/384)** for the hash algorithm.

You can use more than one algorithm at a time.

HTTP Security

Specifies the security level for HTTP. Select either of the following:

Secure Only (HTTPS)

Encrypts all HTTP protocol communications. Only the URLs that begin with https:// are accessible. If a URL beginning with http:// is specified, it will be automatically redirected to "https://".

Not Secure (HTTPS & HTTP)

Enables access for both encrypted and unencrypted HTTP protocol communication. URLs beginning with either "https://" or "http://" are accessible. The former URL establishes encrypted communication and the latter establishes unencrypted communication.

IPP Security

Specifies the security level for IPP. Select either of the following:

Secure Only (IPPS)

Encrypts all HTTP protocol communications.

Not Secure (IPPS & IPP)

Enables access for both encrypted and unencrypted IPP protocol communications.

Enhanced WSD Security

Specifies the security level for Enhanced WSD. Select either of the following:

Secure Only (Enhanced WSD over TLS)

Encrypts all Enhanced WSD over TLS protocol communications.

Not Secure (Enhanced WSD over TLS & Enhanced WSD)

Enables access for both Enhanced WSD over TLS and Enhanced WSD protocol communications.

eSCL Security

Specifies the security level for eSCL. Select either of the following:

Secure Only (eSCL over TLS)

Encrypts all eSCL over TLS protocol communications.

Not Secure (eSCL over TLS & eSCL)

Enables access for both eSCL over TLS and eSCL protocol communications.

REST Security

Specifies the security level for REST. Select either of the following:

Secure Only (REST over TLS)

Encrypts all REST over TLS protocol communications.

Not Secure (REST over TLS & REST)

Enables access for both REST over TLS and REST protocol communications.

3 Select **Submit**.

Configuring clientside settings

1 In the navigation menu, select **Security Settings** > **Network Security**.

2 Specify the required settings for the following:

TLS Version

TLS is a cryptographic protocol that provides communication security between a computer and the machine. Select the TLS version from the following:

- **TLS1.0**
- **TLS1.1**
- **TLS1.2**
- **TLS1.3**

You can use more than one version at a time.

Effective Encryption

Select an encryption algorithm from the following:

- **ARCFOUR**
- **DES**
- **3DES**
- **AES**
- **AES-GCM**
- **CHACHA20/POLY1305**

You can use more than one algorithm at a time.

Hash

Select either **SHA1** or **SHA2(256/384)** for the hash algorithm.

- You can use more than one algorithm at a time.
- When more than one algorithm is selected, the machine selects one algorithm to automatically connect to the server.
- When the TLS is set to **On** and HTTP Security is set to **Secure Only (HTTPS)**, the document boxes cannot be accessed by the TWAIN driver.

3 Select **Submit**.

Network Access Settings

1 In the navigation menu, select **Security Settings** > **Network Security**.

2 Specify the required settings for any of the following:

Filtering/Firewall

Filtering and firewall settings can restrict the network access to the device so that only the specific network addresses are allowed. For details, see *IP Filter(IPv4) Settings* and *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. For details, see *SNMP*.

SNMPv3

The SNMPv3 communication settings are used to control the authentication and encryption communication that occur via SNMP. For details, see *SNMP*.

TLS

To enable TLS, settings for Secure Protocols must be made. For details, see *Network Security*.

IEEE802.1X

To enable IEEE802.1X, you must first make the IEEE802.1X settings. For details, see *IEEE802.1X*.

IPSec

To enable IPSec, you must first make the IPSec settings. For details, see *TCP/IP*.

3 Select **Submit**.

Certificates

This section allows you to create, update, or review details on a certificate. After you have changed this setting, you must restart the network or this machine.

When you open the Command Center RX via https, you will be asked to confirm the security certificate for the website. To change this setting, you can configure the certificate settings through the following:

- Temporary solution: Confirm the security certificate every time the notification is displayed when accessing the Command Center RX.
- Permanent solution: Import the device certificate or root certificate as a trusted certificate into your computer. The web browser will automatically authenticate the Command Center RX certificate.

You can set the following certificates:

- Device Certificate
- Root Certificate

If the settings for the item marked with an asterisk (*) has been changed, you must restart the device or network. In the navigation menu, go to **Management Settings** > **Restart/Reset**.

Device Certificate

This section allows you to configure device certificates.

1. In the navigation menu, select **Security Settings** > **Certificates**.
2. A list of the device certificates will be shown, allowing you to check the following:

   Device Certificate 1 is automatically issued by default. The automatically issued certificate has the country code, common name, and a validity period of about 5 years already configured.

   Status
   Displays whether the certificate is active.

   Subject
   Displays the country code and common name.

   Expiration
   Displays the validity period of the certificate.

   Protocols in Use
   Displays the protocols available (ThinPrint, HTTPS/IPP over TLS, Enhanced WSD over TLS, Other Protocols, eSCL over TLS, REST over TLS, VNC(RFB) over TLS, Enhanced VNC(RFB) over TLS, and S/MIME).

   Function in Use
   Displays the functions used by the device certificate.

3. Specify the required settings for any of the following:

   Device Certificate (1 to 5)
   This section allows you to modify the initial settings, add a new one, and delete the existing settings.

   Select **Settings**. The Device Certificate (1 to 5) page opens to show the current status. If necessary, configure the following:

   Status
   Displays whether the certificate is active.

Expiration

Displays the validity period of the certificate.

View Certificate

Select **View** to view the details of the certificate.

Create Self Certificate

Select **Create** to create a certificate. Configure the following:

- Country Code
- State/Province
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- E-mail Address
- subjectAltName
- Current Universal Time (UTC/GMT)
- Validity Period
- Key Encryption
- Key Length

- Key Length is the information needed to generate encryption.
- When **RSA** is selected in Key Encryption, select **1024 bit**, **2048 bit**, or **4096 bit** in Key Length.
- When **ECDSA** is selected in Key Encryption, select **256 bit**, **384 bit**, or **521 bit** in Key Length.
- After entering the certificate details, make sure to select **Submit** to finish settings.

Import Certificate

Select **Import** on an inactive device certificate. Select **Choose File** to browse for the certificate file, and then select **Open**. Enter the password, then select **Submit**.

Edit Certificate

Select **Edit** on an active device certificate. The Current Universal Time (UTC/GMT) is displayed. Enter the validity period, then select **Submit** to finish settings.

Delete Certificate

Select **Delete** to delete the device certificate.

Export Certificate

Select **Export** to save the device certificate on your computer.

Create Certificate Signing Request

Select **Create** on an inactive device certificate to create a certificate signing request. Configure the following:

- Country Code
- State/Province
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- E-mail Address
- subjectAltName
- Key Encryption
- Key Length

- Key Length is the information needed to generate encryption.
- When **RSA** is selected in Key Encryption, select **1024 bit**, **2048 bit**, or **4096 bit** in Key Length.
- When **ECDSA** is selected in Key Encryption, select **256 bit**, **384 bit**, or **521 bit** in Key Length.
- After entering the certificate details, make sure to select **Submit** to finish settings.

Retrieve Certificate via SCEP

Select **Retrieve** to retrieve the device certificate via SCEP server.

Retrieving device certificates via SCEP server

1. In the navigation menu, select **Security Settings** > **Certificates**.
2. Select **Settings** on an inactive device certificate.
3. Select **Retrieve** to retrieve a device certificate via SCEP server.
4. In CA Server Address, enter `http://123.123.123.123/certsvc/mscep/mscep.dll`, where 123.123.123.123 is the hostname or IP address of the CA server.
5. To get the CA challenge password, from a web browser, enter `http://123.123.123.123/certsvc/mscep_admin/`, where 123.123.123.123 is the hostname or IP address of the CA server.

   Authentication is necessary for acquiring the password. If the challenge password is not included in the link, the challenge password is not required.

6. In CA Challenge Password, enter the obtained password.

7 In SCEP Server Settings, specify the required settings for any of the following:

CA Server Certificate(s) Verification

Select **On** to verify whether the CA server certificate is enabled.

Issued-device Certificate Verification

Select **On** to verify whether the issued-device certificate is enabled.

Timeout

Enter the CA server timeout in minutes. The server will be disconnected if there is no response within the specified time.

Proxy

Configure whether to enable SCEP communication via HTTP proxy or HTTPS proxy. Select **Settings** or go to **Network Settings** > **TCP/IP**. Then, in Proxy settings, set Proxy to **On**.

To configure the detailed settings, refer to *Proxy Settings*.

Proxy Authentication

Enter the user name and password when using the proxy server.

Auto Renewal

Select **On** to automatically obtain the CA server certificate when the renewal period expires.

Renewal Period

Enter the renewal period for the certificate.

8 If necessary, specify the required settings in CSR Settings.

The certificate generated automatically in this machine does not have the signature of the CA. Therefore, depending on the communications partner, a communication error may occur. The data of the certificate signing request is required for the issue of a certificate signed by the CA. The CSR can be generated by the administrator from the Command Center RX.

The country code and generic name are automatically displayed. Other fields should be entered as required.

Country Code

Enter the country code. The country code where the certificate will be used is specified by default.

State/Province

Enter the name of the state or province where you reside.

Locality Name

Enter the locality name where you reside.

Organization Name

Enter your organization name.

Organization Unit Name

Enter your department name.

Common Name

Enter the general name of the device. The host name of the device is specified by default.

E-mail Address

Enter your email address.

subjectAltName

Specify the Subject Alternative Name (SANs) for the CA server certificate. You can specify a maximum of five identifiers, such as the domain name and IP address of the CA server. Select **None**, **E-mail Address**, **DNS**, **IPv4**, or **IPv6** from the drop-down list. If you select a value other than **None**, you can enter an identifier.

Current Universal Time (UTC/GMT)

Displays the standard time for the operating system where the Command Center RX is running.

Key Length

Select a key length from the drop-down list.

9 Select **Submit**, and then select **OK**.

The certificate settings are displayed in a list.

There is a waiting period before the certificate is received.

10 Review the contents, then select **Submit**.

11 To apply settings, restart the device.

For more details on restarting the device, see *Restart*.

Root Certificate

This section allows you to configure root certificates.

1 In the navigation menu, select **Security Settings** > **Certificates**.

2 In Root Certificate (1 to 5), select **Settings**.

3 Specify the required settings for any of the following:

Status

Displays whether the certificate is active or inactive.

Expiration

Displays the validity period of the certificate.

Import Certificate

Select **Import** on a root certificate. Select **Choose File** to browse for the certificate file, and then select **Open**. Make sure to select **Submit** after importing a root certificate.

4 If necessary, you can delete Root Certificate (2 to 5) by selecting **Delete** for the specified root certificate.

A certificate can be assigned to a protocol or a configuration.

10 Management Settings

This page is accessible when you have logged in the embedded server with administrator rights while network authentication or local authentication is enabled.

If necessary, make the following settings:

- Job Accounting
- Authentication
- ID Card
- Notification/Report
- History Settings
- SNMP
- Restart/Reset
- Remote Operation

Job Accounting

This section includes advanced settings for Job Accounting.

Settings

To use Job Accounting, you must first configure the Job Accounting settings.

1. In the navigation menu, select **Management Settings** > **Job Accounting**.
2. Select **Settings**. Specify the required settings for any of the following:

Job Accounting

Select **On** to enable Job Accounting.

Job Accounting Access

Select **Local** to use Job Accounting through local authentication.

Select **Network** to use Job Accounting through network authentication.

To select **Network**, network authentication must be enabled and **Ext.** must be selected for server type.

Action Settings

Specify required settings for any of the following:

Apply Limit

Set the behavior of processing a job when you reach the maximum number of print pages. Select from the following:

- **Immediately**
- **Subsequently**
- **Alert Only**

Copy/Printer Count

Select **Total** to display the total count for both copy and print jobs.

Select **Individual** to display the total copy job count and total print job count separately.

Unknown ID Job

Displays the behavior of processing a job with an unknown or missing account ID.

To configure the detailed settings, go to **Management Settings** > **Authentication** > **Settings**. In Unknown ID Job, select either **Permit** or **Reject**.

3 If necessary, configure the Default Counter Limit. Enter a value from 1 to 9999999 for each counter limit.

This feature is available only when Job Accounting is enabled.

4 Select **Submit**.

Local Job Accounting List

This section includes settings for adding and deleting an account and for departmental accounting.

Add Account

To aggregate pages either by department or by all departments, accounts must be added.

1 Select **Add Account**.

2 You can configure settings for Account Property. Specify the required settings for any of the following:

Account Name

Enter the Account Name.

Account ID

Enter the Account ID.

3 You can configure settings for Restriction. To set restrictions for each function, do the following:

a. Select from the following:

- **Off**
- **Counter Limit**
- **Reject Usage**

b. Enter a decimal value from 1 to 9999999.

4 Select **Submit**.

Delete

1 Select the checkbox to the left of the Account ID. To select all items at once, select **Check All**.

2 Select **Delete**.

Counter

1 Select the checkbox to the left of Account ID.

2 Select **Counter** next to the account name.
The total number of copies for the selected account is displayed.

3 You can view the summary of results for the following:

Printed Pages

Select either **Printed Pages by Function** or **Printed Pages by Layout** from the drop-down list.

Scanned Pages

Shows the total pages scanned using Copy, FAX, and Other Scan.

FAX Counter

Shows both the total pages and total time for FAX transmission.

Counter Reset

Select **Reset** to reset the counters.

4 Select **Counter** in Other Account or Total Account to view the summary of results for the following:

Other Account

The total number of copies for other accounts is displayed.

Total Account

The total number of copies for all accounts is displayed.

Authentication

This section includes advanced settings for authentication.

You can configure the following:

- Settings
- Local User List

Settings

To use authentication, you must first configure the authentication settings.

1. In the navigation menu, select **Management Settings** > **Authentication**.
2. Select **Settings**, and then in Authentication, select from the following:

   Off

   This option disables the authentication settings.

   Local Authentication

   This option allows you to configure the local authentication settings. For details, see *Configuring local authentication settings*.

   Network Authentication

   This option allows you to configure the network authentication settings. For details, see *Configuring network authentication settings*.
3. Select **Submit**.

Configuring local authentication settings

1. In the navigation menu, select **Management Settings** > **Authentication**.
2. Select **Settings**, and then in Authentication, select **Local Authentication**.
3. Do one or more of the following:

   Local Authorization Settings

   For Local Authorization, select either **On** or **Off**.

   Guest Authorization Settings

   For Guest Authorization, select either **On** or **Off**.

   Guest Settings

   a. Select **Guest Settings**.

   b. Enter your user name.

   c. For Access Level, select either **Administrator** or **User**.

d. Review or modify the account name. Select **Account List** to use a different account name, and then select **Submit**.

e. Review or modify the restrictions set for each function.

Unknown User Settings

a. For Unknown ID Job, select either **Reject** or **Permit**.

b. To configure the detailed settings, select **Unknown User Settings**.

c. Enter a user name.

d. Review or modify the account name. Select **Account List** to use a different account name, and then select **Submit**.

Account Name is displayed when Job Accounting is set to **On**.

e. For Print Restriction, select either **Off** or **Reject Usage**.

Simple Login Settings

For Simple Login, select either **On** or **Off**.

Simple Login Key List

a. Select **Simple Login Key List**.

b. To configure Key (1 to 20), select **Settings**.

c. Enter a display name.

d. Select a display icon from the drop-down list.

e. For password, select either **On** or **Off**.

f. For Authentication, select either **Local Authentication** or **Network Authentication**.

g. When **Local Authentication** is selected, review or modify the current user. Select **User List** to select a different user, then select **Submit**.

h. When **Network Authentication** is selected, enter the login user name and password. Then, select a domain from the drop-down list.

Quick Job Printing

This feature is available only when either **NTLM** or **Kerberos** is selected in Server Type.

a. For Display List on Login, select either **On** or **Off**.

b. For the following items, select either **On** or **Off**:

- Logout after Printing

- Skip Password and Copies Confirmation

Universal Print Settings

Select **On** to link with cloud print.

4 Select **Submit**.

Configuring network authentication settings

1 In the navigation menu, select **Management Settings** > **Authentication**.

2 Select **Settings**, and then in Authentication, select **Network Authentication**.

3 Do one or more of the following:

Network Authentication Server

a. Enter the host name or IP address of the network authentication server.

If you entered the host name, make sure that the DNS server information is specified.

b. Enter the port number of the network authentication server.

c. Select the server type from the drop-down list.

When using ID Card, select **Ext.** as server type.

d. If necessary, configure certificate verification setting in **Network Settings** > **Protocol**.

Certificate Verification Setting is available only when **Ext.** is selected as server type.

e. Select the default domain from the drop-down list.

f. To configure the detailed settings, select **Domain List**. Configure the following settings:

- Use Multiple Authentication Server
- Default Host Name

- When Use Multiple Authentication Server is set to **Off**, you can only use the authentication server of the default domain.
- When Use Multiple Authentication Server is set to **On**, you can register a primary server and a secondary server for each domain. Each domain is referred to in the order of the primary server and secondary server.
- If you set the Default Host Name, each domain is referred to in the order of the default host name, primary server, and secondary server.

PIN Login Settings

This feature is available only when **Ext.** is selected as server type.

For PIN Login, select either **On** or **Off**.

Network User Authority

a. For Obtain Network User Property, select either **On** or **Off**.

b. To configure the detailed settings, select **Server Settings**.

c. Confirm that LDAP is set to **On**.

To enable this setting, go to **Network Settings** > **Protocol**.

d. Enter the LDAP server name or IP address, and then enter the port number.

e. Enter the search timeout in seconds.

f. If necessary, configure LDAP Security settings in **Network Settings** > **Protocol**.

g. In Acquisition of User Information, enter Name 1, Name 2, or E-mail address.

h. Select **Submit**, and then select **Back**.

i. For Give Local User Authority, select either **On** or **Off**.

j. For User Full Action, select either **Do Not Add New User** or **Delete Old User**.

k. For Authority When Offline, select either **Specify Enabled Period** or **Always Enabled**.

If you select **Specify Enabled Period**, you can select the number of days from 1 to 180.

l. To configure the detailed settings, select **Settings**.

m. Review or modify the restrictions set for each function.

Group Authorization Settings

For Group Authorization, select either **On** or **Off**.

Group List

a. Select **Group List**.

b. Enter a group ID and group name.

c. For Access Level, select either **Administrator** or **User**.

d. Review or modify the account name. Select **Account List** to use a different account name, and then select **Submit**.

e. Review or modify the restrictions set for each function.

Guest Authorization Settings

For Guest Authorization, select either **On** or **Off**.

Guest Settings

a. Select **Guest Settings**.

b. Enter a user name.

c. For Access Level, select either **Administrator** or **User**.

d. Review or modify the account name. Select **Account List** to use a different account name, and then select **Submit**.

e. Review or modify the restrictions set for each function.

Unknown User Settings

a. For Unknown ID Job, select either **Reject** or **Permit**.

b. To configure the detailed settings, select **Unknown User Settings**.

c. Enter a user name.

d. Review or modify the account name. Select **Account List** to use a different account name, and then select **Submit**.

Account Name is displayed when Job Accounting is set to **On**.

e. For Print Restriction, select either **Off** or **Reject Usage**.

Simple Login Settings

For Simple Login, select either **On** or **Off**.

Simple Login Key List

a. Select **Simple Login Key List**.

b. To configure Key (1 to 20), select **Settings**.

c. Enter a display name.

d. Select a display icon from the drop-down list.

e. For password, select either **On** or **Off**.

f. For Authentication, select either **Local Authentication** or **Network Authentication**.

g. When **Local Authentication** is selected, review or modify the current user. Select **User List** to select a different user, then select **Submit**.

h. When **Network Authentication** is selected, enter the login user name and password. Then, select a domain from the drop-down list.

Quick Job Printing

This feature is available only when either **NTLM** or **Kerberos** is selected in Server Type.

a. For Display List on Login, select either **On** or **Off**.

b. For the following items, select either **On** or **Off**:

- Logout after Printing
- Skip Password and Copies Confirmation

Universal Print Settings

Select **On** to link with cloud print.

4 Select **Submit**.

Local User List

The user information can be added or modified on the Local User List.

Add User

This allows you to add a new user.

1 Go to **Management Settings** > **Authentication**.

2 In Local User List, select **Add User**.

3 You can configure settings for User Property. Specify the required settings for any of the following:

User Name

Enter your user name.

Login User Name

Enter a login user ID.

You cannot use an existing login user name.

Password

Enter a login password.

If Password Policy is enabled, you must meet password requirements. For details, see *Authentication Security Settings*.

Confirm Password

Enter the login password again to confirm.

Access Level

Select either **Administrator** or **User**.

When **User** is selected, configure the following System Administration Permissions:

- Original/Paper
- Address Book
- User/Job Account Information
- Basic Network
- Basic Device
- Advanced Device/Network

Account Name

Select **Account List**. Then, select an account name and select **Submit**.

E-mail Address

Enter your email address.

Notifications will be sent to this email address.

Language

Select a language from the drop-down list.

Default Screen

Select an item for the default screen from the drop-down list.

4 Review or modify the restrictions set for each function.

5 Select **Submit**.

Modify a user

1 Go to **Management Settings** > **Authentication**.

2 In Local User List, select a user.

3 Review or modify the available User Property settings.

4 In Advanced Settings, review or modify any of the following settings:

Cloud User Name

Displays the specified user name for cloud authentication.

> This setting is available only when you configure Cloud Authentication settings.

Cloud Authentication Status

> The status is displayed as Unauthenticated by default and is not shown once Cloud Authentication is configured.

Displays the status for cloud authentication. You can also modify cloud authentication settings by doing the following:

a. Select **Cloud Authentication**.

b. In Cloud Authentication, copy the code, and then select the URL.

c. Paste the code and select **Next**.

d. In Microsoft 365, do either of the following:

- Select a saved account.
- Select **Use another account** and enter the necessary information.

> For Exchange Online accounts with two-factor authentication (2FA) enabled, make sure to have access to your preferred authentication app. Log in to your Exchange Online account, and then follow the instructions to complete 2FA. For more information, contact your Exchange Online server administrator.

e. Enter the multi-factor authentication (MFA) code.

f. To confirm the account selected for signing in, select **Consent on behalf of your organization** > **Accept**.

g. Once the permission request has been approved, select **Continue**.

h. Close the Kyocera Universal Print Client window.

i. In Command Center RX, go back to Cloud Authentication, then select the refresh icon to check the Registration Status.

j. Once authentication is complete, select **OK**, then check the Cloud User Name.

> If you want to delete the existing Cloud User Name, select **Delete** > **OK**.

5 Select **Submit**.

Delete

1. Select the checkbox to the left of the user name. To select all items at once, select **Check All**.
2. Select **Delete** > **OK**.

ID Card

This section includes advanced settings for ID Card authentication.

This feature is available only when ID Card is installed.

ID Card Settings

To use ID Card authentication, you must first configure the ID Card settings.

This feature is available only when ID Card is installed.

1. In the navigation menu, select **Management Settings** > **ID Card**.
2. Configure the Authentication Settings.

   Keyboard Login

   For keyboard login, select either **Prohibit** or **Permit**.

   Additional Authentication

   Select **Off**, **Use Password**, or **Use PIN**.

   - Additional Authentication is available only when either **Local Authentication** or **Network Authentication** is selected in **Management Settings** > **Authentication**.
   - Use PIN is available only when **Network Authentication** is selected as authentication type and **Ext.** is selected as server type in **Management Settings** > **Authentication**.

3. Configure the ID Card Settings. In ID Card Read Type, select from the following:
   - **IDM**
   - **FeliCa**
   - **MIFARE**
4. Configure the FeliCa Read Settings.

   System Code 1

   Enter a hexadecimal value from 0000 to FFFF.

   Service Code 1

   Enter a hexadecimal value from 0000 to FFFF.

Number of Blocks in Use.

Enter a decimal value from 1 to 255.

Service Code 2

Enter a hexadecimal value from 0000 to FFFF.

Number of Blocks in Use.

Enter a decimal value from 1 to 255.

If necessary, configure System Code 2 by repeating the steps from System Code 1.

5 Configure the MIFARE Read Settings (1 to 5).

Sector Number

Enter a hexadecimal value from 00 to 3F.

Secret Key Type

Select either **KeyA** or **KeyB**.

Secret Key

Enter a 12-digit secret key with a hexadecimal value from 0 to F.

6 Select **Submit**.

Notification/Report

This section includes advanced settings for notifications and reports.

Notification/Report Settings

1 In the navigation menu, select **Management Settings** > **Notification/Report**.

2 Specify the required settings for any of the following:

Management Report

This setting allows you to configure management reports. For details, see *Configuring management report settings*.

Result Report

This setting allows you to configure result reports. For details, see *Configuring result report settings*.

Maintenance Report

This setting allows you to configure maintenance reports. For details, see *Configuring maintenance report settings*.

Event Report / Scheduled Report (1 to 3)

This setting allows you to configure event or scheduled reports. For details, see *Configuring event report/scheduled report settings*.

3 Select **Submit**.

Configuring management report settings

1 In the navigation menu, select **Management Settings** > **Notification/ Report**.

2 Do one or more of the following:

Outgoing FAX Report

Select either **On** or **Off**.

Incoming FAX Report

Select either **On** or **Off**.

3 Select **Submit**.

Configuring result report settings

1 In the navigation menu, select **Management Settings** > **Notification/ Report**.

2 Do one or more of the following:

Send Result Report

a. In E-mail/Folder, select from the following:

- **Off**
- **On**
- **Error Only**

When **Error Only** is selected, a report will be emailed to you and stored in a folder only when sending fails.

b. In FAX, select from the following:

- **Off**
- **On**
- **Error Only**
- **Specify Each Job**

When **Error Only** is selected, you will receive a report only when sending fails.

c. In Attach Image, select from the following:

Attach Image is not available if FAX is set to **Off**.

- **Off**
- **Partial Image**
- **Full Image**

d. For Attach Image of Network FAX, select either **Cover Page** or **Body**.

Attach Image of Network FAX is not available if FAX is set to **Off** and Attach Image is set to **Off**.

e. If necessary, set Canceled before Sending to **On**.

f. Select either **Name or Destination** or **Name and Destination** as the recipient format.

Receive Result Report

a. In FAX RX, select from the following:

- **Off**
- **On**
- **Error/Storing in Box**

When **Error/Storing in Box** is selected, you will be notified via email or report only when an error occurs while receiving or when the document is forwarded to the Sub Address Box.

b. Select either **Print Report** or **E-mail** as the report type.

Report Type is not available if FAX RX is set to **Off**.

c. If **E-mail** is selected as the report type, enter your email address.

Job Finish Notice

For Attach Image, select either **On** or **Off**.

3 Select **Submit**.

Configuring maintenance report settings

1 In the navigation menu, select **Management Settings** > **Notification/Report**.

2 Do one or more of the following:

Equipment ID

Enter the equipment ID.

Recipient E-mail Address

Enter the email address for receiving maintenance reports.

Use a semicolon (;) between multiple addresses.

Subject

Enter the subject of the report.

Maintenance Report Interval

a. Select from the following:

- **None**
- **Monthly**
- **Weekly**
- **Daily**
- **Hourly**

b. If you selected **Monthly**, set the month, day, and time.

c. If you selected **Weekly**, set the day and time.

d. If you selected **Daily**, set the time.

e. If you selected **Hourly**, set the hourly interval.

Run once now

Select **Send** to automatically send a maintenance report to the recipient.

3 Select **Submit**.

Configuring event report/scheduled report settings

1 In the navigation menu, select **Management Settings** > **Notification/ Report**.

2 Do one or more of the following:

Recipient (1 to 3) E-mail Address

Enter the recipient email address.

Subject

Enter the subject of the report using a variable.

Event Report

a. Select one or more items for the event report.

b. Enter an interval between event reports.

An event will be reported only when at least one of the selected events occurs during the interval.

c. If necessary, set the following to **On**:

- Notify when Data Sanitization Starts
- Syslog Records Kept Alert
- Notify when Malicious Program is Detected

- When Notify when Data Sanitization Starts is set to **On**, an email will be sent once data sanitization begins.
- When Syslog Records Kept Alert is set to **On**, alerts will be enabled whenever Syslog records are kept.
- When Notify when Malicious Program is Detected is set to **On**, an email will be sent once a malicious program is detected.

Scheduled Report

a. In Scheduled Report Items, select **Counter Status** to attach a counter report.

b. In Scheduled Report Interval, select from the following:

- **None**
- **Monthly**
- **Weekly**
- **Daily**
- **Hourly**

c. If you selected **Monthly**, set the month, day, and time.

d. If you selected **Weekly**, set the day and time.

e. If you selected **Daily**, set the time.

f. If you selected **Hourly**, set the hourly interval.

g. In Run once now, select **Send** to automatically send a scheduled report to the specified recipients.

3 Select **Submit**.

History Settings

This section includes advanced history settings.

History Settings

1 In the navigation menu, select **Management Settings** > **History Settings**.

2 Configure the Job Log History.

Recipient E-mail Address

Enter the recipient email address.

If there are more than one recipient, use a semicolon (;) to separate the email addresses.

Subject

Enter the subject for the Job Log History.

SSFC Subject

Enter the subject for the Job Log History using the ID Card authentication.

This feature is available only when ID Card is installed and SSFC is the ID Card type.

Auto Sending

Determines whether the job log report is sent or not. Select either **On** or **Off**.

Number of Records

Enter the number of job logs for sending.

Personal Information

Determines whether personal information is included in job logs. Select either **Include** or **Exclude**.

Run once now

Select **Send** to automatically send a job log to the recipient.

3 You can configure settings for Audit Log (Syslog) Setting.

Syslog

Displays the status for Syslog.

To configure the default settings, go to **Network Settings** > **Protocol**.

Destination Server

Enter the address for the destination server.

To specify the server name by domain name, configure the DNS server in **Network Settings** > **TCP/IP**.

Port Number

Enter the port number for Syslog. The default port number is 514.

Facility

Select the number of facilities that obtain the log from the drop-down list.

Severity

Select the severity of obtained log from the drop-down list. The higher the number, the greater the severity.

4 Select **Submit**.

SNMP

This section includes advanced settings for SNMP.

If the settings for the item marked with an asterisk (*) has been changed, you must restart the device or network. In the navigation menu, go to **Management Settings** > **Restart/Reset**.

SNMP Settings

1 In the navigation menu, select **Management Settings** > **SNMP**.

2 Configure SNMPv1/v2c as follows.

SNMPv1/v2c

Activate or deactivate the SNMPv1/v2c protocol. Select either **On** or **Off** in **Network Settings** > **Protocol**.

Read Community

Enter the community name for SNMP requests to read a value. The default name is 'public'.

After you have changed the setting, you must restart the device.

Write Community

Enter the community name for SNMP requests to write (change) a value. Community name is required to be able to connect with a utility software. After changing the settings, the machine needs to be reset.

Depending on the region, the Community name is set to Public.

sysContact

The MIB-II sysContact object. Usually this is the email address of the network administrator.

sysName

The MIB-II sysName object. Usually this is the host or domain name of the machine.

sysLocation

The MIB-II sysLocation object. Usually this is the location information of the machine that is described under Location in System. Go to **Device Settings** > **System** to modify the settings.

Authentication Traps

Specifies whether to use authentication traps. If this is enabled, an SNMP trap is generated when an attempt to read or write is made using an incorrect community name. The trap is sent to the configured trap address.

After you have changed the setting, you must restart the device.

Trap Recipient

Select **Settings** to finish the settings.

3 Configure SNMPv3 as follows.

After you have changed the setting, you must restart the device.

SNMPv3

Sets whether to use the SNMPv3 protocol. Select either **On** or **Off** in **Network Settings** > **Protocol**.

Authentication

Selects **On** or **Off** whether to do authentication during SNMP transmission.

Hash

Select either **MD5** or **SHA1** for Hash algorithm. This item becomes active when the Authentication is set to **On**.

Privacy

Sets whether to encrypt the communicated data in SNMP communication. This becomes available when Authentication is set to **On**.

Encryption

Select either **DES** or **AES** for encryption algorithm. This item becomes active when the Authentication is set to **On**.

Read Only User

Enter user name, Authentication Password, and Privacy Password of the read-only user.

Read/Write User

Enter user name, Authentication Password, and Privacy Password of the read/write user.

4 Select **Submit**.

Restart/Reset

This section includes advanced settings for restarting and resetting the device or network.

Restart

1. In the navigation menu, select **Management Settings** > **Restart/Reset**.
2. Restart the device or network as needed.

Restart Device

Select **Restart Device** to restart the machine.

Restart Network

Select **Restart Network** to restart the related network service of the machine only.

Reset device to factory default

1. In the navigation menu, select **Management Settings** > **Restart/Reset**.
2. Select **Initialize** as needed. The machine is reset to factory default settings.

Remote Operation

This section includes advanced settings for remote operation. Using remote operation, a system administrator can remotely access the device operation panel screen from a web browser and explain the operation and troubleshooting procedures to the user.

We recommend the latest supported web browser versions to use Remote Operation. For details, refer to *Web browser*.

To use Remote Operation, Enhanced VNC(RFB) over TLS must be enabled. For details, refer to *Protocol*.

Remote Operation

1. In the navigation menu, select **Network Settings** > **Protocol**.
2. In Other Protocols, set Enhanced VNC(RFB) over TLS to **On**.

   The default setting is On. For other settings, refer to *Protocol*.
3. In the navigation menu, select **Management Settings** > **Remote Operation**.

4 Specify the required settings for any of the following:

Remote Operation

Select **On** to enable remote operation.

Use Restriction

Select **Off**, **Administrator Only**, or **Use Password**.

When **Off** is selected, all users are allowed to use remote operation.

When **Administrator Only** is selected, only administrators are allowed to use remote operation.

When **Administrator Only** is selected, VNC software is unavailable for remote operation.

When **Use Password** is selected, enter the password in Password and Confirm Password.

VNC Compatible Software

When **VNC (RFB)** or **VNC(RFB) over TLS** is selected as the network protocol, *Available* is displayed.

5 Select **Submit**.

Running Remote Operation from Google Chrome web browser

Before using Remote Operation, make sure you have already configured the necessary settings. For details, see *Remote Operation*.

1 Open Google Chrome web browser.

2 Enter `https://` and host name of the machine to start up the Command Center RX.

3 If necessary, select **Advanced** > **Proceed to 123.123.123.123 (unsafe)**, where 123.123.123.123 is the IP address of the device.

4 Log in to the Command Center RX with administrator rights.

5 In the navigation menu, select **Device Information / Remote Operation** > **Remote Operation**.

6 Select **Start**.

When the Remote Operation starts, the operation panel screen will be displayed on your computer.

- If you are logged in to the device, the permission confirmation screen may be displayed on the operation panel. Select **Yes**.
- If browser pop-ups are blocked, select **Always allow pop-ups and redirects from https://123.123.123.123** > **Done**, where 123.123.123.123 is the IP address of the device. Wait for at least one minute before starting Remote Operation.
- If you encounter any problems with Remote Operation, contact your regional technical support.

Running Remote Operation from Microsoft Edge web browser

Before using Remote Operation, make sure you have already configured the necessary settings. For details, see *Remote Operation*.

1. Open Microsoft Edge web browser.
2. Enter `https://` and host name of the machine to start up the Command Center RX.
3. If necessary, select **Advanced** > **Continue to 123.123.123.123 (unsafe)**, where 123.123.123.123 is the IP address of the device.
4. Log in to the Command Center RX with administrator rights.
5. In the navigation menu, select **Device Information / Remote Operation** > **Remote Operation**.
6. Select **Start**.

   When the Remote Operation starts, the operation panel screen will be displayed on your computer.

   - If you are logged in to the device, the permission confirmation screen may be displayed on the operation panel. Select **Yes**.
   - If browser pop-ups are blocked, select **Always allow pop-ups and redirects from https://123.123.123.123** > **Done**, where 123.123.123.123 is the IP address of the device. Wait for at least one minute before starting Remote Operation.
   - If you encounter any problems with Remote Operation, contact your regional technical support.

Running Remote Operation from Firefox web browser

Before using Remote Operation, make sure you have already configured the necessary settings. For details, see *Remote Operation*.

1. Open Firefox web browser.

2 Enter `https://` and host name of the machine to start up the Command Center RX.

3 If necessary, select **Advanced** > **Accept the Risk and Continue**.

4 Log in to the Command Center RX with administrator rights.

5 In the navigation menu, select **Device Information / Remote Operation** > **Remote Operation**.

6 Select **Start**.

When the Remote Operation starts, the operation panel screen will be displayed on your computer.

- If you are logged in to the device, the permission confirmation screen may be displayed on the operation panel. Select **Yes**.
- Browser pop-ups may be blocked. Do the following steps to solve this problem:
  a. In Firefox web browser, go to **Open application menu** > **Settings**.
  b. In the side menu, select **Privacy & Security**, and then in *Block pop-up windows*, select **Exceptions**.
  c. In *Address of website*, enter `https://123.123.123.123` where 123.123.123.123 is the IP address of the device, then select **Allow**.
  d. Confirm that the entered address is included in the list of allowed websites, and then select **Save Changes**.

     After one minute, the exception is applied.
  e. Go to **Device Information / Remote Operation** > **Remote Operation**, and then select **Start**.
- If you encounter any problems with Remote Operation, contact your regional technical support.

Running Remote Operation from Safari web browser

Before using Remote Operation, make sure you have already configured the necessary settings. For details, see *Remote Operation*.

1 Open Safari web browser.

2 Enter `https://` and host name of the machine to start up the Command Center RX.

3 If necessary, select **Show Details** > **view the certificate**, then do the following:

a) Drag the certificate icon to your desktop.

b) In your desktop, double-click the certificate.

c) In Keychain Access, select **View Certificates** > **Trust**.

d) In *When using this certificate*, select **Always Trust**, then select **OK** > **Add**.

e) In Command Center RX, select the web browser refresh button.

4 Log in to the Command Center RX with administrator rights.

5 In the navigation menu, select **Device Information / Remote Operation** > **Remote Operation**.

6 Select **Start**.

When the Remote Operation starts, the operation panel screen will be displayed on your computer.

- If you are logged in to the device, the permission confirmation screen may be displayed on the operation panel. Select **Yes**.
- If you encounter any problems with Remote Operation, contact your regional technical support.

11 Troubleshooting

Refer to the following table for basic solutions to problems you may encounter with the embedded server.

Symptom	Check Items	Corrective Action	Reference
I cannot access the embedded server.	Is the device turned on?	Turn the power on and wait until the device is ready. Then, try to access the embedded server.	*Operation Guide*
	Is the network cable connected properly?	Connect the network cable properly.	*Operation Guide*
	Are the network settings in the device correct?	Check the network settings from the operation panel. Contact your network administrator for the correct settings.	N/A
	Is the correct IP address entered for this device?	Enter the correct IP address. Contact your network administrator for the device IP address.	N/A
	Are the network settings in the web browser correct?	Check the network settings in the web browser. For more details, see the Help feature.	N/A
	Has the administrator set up an IP Filter function?	Access the embedded server from an approved IP address.	*IP Filter(IPv4) Settings* *IP Filter(IPv6) Settings*
	Is HTTP Security set to **Secure Only (HTTPS)** in **Security Settings** > **Network Security** > **Serverside Settings**?	When HTTP Security is set to **Secure Only (HTTPS)**, specify a URL that begins with "https://". You cannot access the embedded server using "http://" for the URL.	*Secure Protocol Settings*
	Is the web browser version supported for the embedded server?	Use a supported web browser version for the embedded server.	*System Requirements*

Symptom	Check Items	Corrective Action	Reference
Characters are not displayed properly in the embedded server.	Is the web browser version supported for the embedded server?	Use a supported web browser version for the embedded server.	*System Requirements*
	Is the same language selected for both the embedded server and the operation panel display?	Select the same language as that displayed on the operation panel.	*Top Bar*
I cannot access other pages.	Is the access level set to **User**?	Change the access level to **Administrator**.	*Local User List*
I cannot do settings.	Is the printer or scanner currently in operation?	Wait until the operation is complete.	N/A
The settings I made were not saved.	Did you select **Submit** after configuring the settings?	Select **Submit** before moving to another page or closing the embedded server window.	N/A
	Did you select **Restart** for settings that require restarting the device?	Restart the device. All settings will be saved.	*Restart/Reset*
	Are you configuring the embedded server and the operation panel system menu at the same time?	Configure the embedded server after you have configured the system menu on the operation panel.	N/A
I forgot my administrator password.	N/A	Contact your regional technical support.	N/A
Error or Warning is displayed.	Is there an error or warning message shown in the operation panel display?	Refer to the machine *Operation Guide* and follow the appropriate instructions for the error message displayed.	*Operation Guide*
The settings I made were not applied.	Did you select **Restart Network** when the prompt message was displayed?	Select **Restart Network** after configuring the settings. Only related network services will restart.	N/A

For the Kyocera contact in your region, see Sales Sites sections here.
https://www.kyoceradocumentsolutions.com/company/directory.html