TOSHIBA

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for the Latest Functions

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

Preface

Thank you for purchasing our product.
This manual describes the latest functions embedded in this equipment.
Read this manual before using the functions.

■ How to read this manual

❑ Symbols in this manual

In this manual, some important items are described with the symbols shown below. Be sure to read these items before using this equipment.

⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death, serious injury, or serious damage, or fire in the equipment or surrounding objects.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, partial damage to the equipment or surrounding objects, or loss of data.
Note	Indicates information to which you should pay attention when operating the equipment.
Tip	Describes handy information that is useful to know when operating the equipment.
📖	Pages describing items related to what you are currently doing. See these pages as required.

❑ Target audience for this manual

This is a manual that is aimed at general users and administrators.

❑ Model and series names in this manual

In this manual, each model name is replaced with a series name as shown below.

Model name	Series name
e-STUDIO2010AC/2510AC	e-STUDIO5015AC Series
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC	
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A	e-STUDIO5018A Series
e-STUDIO5516AC/6516AC/7516AC	e-STUDIO7516AC Series
e-STUDIO5518A/6518A/7518A/8518A	e-STUDIO8518A Series
e-STUDIO330AC/400AC	e-STUDIO400AC Series

❑ Optional equipment

For available options, refer to the **Quick Start Guide**.

❑ Screens in this manual

In this manual, Windows10 is taken for explanation purposes to describe the screens and operation procedures in Windows.
The details on the screens may differ depending on your model and how the equipment is used, such as the status of the installed options, the OS version and the applications.

❑ About the defaults shown in this manual

- The defaults shown in this manual are the values in the standard operating environment. The values may have been changed from these defaults. The defaults for your model may differ from the defaults shown.
- The default for the list item is shown underlined.

❑ Trademarks

AirPrint, iPad, and macOS are trademark of Apple Inc., registered in the U.S. and other countries.
For other trademarks, refer to the **Safety Information**.

CONTENTS

1

HOME SCREEN

■ Remote Assistant Menu

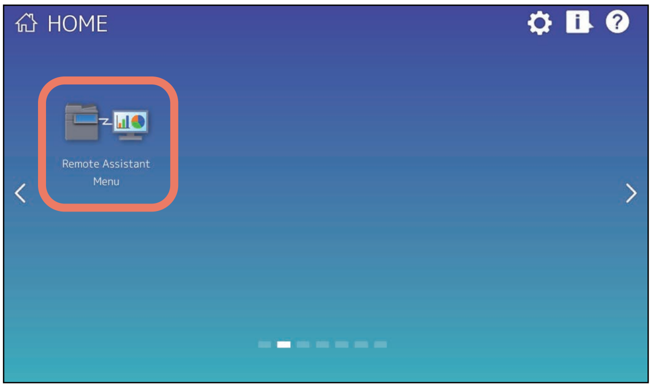
[Remote Assistant Menu] is displayed on the home screen*.

* This may not be displayed depending on the mode in use.

This menu has the following three functions.

- **Logs Transmission**
  This is used to transmit or delete logs of the equipment in order to clear problems.
- **Remote Service**
  This is used to maintain the equipment by the remote operation.
- **Remote Panel Operation**
  This is used to maintain the equipment by the remote operation in order to clear problems.

When you receive a request from your service technician or representative, press [Remote Assistant Menu] and operate the equipment in accordance with the instructions. For details about this, contact your service technician or representative.



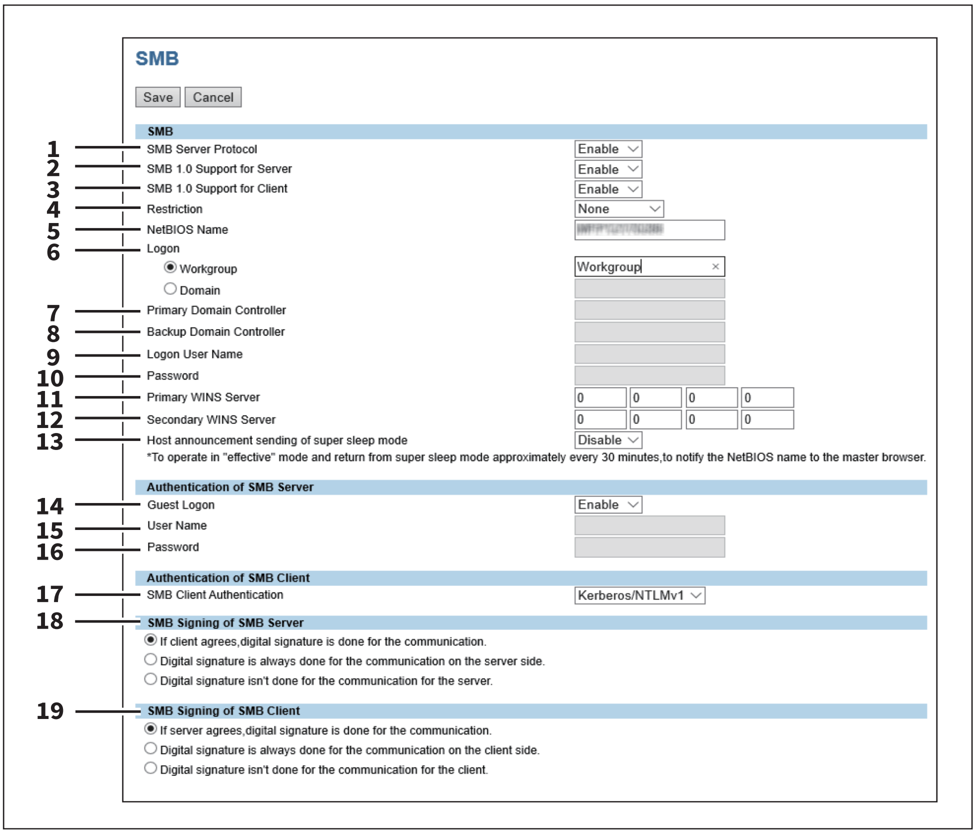
2

TopAccess

■ Network settings

❑ Setting up SMB

In SMB, you can specify the SMB network properties to access this equipment through a Microsoft Windows Network and enable SMB printing. When you enable the SMB, users can also browse the local folder in the equipment. You can also specify the WINS server when the WINS server is used to enable the Windows print sharing and Windows file sharing services between the different subnets.



	Item name	Description
1	SMB Server Protocol	Select whether the SMB protocol is enabled or disabled. • **Enable** — Select this to enable SMB. • **Disable** — Select this to disable SMB.
2	SMB 1.0 Support For Server	Select whether the SMB 1.0 server is enabled or disabled. • **Enable** — Select this to enable the SMB 1.0 server. • **Disable** — Select this to disable the SMB 1.0 server.
3	SMB 1.0 Support For Client	Select whether the SMB 1.0 client is enabled or disabled. • **Enable** — Select this to enable the SMB 1.0 client. • **Disable** — Select this to disable the SMB 1.0 client.
4	Restriction	Specify restrictions on SMB. • **None** — Select this to not specify restrictions on SMB. • **Print Share** — Select this to enable the file sharing service using SMB, but disable SMB printing. • **File Share** — Select this to enable SMB printing, but disable the file sharing service using SMB.

<table>
<tr><th></th><th>Item name</th><th>Description</th></tr>
<tr><td rowspan="2">5</td><td>NetBIOS Name</td><td>Enter the NetBIOS name of this equipment. The equipment uses “MFP<NIC Serial Number>” as the default NetBIOS name.</td></tr>
<tr><td colspan="2">Note
You can enter only alphanumerical characters and “-” (a hyphen) for NetBIOS names. If you use any other characters, a warning message will be displayed.</td></tr>
<tr><td rowspan="2">6</td><td>Logon</td><td>Enter the workgroup or domain that this equipment joins.
• <u>Workgroup</u> — To include the equipment in the workgroup, enter the workgroup name. All client computers can access this equipment without a user name and password.
• Domain — Select this and enter the domain name when the equipment will log on in the domain. Any client computers which are not members of the domain will need a valid user name and password to access this equipment. Use this to enhance access security to this equipment.</td></tr>
<tr><td colspan="2">Note
For workgroup and domain names, you can use only alphanumerical characters and symbols other than the following:
; : " < > + = \ | ? , * #
If you use any other characters, a warning message will be displayed.</td></tr>
<tr><td>7</td><td>Primary Domain Controller</td><td>Specify the server name or IP address of the primary domain controller when this equipment will log on the domain network. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</td></tr>
<tr><td rowspan="2">8</td><td>Backup Domain Controller</td><td>Specify the server name or IP address of the backup domain controller when this equipment will log on the domain network, if required. If the Primary Domain Controller is unavailable, the Backup Domain Controller will be used to log on. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</td></tr>
<tr><td colspan="2">Note
If the wrong primary or backup domain controller is specified, the NETWORK INITIALIZING message will be displayed for up to 4 minutes while the equipment searches for the primary or backup domain controller. In that case, correct the primary or backup domain controller setting after the NETWORK INITIALIZING message disappears.</td></tr>
<tr><td>9</td><td>Logon User Name</td><td>Enter a valid user name to log on to the specified domain. You can enter up to 128 alphanumerical characters and symbols other than " / \ [ ] : ; | = , + * ? < >.</td></tr>
<tr><td>10</td><td>Password</td><td>Enter the password for the specified log on user name to log on the domain network. You can enter up to 128 alphanumerical characters.</td></tr>
<tr><td rowspan="2">11</td><td>Primary WINS Server</td><td>Specify the IP address of the primary WINS server when the WINS server is used to provide the NetBIOS name in your local area network. This option would be more useful to access this equipment using the NetBIOS Name from a different subnet.</td></tr>
<tr><td colspan="2">Tip
When the [Obtain a WINS Server Address automatically] option is enabled in the TCP/IP settings, the primary and secondary WINS server address can be obtained using the DHCP server.</td></tr>
</table>

<table>
<tr><th></th><th>Item name</th><th>Description</th></tr>
<tr><td rowspan="2">12</td><td>Secondary WINS Server</td><td>Specify the IP address of the secondary WINS server as you require when the WINS server is used to provide NetBIOS name in your local area network. If the Primary WINS Server is unavailable, the Secondary WINS Server will be used.</td></tr>
<tr><td colspan="2">Tip
When the [Obtain a WINS Server Address automatically] option is enabled in the TCP/IP settings, the primary and secondary WINS server address can be obtained using the DHCP server.

Note
If “0.0.0.0” is entered for the Primary WINS Server and Secondary WINS Server, this equipment will not use the WINS server.</td></tr>
<tr><td rowspan="2">13</td><td>Host announcement sending of super sleep mode</td><td>Specify this to display this equipment’s icon in the “Network” folder on the Windows computer even in super sleep mode.
• <u>Disable</u>: Disables host announcement sending in super sleep mode.
• Enable: Even in super sleep mode, the icon for this printer is displayed in the “Network” folder on Windows computers.</td></tr>
<tr><td colspan="2">Note
When the printer’s super sleep mode is set to [Disable], the icon for this printer is displayed in the “Network” folder on Windows computers regardless of this setting.</td></tr>
<tr><td>14</td><td>Guest Logon</td><td>Select whether a guest user can log on to the SMB server. [Enable] is set as the default.</td></tr>
<tr><td rowspan="2">15</td><td>User Name</td><td>Enter a name of the user who logs on to the SMB server if [Guest Logon] is set to [Disable]. You can enter up to 32 alphanumerical characters and symbols except " / \ [ ] : ; | = , + * ? < >.</td></tr>
<tr><td colspan="2">Note
If you connect to the SMB server for this equipment before changing the user name, qualification information on the user name and the password is cached in your Windows computer. Restart your Windows computer to clear qualification information.</td></tr>
<tr><td rowspan="2">16</td><td>Password</td><td>Enter a password of the specified user if [Guest Logon] is set to [Disable]. You can enter up to 128 alphanumerical characters and symbols.</td></tr>
<tr><td colspan="2">Note
If you connect to the SMB server for this equipment before changing the password, qualification information on the user name and the password is cached in your Windows computer. Restart your Windows computer to clear qualification information.</td></tr>
</table>

	Item name	Description
17	SMB Client Authentication	Specify the authentication method for the SMB clients. • **<u>Kerberos/NTLMv2</u>** — Specify this when connecting to an SMB server using Kerberos/NLTMv2 authentication. NTLMv2 authentication is used if Kerberos authentication has failed. • **Kerberos/NTLMv1** — Specify this when connecting to an SMB server using Kerberos/NTLMv1 authentication. NTLMv1 authentication is used if Kerberos authentication has failed. • **Kerberos** — Specify this when connecting to an SMB server using Kerberos authentication. • **NTLMv2** — Specify this when connecting to an SMB server using NTLMv2 authentication. • **NTLMv1** — Specify this when connecting to an SMB server using NTLMv1 authentication.
	Note SMB servers running Mac OS X 10.10 or later do not support NTLMv1 authentication.	
18	SMB Signing of SMB Server	Select whether SMB Signing is enabled or disabled when a client accesses this equipment using SMB, such as when a client accesses the shared folder in this equipment. • **<u>If server agrees, digital signature is done for the communication.</u>** — Select this to use the digital signature to secure communication only when a client accesses this equipment with a digital signature. Even if a client accesses this equipment without a digital signature, the communication is allowed without the digital signature. • **Digital signature is always done for the communication on the server side.** — Select this to allow the communication only when a client accesses this equipment with a digital signature. When a client accesses this equipment without a digital signature, the communication is not allowed. • **Digital signature isn't done for the communication for the server.** — Select this to allow the communication only when a client accesses this equipment without a digital signature. When a client is set to always access an SMB server with a digital signature, the communication is not allowed.
	Note If you do not know whether the SMB Signing of SMB Client is enabled or disabled in the client computers, it is recommended to select [If client agrees, digital signature is done for the communication.]. If this is set incorrectly, the SMB communication may become unavailable.	

	Item name	Description
19	SMB Signing of SMB Client	Select whether SMB Signing is enabled or disabled when this equipment accesses the clients using SMB, such as when this equipment stores the scanned data in the network folder using SMB. • **If server agrees, digital signature is done for the communication.** — Select this to use the digital signature to secure the communication to an SMB server only when the SMB Signing of SMB Server that this equipment accesses is enabled. If the SMB Signing of SMB Server is disabled in an SMB server, the communication is performed without the digital signature. • **Digital signature is always done for the communication on the client side.** — Select this to make this equipment always access an SMB server with a digital signature. When the SMB Signing of SMB Server is disabled in an SMB server, the communication is not allowed. • **Digital signature isn't done for the communication for the client.** — Select this to communicate to an SMB server without the digital signature. If the SMB Signing of SMB Server is always enabled in an SMB server, the communication is not allowed.
	Note • If you do not know whether the SMB Signing of SMB Server is enabled or disabled in the SMB servers, it is recommended to select [If server agrees, digital signature is done for the communication.]. If this is set incorrectly, the SMB communication may become unavailable. • The digital signature is always done for the communication on the server side as the default on Windows Server 2012 or later. Therefore specify "If server agrees, digital signature is done for the communication." or "Digital signature is always done for the communication on the client side." for SMB communications with Windows Server 2012 or later.	

❑ Setting up Bonjour

In Bonjour, you can enable or disable the Bonjour networking that is available for Mac OS X.

	Item name	Description
1	Enable Bonjour	Select whether Bonjour is enabled or disabled. [Enable] is set as the default.
2	Link-Local Host Name	Enter the DNS host name of this equipment. You can enter up to 127 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
3	Service Name	Enter the device name of this equipment that will be displayed in the Bonjour network. You can enter up to 63 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
4	Chrome OS Print	Select whether the Chrome OS Print service is enabled or disabled. [Enable] is set as the default.

❑ VNC Setting

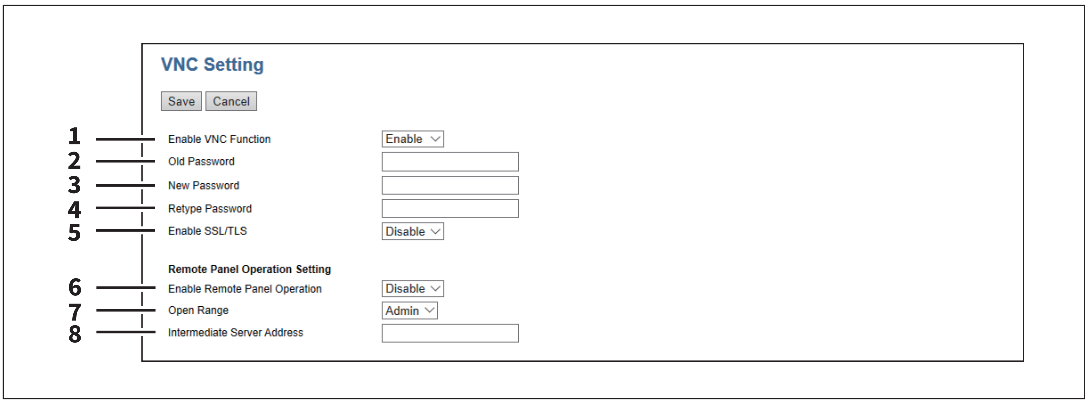
You can use a computer or a mobile terminal such as a tablet and a smartphone to check and operate the control panel.

Note

- The default password for this VNC function is “d9kvgn”. Be sure to change it before using this function. Specify a password with six or more and eight or less alphanumeric letters.
- You can use only one computer or mobile terminal for the VNC function.

Tip

- It is recommended that you use UltraVNC (client software) on Windows 8.1 or later for the VNC function.
- When this VNC function is enabled, the equipment does not enter the Super Sleep mode.



	Item name	Description
1	Enable VNC Function	Select whether the VNC function is enabled or disabled. • **Enable** — Enables the VNC function. • **Disable** — Disables the VNC function.
2	Old Password	Enter the old password for the VNC function.
3	New Password	Enter a new password for the VNC function.
4	Retype Password	Retype the new password for the VNC function.
5	Enable SSL/TLS	Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for the VNC function. • **Enable** — Enables the VNC function. • **Disable** — Disables the VNC function.
6	Enable Remote Panel Operation	Select whether the remote panel operation function is enabled or disabled. • **Enable** — Select this to enable the remote panel operation function. • **Disable** — Select this to disable the remote panel operation function.
	Note For the details about [Enable Remote Panel Operation], contact your service technician or representative.	
7	Open Range	Select the disclosure range of the remote panel operation function. • **Admin** — Permits the administrator. • **User** — Permits general users.
8	Intermediate Server Address	Enter an IP address and port number of the relay server used for the remote panel operation.

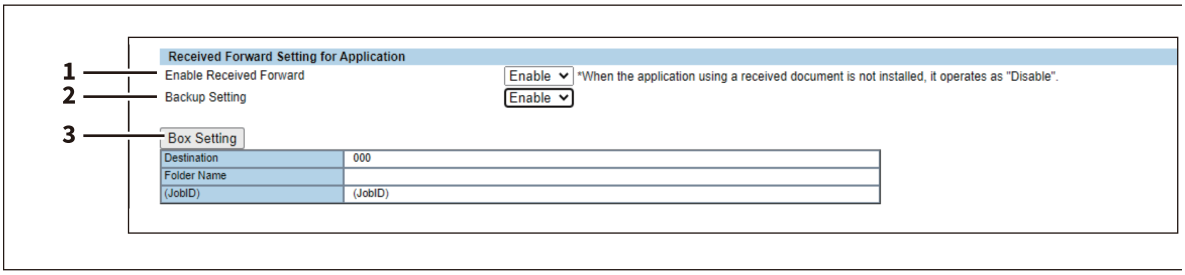
Fax settings

Received Forward Setting for Application

You can set whether or not to save received data (meta data) which can be used for the activation of the received document (image file received by fax) and an application in its storage area. For details about the application, contact your service technician or representative.

Note

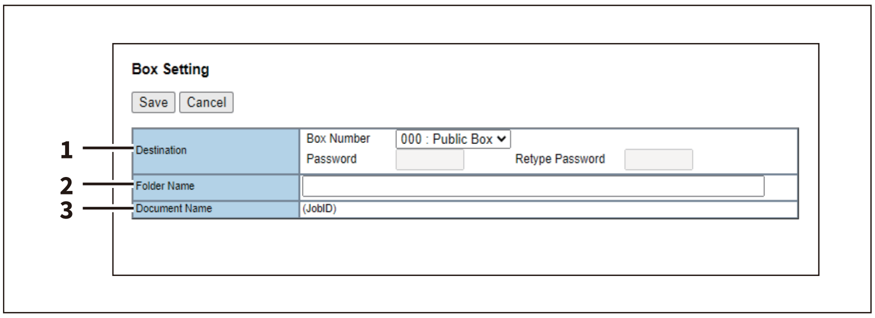
- This cannot be used if an application which uses the received document is not installed in the equipment or the execution permission of the application is disabled.
- Up to 400 documents can be stored in a box or folder, and up to 200 pages can be contained in a document. If an attempt is made to store documents exceeding the available numbers, storing to e-Filing will fail. Delete unnecessary documents in a box or e-Filing periodically. Alternatively, specify the document storage period after which unnecessary documents are automatically deleted.



	Item name	Description
1	Enable Received Forward	Select [Enable] to save the received document in the storage area of the application. [Disable] is the default setting.
	Note When [Enable] is selected for [Enable Received Forward], the Received Forward to Applications setting is taken as the top priority even if other forward settings are also enabled.	
2	Backup Setting	Select [Enable] to save the received document in the specified box as a backup file. [Disable] is the default setting.
	Tip This will be displayed when [Enable] is selected for [Enable Received Forward].	
3	[Box Setting] button	Click this to change the box for saving the received document or to modify the folder name. When you click this button, the [Box Setting] screen will appear. P.16 “Box Setting (Received Forward Setting for Application)”
	Tip You can change the settings when [Enable] is selected for [Backup Setting].	

Box Setting (Received Forward Setting for Application)

You can set the destination to back up the received document.



	Item name	Description
1	Destination	Set the box to save the received document in the storage area of an application. **Box Number** Select the box number to save the received document. “000: Public Box” is set as the default. **Password** Enter the password if it is set for the specified box. **Retype Password** Enter the same password again for a confirmation.
2	Folder Name	Enter the folder name in the box where the received document is saved. You can enter up to 64 characters.
3	Document Name	A job ID applied automatically by means of the equipment is displayed. This cannot be changed.

■ Certificate management settings

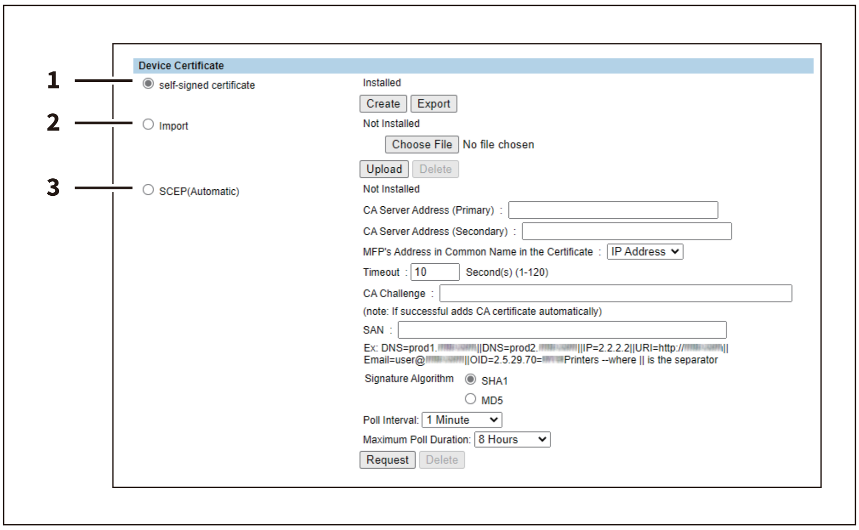
You can manage device certificates and client certificates.

Tip

The [Certificate Management] submenu can be accessed from the [Security] menu on the [Administration] tab. See the following pages for how to access it and information on the [Security] menu:

❑ Setting up Device Certificate

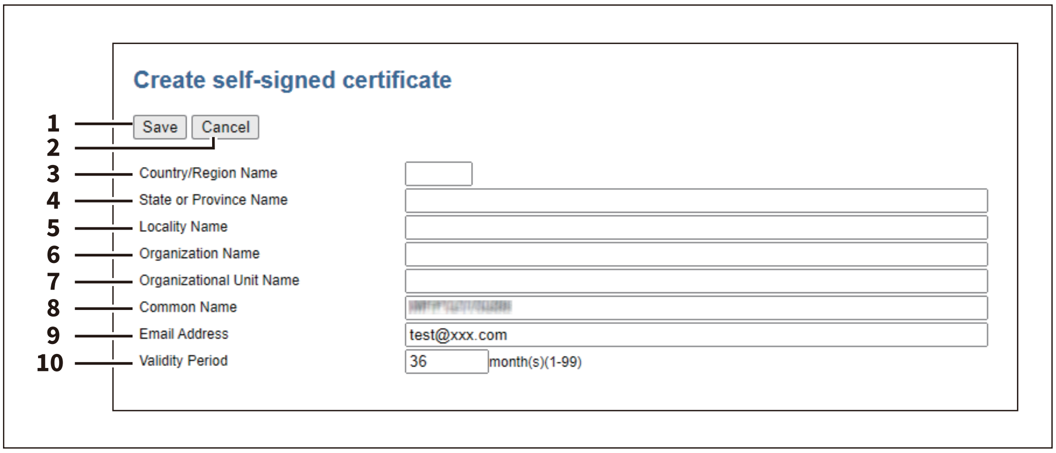
You can configure the device certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS.



	Item name	Description
1	self-signed certificate	Creates a certificate for encrypted communications using SSL/TLS on your device. **[Create] button** — Displays the [Create self-signed certificate] screen. Specify items necessary for the certificate to create the self-signed certificate. 📖 P.18 “[Create self-signed certificate] screen” **[Export] button** — Exports the created self-signed certificate.

	Item name	Description
2	Import	Import the certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS. **[Browse] button** — Allows you to select the certificate file. **[Upload] button** — Uploads the selected certificate file. **[Delete] button** — Deletes the registered certificate file.
3	SCEP(Automatic)	Automatically acquires the certificate for encrypted communications using IP sec or SSL/TLS. **CA Server Address (Primary)** — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols. **CA Server Address (Secondary)** — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols. **MFP's Address in Common Name in the Certificate** — Select whether you use the IP address or FQDN as the address of this equipment to be entered in the [Common Name] box of the certificate. [IP Address] is set as the default. **Timeout** — Enter a timeout period for quitting communication when no response is received from the CA server. Specify within the range from 1 to 120 seconds. "10" is set as the default. **CA Challenge** — Enter the password for the CA challenge. You can enter up to 32 alphanumerical characters. You need to enter a maximum of 32 alphanumerical characters for the first time when you extend the password length. **SAN** — Set the SAN attribute if necessary. Enter DNS, IP address, URI, e-mail address and OID by dividing them with ||. There are some restrictions as below. DNS: You can enter up to 253 letters with alphanumerical characters and symbols "." and "-". URI: You can use alphanumerical characters and symbols "- . _ ~ : / ? # ! @ $ ' ( ) * + ; =". e-mail address: You need to enter "@" and "." in the address. **Signature Algorithm** — Select SHA1 or MD5 as the signature algorithm. **Poll Interval** — Specify the polling interval. [1 Minute] is set as the default. **Maximum Poll Duration** — Specify the polling duration. [8 Hours] is set as the default. **[Request] button** — Click this button to request the certificate. **[Delete] button** — Deletes the registered certificate.

[Create self-signed certificate] screen

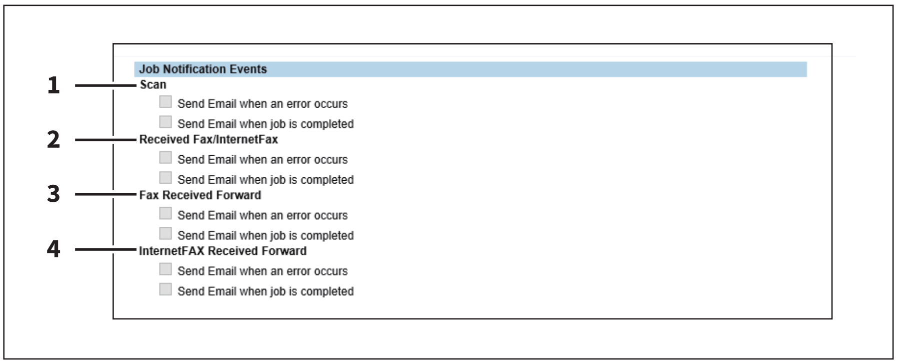


	Item name	Description
1	[Save] button	Saves the self-signed certificate.
2	[Cancel] button	Cancels creating the certificate.

	Item name	Description
3	Country/Region Name	Enter the country or region name using two alphanumerical characters and symbols. (Example: JP)
4	State or Province Name	Enter the state or province name with alphanumerical characters and symbols. You can enter up to 128 characters.
5	Locality Name	Enter the city or town name with alphanumerical characters and symbols. You can enter up to 128 characters.
6	Organization Name	Enter the organization name with alphanumerical characters and symbols. You can enter up to 64 characters.
7	Organizational Unit Name	Enter the organizational unit name with alphanumerical characters and symbols. You can enter up to 64 characters.
8	Common Name	Enter the FQDN or IP address of this equipment with alphanumerical characters and symbols. You can enter up to 64 characters.
9	Email Address	Enter the E-mail address with alphanumerical characters and symbols. You can enter up to 64 characters.
10	Validity Period	Enter the number of months in the validity period of the self-signed certificate.

■ Notification settings

❑ Setting up Job Notification Events



You can select jobs to be notified.

	Item name	Description
1	Scan	**Send Email when an error occurs** **Send Email when job is completed**
2	Received Fax/InternetFax	**Send Email when an error occurs** **Send Email when job is completed**
3	Fax Received Forward	**Send Email when an error occurs** **Send Email when job is completed**
4	InternetFAX Received Forward	**Send Email when an error occurs** **Send Email when job is completed**

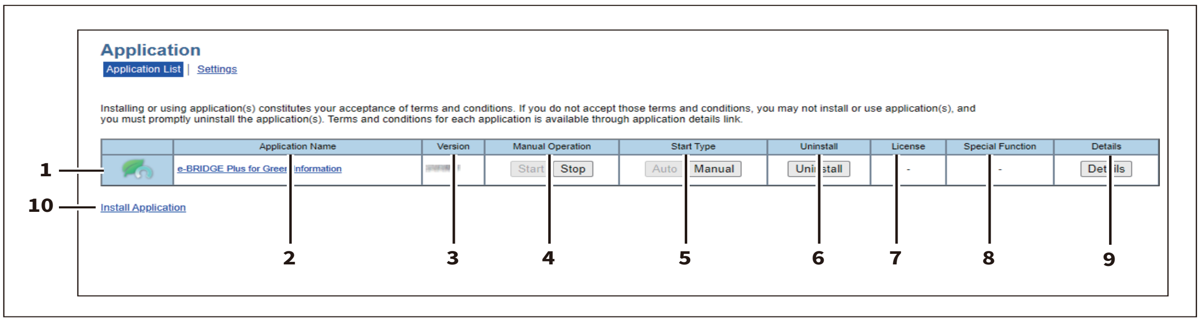
Note

Depending on the applications being used, the following forwarding results performed by the applications are not sent even if items of [Setting up Job Notification Events] are selected.

- A saving result in a storage device for applications.
- A saving result in e-Filing for backup.
- A forwarding result of the received images to a cloud by applications.

Application List

Displays the application list that is already installed.
You can manage operations for each application such as opening/closing, setting the startup method, and uninstalling/installing.



	Item name	Description
1	Application Icon	Displays the application icon.
2	Application Name	Displays the application name. Click the application name to display the application settings page.
3	Version	Displays the application version.
4	Manual Operation	Allows you to start and stop the application manually. This is displayed only when the application package includes the background application. • **Start** — Select this to start the application. • **Stop** — Select this to close the application.
5	Start Type	Changes the applications startup method. This is displayed only when the application package includes the background application. • **Auto** — Select this to start the application automatically after it has been installed or the MFP starts. • **Manual** — Select this to start the application manually.
6	Uninstall	Uninstalls the application. Click this button to display the uninstallation page for the application.
7	License	Displays the installation status of license files to utilize applications. • **-** — Installation of a license file is not necessary. • **Invalid** — An application cannot be used since its license file is not installed. Contact your service technician if you want to use an application with an invalid license. • **Valid** — An application can be used since its license file is installed.
8	Special Function	Contact your service technician or representative for details on Special Function.

	Item name	Description
9	Details	Displays the Application Details screen. By clicking this button, Name, Version, Framework Version, Application ID, Product ID, Authentication, License, Status, Summary, Vendor Name, URL, License Agreement, ReadMe, and Language of an application are displayed. You can set the department or user authentication at the startup of each application. Click [Details] to open [Details] screen, select [Enable] at [Authentication], and click [Save], so that the authentication screen appears at the startup of the application. Select [Disable] and click [Save] not to show the authentication screen. Click [Cancel] to cancel the setting. This [Authentication] setting works at the next startup of the application. It does not appear for the background application.
	Tip • To authenticate users at the application startup, enable “User Authentication According To Function”. • You cannot change [Authentication] for applications that require the authentication and applications that do not have the authentication setting. • The contents of the license agreement are displayed by clicking “Display” in License Agreement. • “Language” is displayed when the application contains the language pack. • [Enable] is displayed for [Use Received Document] if [Enable] is selected for [Enable Received Forward] in the equipment in which an application which uses received documents (an image file received by fax) is installed.	
10	Install Application	Installs the application. Click this link to display the installation page for the application. You can specify the file name for the distribution package on this page, and then install.
	Tip • Installing or using application(s) constitutes your acceptance of the terms and conditions. If you do not accept those terms and conditions, uninstall the application(s). Terms and conditions for each application is available through application details link. • You need to acquire the application’s distribution package in advance. • When installing multiple application packages, install them one at a time. • Only one application which uses received documents (an image file received by fax) can be installed in one unit of equipment. If an attempt is made to install another application in such equipment, “Max. number of registration exceeded. No more registration is allowed.” is displayed. • If a message appears to tell the framework version is old when you install an application, update the system of this equipment. For details, contact your service technician.	

3

AirPrint FUNCTION

When Security Certificate Expired and AirPrint Becomes Unusable

When expiration of the qualification information of the encryption is displayed on the macOS screen being operated and macOS AirPrint Print, macOS AirPrint Fax and macOS AirPrint Scan which use the security communication (*1 or *2) for AirPrint have become unusable, reperform the creation in [self-signed certificate] of [Device Certificate] on TopAccess. For details, see the following reference.
TopAccess Guide: “Chapter 8: [Administration] Tab” - “[Security] How to Set and How to Operate” - “Installing a device certificate”

*1: Enable IPP: Enable, Enable SSL/TLS: Enable
For details, see the following reference.
TopAccess Guide: “Chapter 8: [Administration] Tab” - “[Setup] How to Set and How to Operate” - “Print Service settings”

*2: Secure Scan (SSL/TLS): Enable
For details, see the following reference.
Operator’s Manual for AirPrint: “Chapter 1: USING THE AirPrint FUNCTION” - “Setting up AirPrint in TopAccess” - “Enabling or Disabling AirPrint”

Tip

- iOS AirPrint Print can be used.
- From the viewpoint of the security measures, it is recommended to set 13 months for [Validity Period] of [self-signed certificate].
- After new settings have been made for [self-signed certificate], click [Resume] on the print restart pop-up screen displayed at the first use of AirPrint. After the second time, this pop-up screen is not displayed.

Precautions for AirPrint

■ When using AirPrint Fax

You can use numbers 0 to 9 and symbols “*”, “#”, “-” and “p”. “-” and “p” function as pause and “#” functions as tone switching, too. In the transmission history of this equipment, “p” is indicated by “-”.

4

THE FUNCTION LIST

Function List (Administrator)

FAX

Function	Description	User
Received Forward Setting for Application - Enable Received Forward?	Shows whether Fax Received Forward is enabled or disabled.	NO
Received Forward Setting for Application - Backup Setting?	Shows whether backing up of a received fax is enabled or disabled.	NO

NETWORK SETTING - SESSION - SMB SESSION

Function	Description	User
SMB 1.0 SUPPORT FOR SERVER	Shows whether the SMB 1.0 server is enabled or disabled.	NO
SMB 1.0 SUPPORT FOR CLIENT	Shows whether the SMB 1.0 client is enabled or disabled.	NO

NETWORK SETTING - SESSION - BONJOUR SESSION

Function	Description	User
CHROME OS PRINT	Shows whether the Chrome OS Print service is enabled or disabled.	NO

INDEX

FC-2010AC/2510AC
FC-2515AC/3015AC/3515AC/4515AC/5015AC
DP-2018A/2518A/3018A/3518A/4518A/5018A
FC-5516AC/6516AC/7516AC
DP-5518A/6518A/7518A/8518A
FC-330AC/400AC
OME21007100

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for the Latest Functions

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

Toshiba Tec Corporation

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN

Ver00 F Issued in May 2021