

Regarding the measure against vulnerability measure of RSA Key generation

Contents

Preface	2
Checking whether You Must Perform the Additional Procedures	5
RSA Key Usage and Additional Procedure	12
Procedure for TLS	13
Step 1: Regenerating the Key and Certificate (for TLS)	14
Step 2: Resetting the Key and Certificate (for TLS)	21
Step 3: Deleting a Key/Certificate Generated in the Past (for TLS)	23
Step 4: Disabling the Certificate (for TLS)	25
Step 5: Enabling the New Certificate (for TLS)	26
Procedure for IEEE 802.1X	27
Step 1: Checking the Authentication Method (for IEEE 802.1X)	28
Step 2: Regenerating the Key and Certificate (for IEEE 802.1X)	30
Step 3: Resetting the Key and Certificate (for IEEE 802.1X)	37
Step 4: Deleting a Key/Certificate Generated in the Past (for IEEE 802.1X)	40
Step 5: Disabling the Certificate (for IEEE 802.1X)	42
Step 6: Enabling the New Certificate (for IEEE 802.1X)	43
Procedure for IPSec	44
Step 1: Checking the Authentication Method (for IPSec)	45
Step 2: Regenerating the Key and Certificate (for IPSec)	47
Step 3: Resetting the Key and Certificate (for IPSec)	54
Step 4: Deleting a Key/Certificate Generated in the Past (for IPSec)	57
Step 5: Disabling the Certificate (for IPSec)	59
Step 6: Enabling the New Certificate (for IPSec)	60
Procedure for SIP	61
Step 1: Checking the Settings (for SIP)	62
Step 2: Regenerating the Key and Certificate (for SIP)	65
Step 3: Resetting the Key and Certificate (for SIP)	71
Step 4: Deleting a Key/Certificate Generated in the Past (for SIP)	74
Step 5: Disabling the Certificate (for SIP)	
Step 6: Enabling the New Certificate (for SIP)	
Procedure for Device Signatures	
Step 1: Checking the S/MIME Settings (for Device Signatures)	79
Step 2: Regenerating the Key and Certificate (for Device Signatures)	81
Step 3: Disabling the Certificate (for Device Signatures)	82
Step 4: Enabling the New Certificate (for Device Signatures)	83
Additional Procedures for Bluetooth Settings	86

Procedure for Bluetooth	 87

Step 1: Deleting the Device Registered in Canon PRINT Business (for Bluetooth)	38
Step 2: Registering the Device to Canon PRINT Business Again (for Bluetooth)	39

Additional Procedures for Access Management System Settings	
Procedure for Access Management System	

Preface

Preface

You must update the firmware and perform additional procedures described in this document, in order to upgrade an RSA key that is created with a vulnerable encryption library.

First, check the model and version of your machine.

If you find the model and version of your machine on this page, update the firmware, then perform the additional procedures described in this document. **Checking whether You Must Perform the Additional Procedures(P. 5)** For information on updating the firmware, see the website where you obtained this document.

Checking the Version of Your Machine

Follow the procedure below to check the version of your machine.

Start the Remote UI.

- 2 Click [Status Monitor/Cancel] on the portal page.
- 3 Click [Device Information] > check [Controller] in [Version Information].

Models and Versions Requiring the Additional Procedures

Models	Versions
- iR-ADV 4545 / 4535 / 4525	Ver 59.39 to Ver 67.30
- iR-ADV 715 / 615 / 525	
- iR-ADV 6575 / 6565 / 6560 / 6555	
- iR-ADV 8505 / 8595 / 8585	
- iR-ADV C3530 / C3520	
- iR-ADV C7580 / C7570 / C7565	
- iR-ADV C5560 / C5550 / C5540 / C5535	
- iR-ADV C355 / C255	
- iR-ADV C356 / C256	
- iR-ADV 4545 III / 4535 III / 4525 III	Ver 29.39 to Ver 37.30
- iR-ADV 715 III / 615 III / 525 III	
- iR-ADV 6575 III / 6565 III / 6560 III	
- iR-ADV 8505 III / 8595 III / 8585 III / 8505B III / 8595B III / 8585B III	
- iR-ADV C3530 III / C3520 III	
- iR-ADV C7580 III / C7570 III / C7565 III	
- iR-ADV C5560 III / C5550 III / C5540 III / C5535 III	
- iR-ADV C356 III	
- iR-ADV C475 III	
- iPR C165 / C170	
- iR-ADV 4725 / 4735 / 4745	Ver 17.44 to Ver 27.30
- iR-ADV 8705 / 8705B / 8795 / 8795B / 8786 / 8786B	
- iR-ADV C3730 / C3720	

Preface

Models	Versions
- iR-ADV C7780 / C7770 / C7765	
- iR-ADV C357	Ver 19.34 to Ver 27.30
- iR-ADV C477	
- iR-ADV C5760 / C5750 / C5740 / C5735	Ver 19.40 to Ver 27.30
- iR-ADV 6765 / 6780	Ver 17.44 to Ver 27.33
- iR-ADV C5870 / C5860 / C5850 / C5840	Ver 03.11 to Ver 17.32
- iR-ADV 6860 / 6870	Ver 05.25 to Ver 17.32
- iR-ADV C3830 / C3826 / C3835	Ver 06.28 to Ver 17.32
- iR-ADV C568	Ver 04.13 to Ver 17.08
- iR C3226 / C3222	Ver 01.12 to Ver 02.13
- iR2425	Ver 02.06 to Ver 05.00
- iR2635 / iR2645 / iR2630 / iR2625	Ver 130.0.117 to Ver 707.0.701

NOTE

• The screenshots used in this document may differ from the ones you actually see, depending on the model of your machine. For details on the screenshots, see the manual for your machine on the online manual website.

https://oip.manual.canon/

Checking whether You Must Perform the Additional Procedures

Checking whether You Must Perform the Additional Procedures

Carry out the following three operations to check the additional procedures you must perform. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

Checking the RSA Key(P. 5)

Checking the Bluetooth Settings(P. 8)

Checking the Access Management System Settings(P. 8)

Checking for an RSA key is not required if "Default Key" or "AMS" appears for a key registered in your machine. Check the Bluetooth settings and Access Management System settings, and perform the additional procedures if required.

NOTE

• The screenshots used in this document are only an example. They may differ from the ones you actually see, depending on the model of your machine.

Checking the RSA Key

Check whether there is an RSA key. If there is an RSA key generated with the machine, check the key usage.

Using the Control Panel(P. 5)Using the Remote UI(P. 6)

Using the Control Panel

- 1 Press 🔯 (Settings/Registration).
- Press <Management Settings> > <Device Management> > <Certificate Settings> > <Key and Certificate List>.
- **Press <Key and Certificate List for This Device>**.
- <Key and Certificate List for This Device> does not appear unless the user signature function is enabled on the machine. In this case, proceed to the next step.

4 Select a key other than <Default Key> and <AMS> that has <Used> displayed for <Status> > press <Certificate Details>. Example screen:

Checking whether You Must Perform the Additional Procedures

🗘 Solinar. 🕫	tana 📹 inter	
«Rey and Certificate aid»		
Gry liane	Dates	Gel
Default Key	David	
2 ml	Usel	
🖉 yearst signalant http	1968	21 11
		A
		Ψ.
Certificate Defails	Display Use to call in a	
		DX
🖗 Shiha Monther 📃 🗵 System i	Kanagament mode.	a,

5 Check < Public Key>.

Example screen:

 Vesion 	 8.508v5 	
 Serial Number 	• III	Al a
 Signature Algorithm 	 SBA256-REA 	
 locard flat 	* C+P	Al a
 Validity Start Date 	 31/12 2021 	
 Validity End Date 	 31/12 2023 	
+ louer	* (-#	Al s
 Public Key 	+ ISA 20482	
 Certificate Thumbariet 		Diapizy +
 Issued To (Alts, Hame) 		Al a

For a Certificate Other than RSA

You do not need to perform the additional procedures. Press <OK> to close the screen.

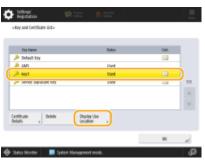
For an RSA Certificate

Proceed to step 6.

- You do not need to perform the additional procedures for the following keys. Press <OK> to close the screen.
- An RSA key that has been generated externally and registered to the machine
- If you must perform the additional procedures, you may need certificate information for disabling the certificate. Make a note of the required information before deleting the key/certificate. Ask the certificate authority that has issued the certificate about the required information.

6 Press <Display Use Location> **>** check the key usage.

Example screen:



Perform the additional procedures according to what appears here. **ORSA Key Usage and Additional Procedure(P. 12)**

■ Using the Remote UI

1 Start the Remote UI ► click [Settings/Registration] ► [Device Management] ► [Key and Certificate Settings].



tificate
1
1
3
1

3 Check [Public Key].

		Verify Certificate
ertificate Details		
Version :	X.509v3	
Serial Number :	00	
Signature Algorithm :	sha256RSA	
Issued To :	C=JP	
Validity Start Date :	31/12/2021	
Validity End Date :	31/12/2023	
Issuer :	C=JP	
Public Key :	RSA 2048bit	
Certificate Thumbprint :	ED18 8EF8 EA2E 796E 3108 6644 ECD6	5 2018 ABAD 4C87
Issued To (Alternate Name) :		

For a Certificate Other than RSA

You do not need to perform the additional procedures.

For an RSA Certificate

Click [Key and Certificate Settings] on the top of the screen > check the key usage.

- Perform the additional procedures according to what appears here. ORSA Key Usage and Additional Procedure(P. 12)
- You do not need to perform the additional procedures for the following keys.
- An RSA key that has been generated externally and registered to the machine
- If you must perform the additional procedures, you may need certificate information for disabling the certificate. Make a note of the required information before deleting the key/certificate. Ask the certificate authority that has issued the certificate about the required information.

Checking the Bluetooth Settings

Check whether Bluetooth is set to <On>. You must perform the additional procedures if it is set to <On>.

Using the Control Panel(P. 8)Using the Remote UI(P. 8)

■ Using the Control Panel

- Press 🔯 (Settings/Registration).
- Press <Preferences> > <Network> > <Bluetooth Settings>.

Check <Use Bluetooth>.

- If <Use Bluetooth> is set to <On>, perform the subsequent procedures. Additional Procedures for Bluetooth Settings(P. 86)
- If <Use Bluetooth> is set to <Off>, you do not need to perform the subsequent procedures.

Using the Remote UI

- Start the Remote UI.
- 2 Click [Settings/Registration] on the portal page.
- 3 Click [Network] ► [Bluetooth Settings].

4 Check [Use Bluetooth].

- If [Use Bluetooth] is selected, perform the subsequent procedures. OAdditional Procedures for Bluetooth Settings(P. 86)
- If [Use Bluetooth] is deselected, you do not need to perform the subsequent procedures.

Checking the Access Management System Settings

Check whether the Access Management System is set to <On>. You must perform the additional procedures if it is set to <On>.

This setting may not appear, depending on your machine. You do not need to perform the additional procedures in that case.

Using the Control Panel(P. 9)Using the Remote UI(P. 9)

Using the Control Panel



2 Press <Management Settings> ► <License/Other> ► <Use ACCESS MANAGEMENT SYSTEM>.

Check < Use ACCESS MANAGEMENT SYSTEM>.

- If <Use ACCESS MANAGEMENT SYSTEM> is set to <On>, perform the subsequent procedures. OAdditional Procedures for Access Management System Settings(P. 91)
- If <Use ACCESS MANAGEMENT SYSTEM> is set to <Off>, you do not need to perform the subsequent procedures.

Using the Remote UI

Start the Remote UI.

2 Click [Settings/Registration] on the portal page.

3 Click [License/Other] > [ACCESS MANAGEMENT SYSTEM Settings].

4 Check [Use ACCESS MANAGEMENT SYSTEM].

- If [Use ACCESS MANAGEMENT SYSTEM] is selected, perform the subsequent procedures. OAdditional Procedures for Access Management System Settings(P. 91)
- If [Use ACCESS MANAGEMENT SYSTEM] is deselected, you do not need to perform the subsequent procedures.

RSA Key Usage and Additional Procedure	. 12
Procedure for TLS	. 13
Step 1: Regenerating the Key and Certificate (for TLS)	14
Step 2: Resetting the Key and Certificate (for TLS)	. 21
Step 3: Deleting a Key/Certificate Generated in the Past (for TLS)	23
Step 4: Disabling the Certificate (for TLS)	25
Step 5: Enabling the New Certificate (for TLS)	26
Procedure for IEEE 802.1X	. 27
Step 1: Checking the Authentication Method (for IEEE 802.1X)	. 28
Step 2: Regenerating the Key and Certificate (for IEEE 802.1X)	. 30
Step 3: Resetting the Key and Certificate (for IEEE 802.1X)	37
Step 4: Deleting a Key/Certificate Generated in the Past (for IEEE 802.1X)	. 40
Step 5: Disabling the Certificate (for IEEE 802.1X)	. 42
Step 6: Enabling the New Certificate (for IEEE 802.1X)	. 43
Procedure for IPSec	. 44
Step 1: Checking the Authentication Method (for IPSec)	45
Step 2: Regenerating the Key and Certificate (for IPSec)	47
Step 3: Resetting the Key and Certificate (for IPSec)	. 54
Step 4: Deleting a Key/Certificate Generated in the Past (for IPSec)	57
Step 5: Disabling the Certificate (for IPSec)	59
Step 6: Enabling the New Certificate (for IPSec)	
Procedure for SIP	61
Step 1: Checking the Settings (for SIP)	62
Step 2: Regenerating the Key and Certificate (for SIP)	. 65
Step 3: Resetting the Key and Certificate (for SIP)	71
Step 4: Deleting a Key/Certificate Generated in the Past (for SIP)	. 74
Step 5: Disabling the Certificate (for SIP)	. 76
Step 6: Enabling the New Certificate (for SIP)	. 77
Procedure for Device Signatures	. 78
Step 1: Checking the S/MIME Settings (for Device Signatures)	
Step 2: Regenerating the Key and Certificate (for Device Signatures)	. 81

Step 3: Disabling the Certificate (for Device Signatures)	82
Step 4: Enabling the New Certificate (for Device Signatures)	83

Refer to "Additional Procedures" and perform them according to the key usage.

RSA Key Usage	Conditions	Additional Procedures
TLS	You must perform the additional procedures in any conditions.	Procedure for TLS(P. 13)
IEEE 802.1X	You must perform the additional procedures if the IEEE 802.1X authentication method is set to EAP-TLS.	Procedure for IEEE 802.1X(P. 27)
IPSec	You must perform the additional procedures if the IKE authentication method is set to the digital signature method.	Procedure for IPSec(P. 44)
SIP	You must perform the additional procedures if TLS is used.	OProcedure for SIP(P. 61)
Device Signature	 You must perform the additional procedures in the following cases: When a digital signature is added to sent files using a key for device signatures When encryption is enabled in the S/MIME encryption settings 	OProcedure for Device Signatures(P. 78)

NOTE

• The screenshots used in this document are only an example. They may differ from the ones you actually see, depending on the model of your machine.

Procedure for TLS

- Step 1: Regenerating the Key and Certificate (for TLS)(P. 14)
- Step 2: Resetting the Key and Certificate (for TLS)(P. 21)
- Step 3: Deleting a Key/Certificate Generated in the Past (for TLS)(P. 23)
- Step 4: Disabling the Certificate (for TLS)(P. 25)
- Step 5: Enabling the New Certificate (for TLS)(P. 26)

Step 1: Regenerating the Key and Certificate (for TLS)

You can generate three types of certificates for a key generated with the machine: a self-signed certificate, CSR certificate, and SCEP certificate. The procedure differs according to the type of certificate. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

For a Self-Signed Certificate(P. 14)
For a CSR Certificate(P. 17)
For an SCEP Certificate(P. 19)

For a Self-Signed Certificate

Using the Control Panel(P. 14)Using the Remote UI(P. 15)

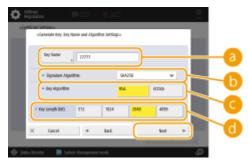
Using the Control Panel

Press 💽 (Settings/Registration).

Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Generate Key> ► <Generate Network Communication Key>.

3 Configure the required settings and proceed to the next screen.

Example screen:



👩 <Key Name>

Enter a name for the key. Enter a name that will be easy to find in a list.

🕒 <Signature Algorithm>

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms. If you select <RSA> for (, and set <Key Length (bit)> to <1024> or more for (, you can select the SHA384 and SHA512 hash algorithms.

🔁 <Key Algorithm>

Select the key algorithm. If you select <RSA>, <Key Length (bit)> appears as a setting item for 1. If you select <ECDSA>, <Key Type> appears instead.

📵 <Key Length (bit)>/<Key Type>

Specify the key length if you select <RSA> for (G), or specify the key type if you select <ECDSA>. In both cases, a higher value provides greater security but reduces the communication processing speed.

▲ Configure the necessary items for the certificate > press <Generate Key>.

Example screen:

🐴 they using the m	umaric lugis.			
Salidity Start: Sale	F (Tuildty End Dele		
Country/Merginal	United Ringdom (SE)	Brganization		
924+ s		brgonization Brit		
os ,		Common Visite	J	

Contemporal Contemporal Contemporal Contemporation Contemporatio Contemporation Contemporatio

Enter the start date and end data of the validity period for the certificate.

Country/Region>/<State>/<City>/<Organization>/<Organization Unit>

Select the country code from the list, and enter the location and the organization name.

🧿 <Common Name>

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

Using the Remote UI

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** Click [Generate Key].
- **5** Click [Network Communication].
- **6** Configure the key and certificate settings.

Settings/Registration			E-Mail	to System Manager
nestart pevice	Settings/Registration : Management Setti	ngs : Denite Management = Kay and Car	tificate Settings = Oers	erate Key =
Apply setting changes	Generate Network Communication Key Generate Network Comm	unication Key	Last Undated	2821 01:03 1:2657
denarco	Selferate Hetwork Comm	anication ney		cancel
Raper Settings			OK	Cancel
TimeryEnergy Settings	Key Name :			
Network Settings	Signature Algorithm :	SHA256 M		
-	Key Algorithm :	RSA 2048-b€ ₩		
External interface		⊖ ECDSA P256 ♥		
i/olume Settings	Certificate Settings			
Sjurtment/Waintmance	Valid By Start Date (YYV/MM/DC) :	7 7		
Azjunt Image Quality	Validity End Data (YYY)/MM(DD) :	/ /		
Maintenance	Country/Region :	(E) Select Country/Region Name		
ncton Settings		Apen 0P1 Enter Internet Country Code		
Common Settings				
Asister	State :			
Send	City:			
	Organization :		<u> </u>	
leceive .	Organization Unit :			

🔁 [Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms.

🔁 [Key Algorithm]

Select [RSA] or [ECDSA] as the key generation algorithm. Specify the key length if you select [RSA], or specify the key type if you select [ECDSA]. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

• If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

🚯 [Validity Start Date (YYYY/MM/DD)]/[Validity End Date (YYYY/MM/DD)]

Enter the start date and end data of the validity period for the certificate. You cannot set [Validity End Date (YYYY/MM/DD)] to a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]

Click [Select Country/Region Name] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[[State]/[City]

Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]

Enter the organization name using alphanumeric characters as necessary.

🚹 [Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key. You can configure this setting only from the Remote UI.

■ 1. Generating a Key and CSR

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].
- **4** Click [Generate Key].
- **5** Click [Key and Certificate Signing Request (CSR)].
- **6** Configure the key and certificate settings.

		Te Portal	Login User : Adm	inistrator Log Out
Settings/Registration				
Restart Device	tetting (the gistuation : Managenew Generate Key and Certificate Signir	rt settings : mexice Management > Key and certific	ato tartings > tara	nata Kay >
Apply Setting Changes		tificate Signing Request (CSR)	Last: Updatad : 2	021 01/02 23:1658
For less mans.	,		OK	Cancel
Papersettings	Key Name :			
Times brongy sattings	Signature Algorithm:	1-6239 V		\rightarrow
Network Settings	Key Algorithm :	* RSA 28-68-581 V - RCBSA P236 V		
External interface Volume Settings	Certificate Signing Request (CS)			
djuranent/Maintenance Acjust Irrage Quality Maintenance	Country/Region :	Select Country/Region Name Lapan (P) Index Internet Countly Code		
unction Settings	Sala:			
Common Settings	city:			
nine	Organization :			
sant	Cryanisation Unit :			
Facative	Common Name :			
Store/Access Riles	Ŧ			
fanagere ent Settinge				
User Hanagement				
Desice Management				
License/Dther				

🔁 [Key Name]

Enter a name for the key. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature.

🕒 [Key Algorithm]

Select the key algorithm, and specify the key length if you select [RSA], or specify the key type if you select [ECDSA].

[Country/Region]

Select the country code from the list, or enter it directly.

[State]/[City]

Enter the location.

[Organization]/[Organization Unit]

Enter the organization name.

🕑 [Common Name]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

7 Click [OK].

- The CSR data appears.
- If you want to save the CSR data to a file, click [Store in File] and specify the save location.

NOTE:

• The key that has generated the CSR appears on the key and certificate list screen, but you cannot use the key by itself. To use this key, you need to register the certificate that is later issued based on the CSR.

Request the certificate authority to issue a certificate based on the CSR data.

■ 2. Registering the Issued Certificate to the Key

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** In the [Certificate] list, click 🛄 for the certificate that you want to register.

			To Ports	d Login User: Administrator Log Ou
Settings/Registration				E-Mail to System Manage
Restart Device	Settings/Regi	stration : Manageme	ent Settings : Device Management > Key and C	etilicate Settings
Apply Setting Changes	Key and	Certificate S	ettings	Last Updated : 2021 01/02 23:10/46
Praferences	Delete	Generate Key	Register Key and Certificate	
Paper Settings	select R	cey Name	Key Usage	certificate
Timet/Energy Settings	0	🔎 Defealt Key		6
Network Settings	0	🔎 Default Key	17130	C
External Interface	0	🔎 AMS	(Access Control)	10
Volume Settings	0	🔎 сэя		
idjustment/Walntenance Acjust image Quality	×			
Maintesance				
anction Settings				
Common Settings				
Animber				
Send				
lacative				
Dore/Access Files				
anagement SetEngs				
iser Management				
texi ce Management				
Lanca webar				



5 Register the certificate.

• Click [Browse...] > specify the file (certificate) to register > click [Register].

For an SCEP Certificate

Manually request the SCEP server to issue a certificate. You can configure this setting only from the Remote UI.

NOTE

• You cannot send a manual request for issuing a certificate if [Enable Timer for Certificate Issuance Auto Request] is selected. Deselect it if it is selected.

Start the Remote UI > click [Settings/Registration] > [Device Management] > [Settings for Certificate Issuance Request (SCEP)] > [Settings for Certificate Issuance Auto Request] > deselect [Enable Timer for Certificate Issuance Auto Request] > click [Update].

```
1 Start the Remote UI.
```

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] > [Settings for Certificate Issuance Request (SCEP)].

4 Click [Certificate Issuance Request].

5 Configure the settings required for requesting a certificate.

	To Portal Login User: Administrator Log Out
ance Request (SCEP)	
settings for certificate issuance Ne	quest dictrin i certificate assance itequest
Certificate Issuance Re	-
	Send Request Cancel
Certificate Issuance Request	
Key Name:	
signature Algorithm	SHA256 M
Key Length (bit)	READER V
Organization:	
Common Name:	
Challenge Password	
Key Use Location	@Nate
	011.5 01666 602:0X
	DIPSK IPSec1 M
x	
	bettings for Certificate Issuance Re Certificate Issuance Reposit Reg Name: Signature Algorithms Reg Longith (ER): Organization: Common Name: Cholenge Personnt

🔁 [Key Name:]

Enter a name for the key. Enter a name that will be easy to find in a list.

[Signature Algorithm:]

Select the hash algorithm to use for the signature.

🧿 [Key Length (bit):]

Select the key length.

[Organization:]

Enter the organization name.

🕒 [Common Name:]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

[Challenge Password:]

When a password is set on the SCEP server side, enter the challenge password included in the request data (PKCS#9) for requesting a certificate to be issued.

[Key Use Location:]

Select [TLS].

NOTE:

• When selecting something other than [None], enable each function in advance. If a certificate is successfully obtained with each function disabled, the certificate is assigned to the key use location, but each function is not automatically enabled.

6 Click [Send Request].

7 Click [Restart].

Step 2: Resetting the Key and Certificate (for TLS)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI. This procedure is not required for an SCEP certificate.

For a Self-Signed Certificate/CSR Certificate

Using the Control Panel(P. 21)Using the Remote UI(P. 22)

- Using the Control Panel
 - Press 🔯 (Settings/Registration).
 - Press <Preferences> > <Network> > <TCP/IP Settings> > <TLS Settings>.
 - Press <Key and Certificate>.
 - Select the key and certificate to use for TLS encrypted communication > press <Set as Default Key> > <Yes>.

Example screen:



• If you want to use the preinstalled key and certificate, select <Default Key>.

NOTE:

• TLS encrypted communication cannot use <Device Signature Key>, which is used for device signatures, or <AMS>, which is used for access restrictions.

5 Press <OK>.

6 Press 🔯 (Settings/Registration) ► <Apply Setting Changes> ► <Yes>.

The machine restarts, and the settings are applied.

■ Using the Remote UI

1 Start the Remote UI.

- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Network] > [TLS Settings].

4 Click [Key and Certificate].

5 Click [Use] for the key and certificate to use for TLS encrypted communication.

			To Portal	Lagin User:	Administrator Log Out
Settings/Registration					E-Mail to System Manager
Restart Device	Settings/Registration : Preference	en : Network Settings > 11.5 Setting	s > Key and Cer	ificate Setting	5
Apply setting changes	Key and Certificate 5	settings		Last Updates	41 2021 01/05 1:24:35 📌
Preferences	Key and Certificate to Use				
Raper Settings	Registered Key and Certifica	An .			
	Key Name	Key Usage	0	rtificate 🦰	
TimeoEnergy Settings	🔎 Detsuit Key		1	2	Lise
Network Settings	🔎 Detault Key	(7.5)			Usa
external interface					

• If you want to use the preinstalled key and certificate, select [Default Key].

6 Click [Apply Set. Changes] to restart the machine.

The machine restarts, and the settings are applied.

Step 3: Deleting a Key/Certificate Generated in the Past (for TLS)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

NOTE

You may need to convey information to the certificate authority when disabling the certificate. See C
 Checking whether You Must Perform the Additional Procedures(P. 5) , and make a note of the required information before deleting the key/certificate.

Using the Control Panel(P. 23)Using the Remote UI(P. 24)

Using the Control Panel



- Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Key and Certificate List> ► <Key and Certificate List for This Device>.
- <Key and Certificate List for This Device> does not appear unless the user signature function is enabled on the machine. In this case, proceed to the next step.

Select the key and certificate > press <Delete> > <Yes>.

Example screen:



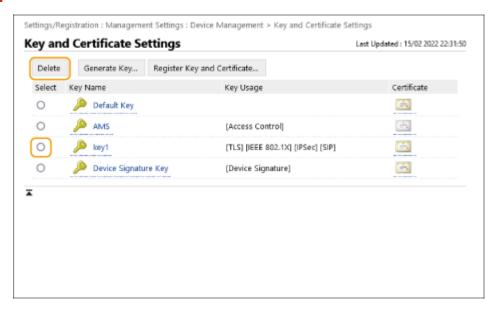
NOTE:

- If \chi appears, the key is corrupt or invalid.
- If 🛅 does not appear, the certificate for the key does not exist.
- If you select a key and certificate and press <Certificate Details>, detailed information about the certificate appears. You can also press <Verify Certificate> on this screen to check whether the certificate is valid.

Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].

4 Select the key and certificate > click [Delete] > [OK].



NOTE

- If \chi appears, the key is corrupt or invalid.
- If 🔄 appears, the certificate for the key does not exist.
- Click a key name to display detailed information about the certificate. You can also click [Verify Certificate] on this screen to check whether the certificate is valid.

Step 4: Disabling the Certificate (for TLS)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered in a computer or Web browser as a trusted certificate, delete the registered certificate.

■ For a CSR/SCEP Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in a computer or Web browser that communicates with the machine, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 5: Enabling the New Certificate (for TLS)

Enable the certificate that is newly generated on the machine.

■ For a Self-Signed Certificate

Register the new certificate to the computer or Web browser as a trusted certificate.

■ For a CSR/SCEP Certificate

You do not need to perform the additional procedures.

Procedure for IEEE 802.1X

- Step 1: Checking the Authentication Method (for IEEE 802.1X)(P. 28)
- Step 2: Regenerating the Key and Certificate (for IEEE 802.1X)(P. 30)

Step 3: Resetting the Key and Certificate (for IEEE 802.1X)(P. 37)

Step 4: Deleting a Key/Certificate Generated in the Past (for IEEE 802.1X)(P. 40)

Step 5: Disabling the Certificate (for IEEE 802.1X)(P. 42)

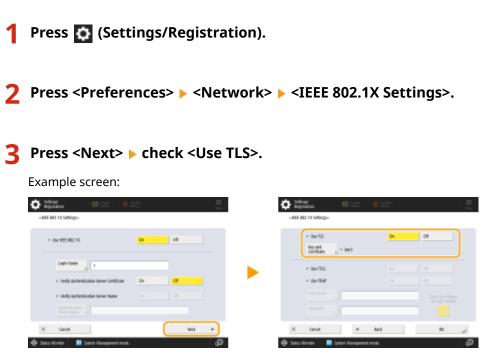
Step 6: Enabling the New Certificate (for IEEE 802.1X)(P. 43)

Step 1: Checking the Authentication Method (for IEEE 802.1X)

You must perform the subsequent procedures if the IEEE 802.1X authentication method is set to EAP-TLS. Follow the procedure below to check the authentication method. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

OUsing the Control Panel(P. 28) OUsing the Remote UI(P. 28)

■ Using the Control Panel



- If <Use TLS> is set to <On> and a key name appears for <Key and Certificate>, perform the subsequent procedures.
- If <Use TLS> is set to <Off>, you do not need to perform the subsequent procedures.

Using the Remote UI

1 Start the Remote UI.

- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Network] **>** [IEEE 802.1X Settings].

4 Check [Use TLS].

Settings/Registration : Preferences : Netwo	ork Settings > IEEE 802.1X Settings		
IEEE 802.1X Settings		Last Updated : 1	5/02 2022 22:34:16
		OK	Cancel
Use IEEE 802.1X			
Login Name :	1		
Verify Authentication Server Certifi	cate		
Verify Authentication Server N	ame		
Authentication Server Name :			
Use TLS		ר	
*Set the default key in Key and Certifi	cate Settings under [TLS Settings] to use TLS.		
Key Name :	key1		
Key and Certificate :	Key and Certificate		
Use TTLS			
TTLS Settings (TTLS Protocol) :	 Use MSCHAPv2 Use PAP 		

- If [Use TLS] is selected and a key name appears, perform the subsequent procedures.
- If [Use TLS] is deselected, you do not need to perform the subsequent procedures.

Step 2: Regenerating the Key and Certificate (for IEEE 802.1X)

You can generate three types of certificates for a key generated with the machine: a self-signed certificate, CSR certificate, and SCEP certificate. The procedure differs according to the type of certificate. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

For a Self-Signed Certificate(P. 30) For a CSR Certificate(P. 33) For an SCEP Certificate(P. 35)

For a Self-Signed Certificate

OUsing the Control Panel(P. 30) OUsing the Remote UI(P. 31)

Using the Control Panel

- Press 🚺 (Settings/Registration).
- 2 Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Generate Key> ► <Generate Network Communication Key>.
- **3** Configure the required settings and proceed to the next screen.

Example screen:



60 <Key Name>

Enter a name for the key. Enter a name that will be easy to find in a list.

🜔 <Signature Algorithm>

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms. If you select <RSA> for (\bigcirc , and set <Key Length (bit)> to <1024> or more for (\bigcirc , you can select the SHA384 and SHA512 hash algorithms.

Colored Algorithm>

Select the key algorithm. If you select <RSA>, <Key Length (bit)> appears as a setting item for 🔂. If you select <ECDSA>, <Key Type> appears instead.

📵 <Key Length (bit)>/<Key Type>

Specify the key length if you select <RSA> for C, or specify the key type if you select <ECDSA>. In both cases, a higher value provides greater security but reduces the communication processing speed.

4 Configure the necessary items for the certificate ► press <Generate Key>.

Example screen:



elidity Start Date>/<Validity End Date>

Enter the start date and end data of the validity period for the certificate.

Country/Region>/<State>/<City>/<Organization>/<Organization Unit>

Select the country code from the list, and enter the location and the organization name.

🧿 <Common Name>

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

Using the Remote UI

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** Click [Generate Key].
- **5** Click [Network Communication].
- **6** Configure the key and certificate settings.

Settings/Registration			E-Mai	to System Manager
restart pevice	Settings/Registration : Management Setti	rgs : Device Management = Kay and Car	tificale Settings = Gera	erate Key =
Apply setting changes	Generate Network Communication Key Generate Network Comm	mication Key	Lost Undated	3821 01/03 1/2657
formes	Selected Pretwork Commis	anication ney		cancel
aper Settings			OK	Cancel
imer/Energy Settings	Key Name :			
	Signature Algorithm :	SHA256 Y		
letwork Settings	Key Algorithm:	③ RSA 2046-b∉ ▼		
aternal interface		⊖ ECDSA P256 V		
olume Settings	Certificate Settings			
justment/Waintenaece	Valid by Start Date (1979, MM, DC) :	7 7		
zýunt Image Quality	Validity Ind Data (YYY)/MM(DD) :	/ /		
fainte nance	Country/Region :	(i) Select Country/Region Name		
xtion Settings		□ Repen OP1		
onvition Settings				
Sitter	State :			
	City:			
end	Organization :			
eceive	Organization Unit :			
tore:rAccess niles			\rightarrow	
ragement Settings	Common Name :			

🔁 [Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms.

🔁 [Key Algorithm]

Select [RSA] or [ECDSA] as the key generation algorithm. Specify the key length if you select [RSA], or specify the key type if you select [ECDSA]. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

• If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

🚯 [Validity Start Date (YYYY/MM/DD)]/[Validity End Date (YYYY/MM/DD)]

Enter the start date and end data of the validity period for the certificate. You cannot set [Validity End Date (YYYY/MM/DD)] to a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]

Click [Select Country/Region Name] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[[State]/[City]

Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]

Enter the organization name using alphanumeric characters as necessary.

🚹 [Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key. You can configure this setting only from the Remote UI.

■ 1. Generating a Key and CSR

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].
- 4 Click [Generate Key].
- **5** Click [Key and Certificate Signing Request (CSR)].
- **6** Configure the key and certificate settings.

		Te Portal	Login User : Adm	inistrator Log Out
Settings/Registration				
Restart Device	tetting (the gistuation : Managenew Generate Key and Certificate Signir	rt settings : mexice Management > Key and certific	ato tartings > tara	nata Kay >
Apply Setting Changes		tificate Signing Request (CSR)	Last: Updatad : 2	021 01/02 23:1658
For less mans.	,		OK	Cancel
Papersettings	Key Name :			
Times brongy sattings	Signature Algorithm:	1-6239 V		\rightarrow
Network Settings	Key Algorithm :	* RSA 28-68-581 V - RCBSA P236 V		
External interface Volume Settings	Certificate Signing Request (CS)			
djuranent/Maintenance Acjust Irrage Quality Maintenance	Country/Region :	Select Country/Region Name Lapan (P) Index Internet Countly Code		
unction Settings	Sala:			
Common Settings	city:			
nine	Organization :			
sant	Cryanisation Unit :			
Facative	Common Name :			
Store/Access Riles	Ŧ			
fanagere ent Settinge				
User Hanagement				
Desice Management				
License/Dther				

🔁 [Key Name]

Enter a name for the key. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature.

🕒 [Key Algorithm]

Select the key algorithm, and specify the key length if you select [RSA], or specify the key type if you select [ECDSA].

[Country/Region]

Select the country code from the list, or enter it directly.

[State]/[City]

Enter the location.

[Organization]/[Organization Unit]

Enter the organization name.

[[Common Name]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

7 Click [OK].

- The CSR data appears.
- If you want to save the CSR data to a file, click [Store in File] and specify the save location.

NOTE:

• The key that has generated the CSR appears on the key and certificate list screen, but you cannot use the key by itself. To use this key, you need to register the certificate that is later issued based on the CSR.

Request the certificate authority to issue a certificate based on the CSR data.

■ 2. Registering the Issued Certificate to the Key

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** In the [Certificate] list, click 🛄 for the certificate that you want to register.

RSA Key Usage and Additional Procedure

			To Ports	al Login User: Administrator Log Ou
Settings/Registration				E-Mail to System Manage
Restart Device	Settings/Re	gistration : Nanagem	ent Settings : Device Management > Key and C	ertificate Settings
Apply Setting Changes	Key and	l Certificate S	ettings	Last Updated : 2021 01/02 231046
Praferences	Delete	Generate Key_	Register Key and Certificate	
Paper Settings	select	Key Name	Key Usage	cartificate
Timet/Energy Settings	0	🔎 Defealt Key		<u>65</u>
Network Settings	0	🔎 Default Key	171.50	E5
External interface	0	🔎 AMS	(Access Control)	10
Volume Settings	0	🔎 сая		
idjustment/Walntenance	×			
Adjust image Quality				
Maintenance anction Settings				
Convision Settings				
Deleter				
Send				
leceive				
Store (Access Files				
anagement Settings				
User Management				
toxi te Management				
iner of the second s				



5 Register the certificate.

• Click [Browse...] > specify the file (certificate) to register > click [Register].

For an SCEP Certificate

Manually request the SCEP server to issue a certificate. You can configure this setting only from the Remote UI.

NOTE

• You cannot send a manual request for issuing a certificate if [Enable Timer for Certificate Issuance Auto Request] is selected. Deselect it if it is selected.

Start the Remote UI > click [Settings/Registration] > [Device Management] > [Settings for Certificate Issuance Request (SCEP)] > [Settings for Certificate Issuance Auto Request] > deselect [Enable Timer for Certificate Issuance Auto Request] > click [Update].

```
1 Start the Remote UI.
```

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] > [Settings for Certificate Issuance Request (SCEP)].

4 Click [Certificate Issuance Request].

5 Configure the settings required for requesting a certificate.

	To Portal Login User: Administrator Log Out
ance Request (SCEP)	
settings for certificate issuance Ne	quest dictrin i certificate assance itequest
Certificate Issuance Re	-
	Send Request Cancel
Certificate Issuance Request	
Key Name:	
signature Algorithm	SHA256 M
Key Length (bit)	READER V
Organization:	
Common Name:	
Challenge Password	
Key Use Location	@Nate
	011.5 01666 602:0X
	CIPSIO IPSic1 M
x	
	bettings for Certificate Issuance Re Certificate Issuance Reposit Reg Name: Signature Algorithms Reg Longith (ER): Organization: Common Name: Cholenge Personnt

🔁 [Key Name:]

Enter a name for the key. Enter a name that will be easy to find in a list.

[Signature Algorithm:]

Select the hash algorithm to use for the signature.

🧿 [Key Length (bit):]

Select the key length.

[Organization:]

Enter the organization name.

🕒 [Common Name:]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

[Challenge Password:]

When a password is set on the SCEP server side, enter the challenge password included in the request data (PKCS#9) for requesting a certificate to be issued.

[Key Use Location:]

Select [IEEE 802.1X].

NOTE:

• When selecting something other than [None], enable each function in advance. If a certificate is successfully obtained with each function disabled, the certificate is assigned to the key use location, but each function is not automatically enabled.

6 Click [Send Request].

7 Click [Restart].

Step 3: Resetting the Key and Certificate (for IEEE 802.1X)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI. This procedure is not required for an SCEP certificate.

For a Self-Signed Certificate/CSR Certificate

Using the Control Panel(P. 37)Using the Remote UI(P. 38)

■ Using the Control Panel



Press <Preferences> > <Network> > <IEEE 802.1X Settings>.

Press <On> for <Use IEEE 802.1X> > configure the required settings > press <Next>.

Example screen:



elogin Name>

Enter the name (EAP Identity) of the login user to receive IEEE 802.1X authentication.

<Verify Authentication Server Certificate>

Set this setting to <On> when verifying server certificates sent from an authentication server.

Contemporal Contention Server Name>

To verify a common name in the server certificate, select <On>. Then enter the name of the authentication server where the login user is registered in <Authentication Server Name>.

4 Press <On> for <Use TLS> ▶ press <Key and Certificate>.

5 Select the key and certificate to use in the list **>** press <Set as Default Key> **>** <Yes>.

6 Press <OK>.

Press (Settings/Registration) > (Settings/Registration) > <Apply Set. Changes> > <Yes>.

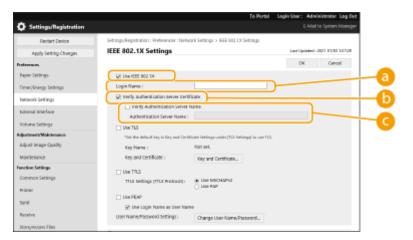
The machine restarts, and the settings are applied.

Using the Remote UI

Start the Remote UI.

- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Network Settings] ▶ [IEEE 802.1X Settings].

4 Select [Use IEEE 802.1X] ▶ configure the required settings.



🔁 [Login Name]

Enter the name (EAP Identity) of the login user to receive IEEE 802.1X authentication.

[Verify Authentication Server Certificate]

Select this check box when verifying server certificates sent from an authentication server.

[Verify Authentication Server Name]

To verify the common name in the server certificate, select this check box. Then enter the name of the authentication server where the login user is registered in [Authentication Server Name].

5 Select [Use TLS] > click [Key and Certificate].

RSA Key Usage and Additional Procedure

	Te Portal	Legin User: Administrator Log Out
Settings/Registration		E-Mail to System Manager
Restart Device	Satings,Registration : Preferences : Network Satings > 1885 802.03 Satings	
Apply Setting Changes	IEEE 802.1X Settings	Last Updated - 3021 01/08 142529
Preimmuns		OK Carrol
Report Settings	27 Use 822 802.18	
Timer/Energy Settings	Login Name :	
Network Settings	[2] Velly authentization terver certificate	
Internal actestica	Verify Authentication Server Name Authentication Server Name :	
Volume Settings	Use TLS	
Adjustment Maintenance	"het ihre diehach key in Key and Deckfastie Leitings ander (713 Leitings) in ose 713.	
Adjust image Quality	Key Name : Not set.	
Maintenance	key and Certificate i Key and Certificate	
Function Settings Common Settings Invisor	Over TRUS True percession (): We have been compared Over percentage	
Send	□ Use RGAP ☑ Use Login Name as User Name	
Receive	User Name/Password Settings i Dhanga User Name/Password	
Store/Access Files		·

6 Click [Use] for the key to use in the list.

7 Click [OK].

8 Click [Apply Setting Changes] to restart the machine.

The machine restarts, and the settings are applied.

Step 4: Deleting a Key/Certificate Generated in the Past (for IEEE 802.1X)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

NOTE

You may need to convey information to the certificate authority when disabling the certificate. See C
 Checking whether You Must Perform the Additional Procedures(P. 5) , and make a note of the required information before deleting the key/certificate.

Using the Control Panel(P. 40)Using the Remote UI(P. 41)

Using the Control Panel



- Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Key and Certificate List> ► <Key and Certificate List for This Device>.
- <Key and Certificate List for This Device> does not appear unless the user signature function is enabled on the machine. In this case, proceed to the next step.

Select the key and certificate ► press <Delete> ► <Yes>.

Example screen:



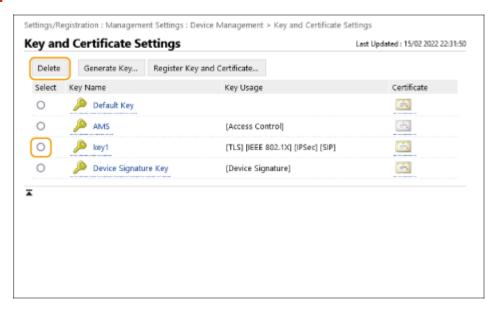
NOTE:

- If \chi appears, the key is corrupt or invalid.
- If 🛅 does not appear, the certificate for the key does not exist.
- If you select a key and certificate and press <Certificate Details>, detailed information about the certificate appears. You can also press <Verify Certificate> on this screen to check whether the certificate is valid.

Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].

4 Select the key and certificate > click [Delete] > [OK].



NOTE

- If \chi appears, the key is corrupt or invalid.
- If 🔄 appears, the certificate for the key does not exist.
- Click a key name to display detailed information about the certificate. You can also click [Verify Certificate] on this screen to check whether the certificate is valid.

Step 5: Disabling the Certificate (for IEEE 802.1X)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered to the IEEE 802.1X authentication server as a trusted certificate, delete the registered certificate.

■ For a CSR/SCEP Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in an IEEE 802.1X authentication server, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 6: Enabling the New Certificate (for IEEE 802.1X)

Enable the certificate.

■ For a Self-Signed Certificate

Register the new certificate to the IEEE 802.1X authentication server as a trusted certificate.

■ For a CSR/SCEP Certificate

You do not need to perform the additional procedures.

Procedure for IPSec

- Step 1: Checking the Authentication Method (for IPSec)(P. 45)
- Step 2: Regenerating the Key and Certificate (for IPSec)(P. 47)
- Step 3: Resetting the Key and Certificate (for IPSec)(P. 54)
- Step 4: Deleting a Key/Certificate Generated in the Past (for IPSec)(P. 57)
- Step 5: Disabling the Certificate (for IPSec)(P. 59)
- Step 6: Enabling the New Certificate (for IPSec)(P. 60)

Step 1: Checking the Authentication Method (for IPSec)

You must perform the subsequent procedures if the authentication method for IKE setting in IPSec is set to <Digital Sig. Method>.

Follow the procedure below to check the authentication method.

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

OUsing the Control Panel(P. 45) OUsing the Remote UI(P. 46)

- Using the Control Panel
 - Press 🔯 (Settings/Registration).
 - Press <Preferences> > <Network> > <TCP/IP Settings> > <IPSec Settings>.

3 Select the registered policy > press <Edit> > <IKE Settings>.

Example screen:

Sting' Singlet	🎓 instan		0 2	Tings' pidation	🛱 baad 🍵 badas	
<plecietings-< td=""><td></td><td></td><td>- 25</td><td>sidta</td><td></td><td></td></plecietings-<>			- 25	sidta		
 Uni PSec 	Ds	04				
 Receive New-Policy Packets 		Aper Reject	100	PA .	ity Name 1	
Anala Balli Ania Kana						
		the Printy			Selector Settings a	
3		# liter	· ·		HE Settings	Orb Alice 255.64
4					Pirchmox	for HIS Rey Length
5		Print EM			Settings a	
Police CwID1 Resident , 6d	, Dekte					
X Canori		ж "	×	× ta		نړ x
🕀 Status Monitor 🛛 🔝 System Hamagemen	rf mode.	Ð	👄 2m	s Monther 📃	System Klanagement mode.	

Press <Next> > check <Authentication Method>.

Example screen:

 Softmary Regionation KE Settings- 	😭 trant 🧉 katal Kata			CRE Settings	🛱 tanj 👘 talj	•	=
• IKZ Mode	Man	Appresire	•	* Judiwritation Method	ter ent centure ,	he-stand Sep Method	Doptini Kig. Method
* Vulidity X Cancel	480 mm. So ther using the r	unericites.		 Authentication/Encryption Canoel 	Algolithes	<u>A.5</u>	Manuf Settings
\ominus Slaka Monter 🛛 🛄 Spil	on Hanupunent mode.	a		🕀 Slatus Monitor 🛛 🛄 Spal	ion Nunupiment mode.		a,

- If <Authentication Method> is set to <Digital Sig. Method> and a key name appears for <Key and Certificate>, perform the subsequent procedures.
- If <Authentication Method> is set to <Pre-Shared Key Method>, you do not need to perform the subsequent procedures.

Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Network Settings] > [IPSec Policy List].
- **4** Click the policy in the list ► click [IKE Settings].

5 Check [Authentication Method].

Œ		Last Updated :	15/02 2022 22:3
		OK	Cancel
KE Mode			
 Main 			
 Aggressive 			
alidity			
Time	480 min. (1-65535)		
uthentication Method			
O Pre-Shared Key Method :	Shared Key Settings		
Digital Signature Method :			
Key Name :	Not set.		
Key and Certificate :	Key and Certificate		

- If [Authentication Method] is set to [Digital Signature Method] and a key name appears, perform the subsequent procedures.
- If <Authentication Method> is set to <Pre-Shared Key Method>, you do not need to perform the subsequent procedures.

Step 2: Regenerating the Key and Certificate (for IPSec)

You can generate three types of certificates for a key generated with the machine: a self-signed certificate, CSR certificate, and SCEP certificate. The procedure differs according to the type of certificate. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

For a Self-Signed Certificate(P. 47)
 For a CSR Certificate(P. 50)
 For an SCEP Certificate(P. 52)

For a Self-Signed Certificate

Using the Control Panel(P. 47)Using the Remote UI(P. 48)

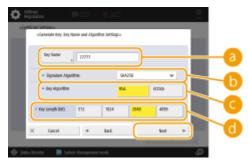
Using the Control Panel

Press 🔯 (Settings/Registration).

Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Generate Key> ► <Generate Network Communication Key>.

3 Configure the required settings and proceed to the next screen.

Example screen:



👩 <Key Name>

Enter a name for the key. Enter a name that will be easy to find in a list.

🕒 <Signature Algorithm>

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms. If you select <RSA> for (, and set <Key Length (bit)> to <1024> or more for (, you can select the SHA384 and SHA512 hash algorithms.

🔁 <Key Algorithm>

Select the key algorithm. If you select <RSA>, <Key Length (bit)> appears as a setting item for 1. If you select <ECDSA>, <Key Type> appears instead.

📵 <Key Length (bit)>/<Key Type>

Specify the key length if you select <RSA> for (G), or specify the key type if you select <ECDSA>. In both cases, a higher value provides greater security but reduces the communication processing speed.

▲ Configure the necessary items for the certificate ▶ press <Generate Key>.

Example screen:

State using the s	umaric legis.		
Salidity Start: Salid	•/	Twildby End Delte	
Country/Briglan	United Ringdom (SB)	Brganization .	
aae "		Brganization	
os ,		Common Hame	

elidity Start Date>/<Validity End Date>

Enter the start date and end data of the validity period for the certificate.

Country/Region>/<State>/<City>/<Organization>/<Organization Unit>

Select the country code from the list, and enter the location and the organization name.

🧿 <Common Name>

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

Using the Remote UI

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** Click [Generate Key].
- **5** Click [Network Communication].
- **6** Configure the key and certificate settings.

RSA Key Usage and Additional Procedure

Settings/Registration			E-Mai	to System Manager
nestart Device	Settings/Registration : Management Setti	ngs : Denice Management = Kay and Car	tiřisete Settings = Gere	orate Key =
Apply setting changes	Generate Network Communication Key Generate Network Comm	unication Key	Last Undated	2821 01:03 1:2657
denares	Selected Pretwork Comm	anication ney		cancel
Raper Settings			OK	Cancel
Timeo@nergy Settings	Key Name :			
Network Settings	Signature Algorithm :	SHA256 Y		
-	Key Algorithm :	RSA 2041-be M		
External interface		⊖ ECDSA P256 ♥		
Volume Settings	Certificate Settings			
Sjurtment/Waintmance	Valid ity Start Date (YYYV/MM/DC) :	7 7		
Azjunt Image Quality	Validity End Data (YYV/MM/DD) :	/ /		
Maintenance	Country/Region :	(8) Select Country/Region Name		
nction Settings		Enter Internet Country Code		
Common Settings				
Asister	State :			
Send	aty:			
	Organization :			
Receive	Organization Unit :			

🔁 [Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms.

🔁 [Key Algorithm]

Select [RSA] or [ECDSA] as the key generation algorithm. Specify the key length if you select [RSA], or specify the key type if you select [ECDSA]. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

• If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

🚯 [Validity Start Date (YYYY/MM/DD)]/[Validity End Date (YYYY/MM/DD)]

Enter the start date and end data of the validity period for the certificate. You cannot set [Validity End Date (YYYY/MM/DD)] to a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]

Click [Select Country/Region Name] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[[State]/[City]

Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]

Enter the organization name using alphanumeric characters as necessary.

🚹 [Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key. You can configure this setting only from the Remote UI.

■ 1. Generating a Key and CSR

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].
- 4 Click [Generate Key].
- **5** Click [Key and Certificate Signing Request (CSR)].
- **6** Configure the key and certificate settings.

		Te Portal	login User : Adm	inistrator Log Out
Settings/Registration				
Restart Device	tetting (the gistuation : Managener Generate Key and Certificate Signin	it settings : mexice Management > Key and certific in Demonst 17528.	ato santings > meas	наля колу >
Apply Setting Changes		tificate Signing Request (CSR)	Last Updated : 2	02101/02231658
ordenenaues.	,		OK	Cancel
Paper Tettings	Key Name :			
timesterogy sattings	Saniture Alcorithm:	1H42356 ¥		$ \rightarrow$
Network Settings	Key Algorithm :	* 854 2346-581 V - 50254 p256 V		
Volume Settings	Contribute Signing Request (CSI			
djartment/Maintenance Adjust Irnage Quality Maintenance	Country/Region :	Select Country/Region Name Inpan (P) Internet Country Code		
action Settings	Station :			
ommon Settings	city:			
sinte	Organization :			
ent	Criganisation Unit I			
acativa	Common Name :			
Store, Access Files	I			
inageneent Settings				
iser Management				
Denica Management				
Licenseillither				

🔁 [Key Name]

Enter a name for the key. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature.

🕒 [Key Algorithm]

Select the key algorithm, and specify the key length if you select [RSA], or specify the key type if you select [ECDSA].

[Country/Region]

Select the country code from the list, or enter it directly.

[State]/[City]

Enter the location.

[Organization]/[Organization Unit]

Enter the organization name.

[[Common Name]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

7 Click [OK].

- The CSR data appears.
- If you want to save the CSR data to a file, click [Store in File] and specify the save location.

NOTE:

• The key that has generated the CSR appears on the key and certificate list screen, but you cannot use the key by itself. To use this key, you need to register the certificate that is later issued based on the CSR.

Request the certificate authority to issue a certificate based on the CSR data.

■ 2. Registering the Issued Certificate to the Key

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** In the [Certificate] list, click 🛄 for the certificate that you want to register.

RSA Key Usage and Additional Procedure

			To Ports	Login User: Administrator Log Ou
🔅 Settings/Registration				E-Mail to System Manage
Restart Device	Settings/Regists	ation : Managem	ent Settings : Device Management > Key and C	etiFicate Settings
Apply Setting Changes	Key and C	ertificate S	ettings	Last Updated : 2021 01/02 23:1846
Praferances	Delete	Generate Key_	Register Key and Certificate	
Report Settings	select. Key	Name	Key Usage	certificate
Timet/Trange Settings	0 🌶	Default Key		6
Network Settings	0 🌶	Default Key	171.50	E5
External Interface	0 🌶	AMS	(Access Control)	10
Volume Settings	0 🖌	сяя		
Acjust Image Quality Maintenance				
ancion Settings				
Common Settings				
Printer				
Send				
lacalivo				
Store/Access Files				
anagement Settings				
Jser Management				
Device Management				
i kanca metar				



5 Register the certificate.

• Click [Browse...] > specify the file (certificate) to register > click [Register].

For an SCEP Certificate

Manually request the SCEP server to issue a certificate. You can configure this setting only from the Remote UI.

NOTE

• You cannot send a manual request for issuing a certificate if [Enable Timer for Certificate Issuance Auto Request] is selected. Deselect it if it is selected.

Start the Remote UI > click [Settings/Registration] > [Device Management] > [Settings for Certificate Issuance Request (SCEP)] > [Settings for Certificate Issuance Auto Request] > deselect [Enable Timer for Certificate Issuance Auto Request] > click [Update].

```
1 Start the Remote UI.
```

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] > [Settings for Certificate Issuance Request (SCEP)].

4 Click [Certificate Issuance Request].

5 Configure the settings required for requesting a certificate.

	To Portal Login User: Administrator Log Out
ance Request (SCEP)	
settings for certificate issuance Ne	quest dictrin i certificate assance itequest
Certificate Issuance Re	-
	Send Request Cancel
Certificate Issuance Request	
Key Name:	
signature Algorithm	SHA256 M
Key Length (bit)	READER V
Organization:	
Common Name:	
Challenge Password	
Key Use Location	@Nate
	011.5 01666 602:0X
	CIPSIO IPSic1 M
x	
	bettings for Certificate Issuance Re Certificate Issuance Reposit Reg Name: Signature Algorithms Reg Longith (ER): Organization: Common Name: Cholenge Personnt

🔁 [Key Name:]

Enter a name for the key. Enter a name that will be easy to find in a list.

[Signature Algorithm:]

Select the hash algorithm to use for the signature.

🧿 [Key Length (bit):]

Select the key length.

[Organization:]

Enter the organization name.

🕒 [Common Name:]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

[Challenge Password:]

When a password is set on the SCEP server side, enter the challenge password included in the request data (PKCS#9) for requesting a certificate to be issued.

[Key Use Location:]

Select [IPSec].

NOTE:

• When selecting something other than [None], enable each function in advance. If a certificate is successfully obtained with each function disabled, the certificate is assigned to the key use location, but each function is not automatically enabled.

6 Click [Send Request].

7 Click [Restart].

Step 3: Resetting the Key and Certificate (for IPSec)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI. This procedure is not required for an SCEP certificate.

For a Self-Signed Certificate/CSR Certificate

Using the Control Panel(P. 54)Using the Remote UI(P. 55)

- Using the Control Panel
 - Press 🔯 (Settings/Registration).
 - Press <Preferences> > <Network> > <TCP/IP Settings> > <IPSec Settings>.
 - **3** Select the policy to reset the key and certificate for ▶ press <Edit> ▶ <IKE Settings>.

Example screen:



4 Press <Next> > select <Digital Sig. Method> in <Authentication Method> > press <Key and Certificate>.

Example screen:

Sellings Replation 1 «KE Sellings»	🛱 tanga 🦉 tanga	All beings-	ina hat. Ina hat.
 IKE Mode 	Man Approxim	+ Juliversization Method	Per-litand Biglat Ng. Rey Method A
* Validby	483 MA. So ther using the numeric large. C 0 05550	a Autorization/sucycliss Applitum	alta Manuf intiga
X Canoel Sultus Monitor 🗾 Spiler	Ked +	X Casol -r Bal Ø Ø Saka Kontor B System Kanagement mote	k DK

5 Select the key and certificate to use in the list > press <Set as Default Key> > <Yes>.

6 Press <OK>.

Press (Settings/Registration) > (Settings/Registration) > <Apply Set. Changes> > <Yes>.

The machine restarts, and the settings are applied.

Using the Remote UI

Start the Remote UI.

2 Click [Settings/Registration] on the portal page.

3 Click [Network Settings] > [IPSec Policy List].

4 Click the policy to reset the key and certificate for in the list **>** click [IKE Settings].

5 Select [Digital Signature Method] in [Authentication Method] ► click [Key and Certificate].

Æ		Last Updated :	15/02 2022 22:3
		OK	Cancel
(E Mode			
 Main 			
 Aggressive 			
alidity			
Time	480 min. (1-65535)		
uthentication Method			
O Pre-Shared Key Method :	Shared Key Settings		
Digital Signature Method :			
Key Name :	Not set.		
Key and Certificate :	Key and Certificate		

6 Click [Use] for the key to use in the list.

7 Click [OK].

8 Click [Apply Setting Changes] to restart the machine.

The machine restarts, and the settings are applied.

Step 4: Deleting a Key/Certificate Generated in the Past (for IPSec)

You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

NOTE

You may need to convey information to the certificate authority when disabling the certificate. See C
 Checking whether You Must Perform the Additional Procedures(P. 5) , and make a note of the required information before deleting the key/certificate.

OUsing the Control Panel(P. 57) Using the Remote UI(P. 58)

Using the Control Panel



- Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Key and Certificate List> ► <Key and Certificate List for This Device>.
- <Key and Certificate List for This Device> does not appear unless the user signature function is enabled on the machine. In this case, proceed to the next step.

Select the key and certificate ► press <Delete> ► <Yes>.

Example screen:



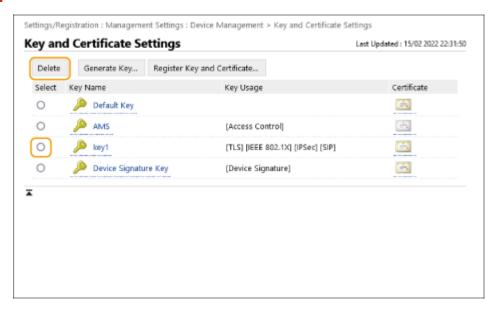
NOTE:

- If \chi appears, the key is corrupt or invalid.
- If 🛅 does not appear, the certificate for the key does not exist.
- If you select a key and certificate and press <Certificate Details>, detailed information about the certificate appears. You can also press <Verify Certificate> on this screen to check whether the certificate is valid.

Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].

4 Select the key and certificate > click [Delete] > [OK].



NOTE

- If \chi appears, the key is corrupt or invalid.
- If 🔄 appears, the certificate for the key does not exist.
- Click a key name to display detailed information about the certificate. You can also click [Verify Certificate] on this screen to check whether the certificate is valid.

Step 5: Disabling the Certificate (for IPSec)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered in the device that communicates with IPSec as a trusted certificate, delete the registered certificate. After deleting the registered certificate, register the certificate of the regenerated key.

■ For a CSR/SCEP Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using a CRL in the device that communicates with IPSec, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 6: Enabling the New Certificate (for IPSec)

Enable the certificate.

■ For a Self-Signed Certificate

Register the new certificate to the device that communicates with IPSec as a trusted certificate.

■ For a CSR/SCEP Certificate

You do not need to perform the additional procedures.

Procedure for SIP

- Step 1: Checking the Settings (for SIP)(P. 62)
- Step 2: Regenerating the Key and Certificate (for SIP)(P. 65)
- Step 3: Resetting the Key and Certificate (for SIP)(P. 71)
- Step 4: Deleting a Key/Certificate Generated in the Past (for SIP)(P. 74)
- Step 5: Disabling the Certificate (for SIP)(P. 76)
- Step 6: Enabling the New Certificate (for SIP)(P. 77)

Step 1: Checking the Settings (for SIP)

You must perform the additional procedures when both of the following conditions are met:

- <Use TLS> is enabled in <Intranet Settings> in <SIP Settings>
- The key name appears for <Key and Certificate> in <TLS Settings> in <SIP Settings>

Follow the procedure below to check the settings.

Using the Control Panel(P. 62)Using the Remote UI(P. 63)

Using the Control Panel

Checking <Use TLS>



2 Press <Preferences> ► <Network> ► <TCP/IP Settings> ► <SIP Settings> ► <Intranet Settings>.

3 Check <Use TLS>.

Example screen:



- If <Use TLS> is set to <On>, proceed to check <Key and Certificate>.
- If <Use TLS> is set to <Off>, you do not need to perform the subsequent procedures.

Checking <Key and Certificate>

1 Press 🔯 (Settings/Registration).

2 Press <Preferences> ► <Network> ► <TCP/IP Settings> ► <SIP Settings> ► <TLS Settings>. **3** Check whether the key name appears for <Key and Certificate>.

Example screen:

Selling: Imposition	(interpretation)	🎓 inches. Secure		
<tti settingo-<="" td=""></tti>				
* BX3rSings				
 Require Cire 	it authentication	D h	CB.	
 Til Settings. 				
 Verify Server 	Certificate	0n	08	
 tellycs 				
Ryand Certificate	- iteji)		
X Garol			DK.	a.
🖗 Saka Honter 💦 📕	System Hanagement	mode.		B

- If a key name appears for <Key and Certificate>, perform the subsequent procedures.
- If the key name does not appear for <Key and Certificate>, you do not need to perform the subsequent procedures.

Using the Remote UI

Checking [Use TLS] and [Key and Certificate]

Start the Remote UI.

2 Click [Settings/Registration] on the portal page.

3 Click [Network Settings] > [SIP Settings].

4 Check [Use TLS] in [Intranet Settings].

SIP Settings CK Cancel Intranet Settings Use Intranet Main Unit URI : SIP RX Port Number : 5060 (1- 65535) SIP TX Transport : UDP UDP USe TLS *Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	Settings/Registration : Preferences : Network Setting	is > SIP Settings		
Intranet Settings Use Intranet Main Unit URI: SIP RX Port Number: S060 (1-65533) SIP TX Transport: UDP UDP Use TLS *Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	SIP Settings	La	st Updated : 15/02.2	022 22:36:05 🛟
 ✓ Use Intranet Main Unit URI : SIP RX Port Number : S060 (1-65535) SIP TX Transport : UDP TCP ✓ Use TLS *Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual 			ОК	Cancel
Main Unit URI : SIP RX Port Number : 5060 (1-65535) SIP TX Transport : UDP © TCP Vuse TLS *Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	Intranet Settings			
SIP RX Port Number : 5060 (1- 65535) SIP TX Transport : UDP UDP Use TLS "Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	🛃 Use intranet			
SIP TX Transport : UDP TCP Use TLS "Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	Main Unit URI :			
TCP Use TLS "Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	SIP RX Port Number :	5060 (1-65535)		
"Set the default key in Key and Certificate Settings under [TLS Settings] to use TLS. Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual	SIP TX Transport :	0		
Always Use Specified SIP Server SIP Server Address Acquisition Method : Manual		s Settings under [TLS Settings] to use TLS.		
SIP Server Address Acquisition Method : Manual 				
O DHCP O DHCPv6	SIP Server Address Acquisition Method :	 DHCP 		
*Depending on the IPv4 or IPv6 settings, the method used may be (Manual).	*Depending on the IPv4 or IPv6 settings,	the method used may be (Manual).		

- If [Use TLS] is selected, proceed to check [Key and Certificate].
- If [Use TLS] is deselected, you do not need to perform the subsequent procedures.

5 Check [Key Name] in [TLS Settings].

media (1.36) Settings		
T.38 TX Transport :	UDPTL	
T.38 Media Type :	image	
T.38 RX Port Number :	49152 (1-65535)	
RTP RX Port Number :	5004 (1024-65534)	
FLS Settings		
Key Name	key1	
	Key and Certificate	
RX Settings		
Require Client Authenticatio	n	
TX Settings		
Verify Server Certificate		
Add CN to Verification	Items	
•		

- If a key name appears, perform the subsequent procedures.
- If the key name does not appear, you do not need to perform the subsequent procedures.

Step 2: Regenerating the Key and Certificate (for SIP)

You can generate two types of certificates for a key generated with the machine: a self-signed certificate and CSR certificate. The procedure differs according to the type of certificate. You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

For a Self-Signed Certificate(P. 65)
 For a CSR Certificate(P. 68)

For a Self-Signed Certificate

Using the Control Panel(P. 65)Using the Remote UI(P. 66)

Using the Control Panel

Press 🔯 (Settings/Registration).

2 Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Generate Key> ► <Generate Network Communication Key>.

3 Configure the required settings and proceed to the next screen.

Example screen:



60 <Key Name>

Enter a name for the key. Enter a name that will be easy to find in a list.

🕞 <Signature Algorithm>

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms. If you select <RSA> for (\bigcirc , and set <Key Length (bit)> to <1024> or more for (\bigcirc , you can select the SHA384 and SHA512 hash algorithms.

🔁 <Key Algorithm>

Select the key algorithm. If you select <RSA>, <Key Length (bit)> appears as a setting item for 1. If you select <ECDSA>, <Key Type> appears instead.

📵 <Key Length (bit)>/<Key Type>

Specify the key length if you select <RSA> for (G), or specify the key type if you select <ECDSA>. In both cases, a higher value provides greater security but reduces the communication processing speed.

▲ Configure the necessary items for the certificate > press <Generate Key>.

Example screen:

🖐 totor using the r	umaric large.			
Set Set	€(** ****	Twildty End Delte	**)—(
Country Manufact	United Ringstom (SIE)	Brganization		
924+ "		branization int ,		
05		Common Harter		

Contemporal Contemporal Contemporal Contemporation Contemporatio Contemporation Contemporatio

Enter the start date and end data of the validity period for the certificate.

Country/Region>/<State>/<City>/<Organization>/<Organization Unit>

Select the country code from the list, and enter the location and the organization name.

🧿 <Common Name>

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

Using the Remote UI

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** Click [Generate Key].
- **5** Click [Network Communication].
- **6** Configure the key and certificate settings.

RSA Key Usage and Additional Procedure

Settings/Registration			E-Mail	to System Manager
nestart Device	Settings/Registration : Management Setti	ngs : Denice Management = Kay and Car	tiřisela Settings = Oera	anata Key =
Apply setting changes	Generate Network Communication Key Generate Network Comm	unication Key	Last Undated	3821 01:03 1:2657
denares	Selected Pretwork Comm	anication ney		cancel
Raper Settings			OK	Cancel
Timeo@nergy Settings	Key Name :			
Network Settings	Signature Algorithm :	SHA256 Y		
-	Key Algorithm :	RSA 2041-be M		
External interface		⊖ ECDSA P256 V		
Volume Settings	Certificate Settings			
Sjurtment/Waintmance	Valid ity Start Date (YYYV/MM/DC) :	7 7		
Azjunt Image Quality	Validity End Data (YYV/MM/DD) :	/ /		
Maintenance	Country/Region :	(8) Select Country/Region Name		
nction Settings		Enter Internet Country Code		
Common Settings				
Asister	State :			
Send	aty:			
	Organization :			
Receive	Organization Unit :			

🔁 [Key Name]

Enter a name for the key using alphanumeric characters. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature. The available hash algorithms vary depending on the key length. A key length of 1024 bits or more can support SHA384 and SHA512 hash algorithms.

🕒 [Key Algorithm]

Select [RSA] or [ECDSA] as the key generation algorithm. Specify the key length if you select [RSA], or specify the key type if you select [ECDSA]. In both cases, a higher value provides greater security but reduces the communication processing speed.

NOTE:

• If you select [SHA384] or [SHA512] for [Signature Algorithm], you cannot set the key length to [512-bit] when you select [RSA] for [Key Algorithm].

[Ualidity Start Date (YYYY/MM/DD)]/[Validity End Date (YYYY/MM/DD)]

Enter the start date and end data of the validity period for the certificate. You cannot set [Validity End Date (YYYY/MM/DD)] to a date before the date in [Validity Start Date (YYYY/MM/DD)].

[Country/Region]

Click [Select Country/Region Name] and select the country/region from the drop-down list. Alternatively, click [Enter Internet Country Code] and enter a country code, such as "US" for the United States.

[[State]/[City]

Enter the location using alphanumeric characters as necessary.

[Organization]/[Organization Unit]

Enter the organization name using alphanumeric characters as necessary.

🚹 [Common Name]

Enter the common name of the certificate using alphanumeric characters as necessary. "Common Name" is often abbreviated as "CN".

7 Click [OK].

- Generating a key and certificate may take some time.
- Generated keys and certificates are automatically registered to the machine.

For a CSR Certificate

Generate a key and CSR on the machine. Use the CSR data displayed on the screen or output to a file to request the certificate authority to issue a certificate. Then, register the issued certificate for the key. You can configure this setting only from the Remote UI.

■ 1. Generating a Key and CSR

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].
- 4 Click [Generate Key].
- **5** Click [Key and Certificate Signing Request (CSR)].
- **6** Configure the key and certificate settings.

		Te Portal	Logis Users: Adve	inistrator Log Out
Settings/Registration			E-Mail	
Restart Device	tetting (megiztution : Manageme Generate Key and Certificate Signi	rit tettings : thereice Management > Key and thereifs	ato settings > then	ная коу >
Apply Setting Changes		rtificate Signing Request (CSR)	Last Updated : 7	02101/02231658
for bransues.			OK.	Cancel
Paper tettings	Key Name :			
time/brogy satings	Signature Algorithms:	0-6236 M		
Network Settings	Key Algorithm :	8 854 1640-681 ♥ 0 000564 p236 ♥		
Ddernal interface Volume Settings	Certificate Signing Request (CS			
Bartmenty Maintenance Adjust Irnage Quality Maintenance	Country/Region :	Select Country/Region hiame Inpan (P) there internet country code		
action Settings	Sala:			\neg
common Settings	cityi			
ine	Organization :			
ent	criganisation Unit :			
cativa	Common Name :			
tore/Access Files	Ŧ			
brageneent Settings				
Joer Management				
Dexice Management				
License (19th er				

🔁 [Key Name]

Enter a name for the key. Enter a name that will be easy to find in a list.

🜔 [Signature Algorithm]

Select the hash algorithm to use for the signature.

🕒 [Key Algorithm]

Select the key algorithm, and specify the key length if you select [RSA], or specify the key type if you select [ECDSA].

[Country/Region]

Select the country code from the list, or enter it directly.

[State]/[City]

Enter the location.

[Organization]/[Organization Unit]

Enter the organization name.

[[Common Name]

Enter the IP address or FQDN.

- When performing IPPS printing in a Windows environment, make sure to enter the IP address of the machine.
- A DNS server is required to enter the FQDN of the machine. Enter the IP address of the machine if you are not using a DNS server.

7 Click [OK].

- The CSR data appears.
- If you want to save the CSR data to a file, click [Store in File] and specify the save location.

NOTE:

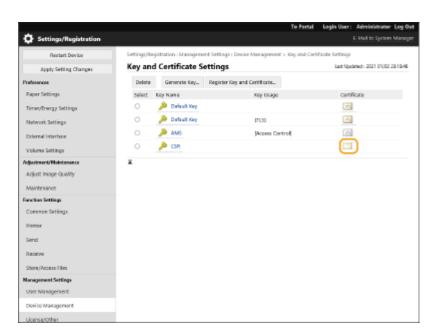
• The key that has generated the CSR appears on the key and certificate list screen, but you cannot use the key by itself. To use this key, you need to register the certificate that is later issued based on the CSR.

Request the certificate authority to issue a certificate based on the CSR data.

■ 2. Registering the Issued Certificate to the Key

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** In the [Certificate] list, click 🛄 for the certificate that you want to register.

RSA Key Usage and Additional Procedure



5 Click [Register Certificate...].

6 Register the certificate.

• Click [Browse...] > specify the file (certificate) to register > click [Register].

Step 3: Resetting the Key and Certificate (for SIP)

Set the generated key and certificate as the key and certificate to use in the TLS encrypted communication of SIP.

Using the Control Panel(P. 71)Using the Remote UI(P. 72)

Using the Control Panel



- 2 Press <Preferences> ► <Network> ► <TCP/IP Settings> ► <SIP Settings> ► <TLS Settings>.
- **3** Configure the various settings in <RX Settings> and <TX Settings> > press <Key and Certificate>.

Example screen:

+ IX3ethigs			
Require Client Sufferdication	0h	CB.	
 Til Settings 			
 Verify Senser Contification 	Dn	08	
+ nettycn			
Byand retilione , rikeyi			-

<rx settings=""></rx>	
<require client<br="">Authentication></require>	Select <on> or <off>. If you select <on>, the machine requests client authentication when the machine receives an IP fax.</on></off></on>
<tx settings=""></tx>	
<verify certificate="" server=""></verify>	Select <on> or <off>. If you select <on>, the machine checks whether the TLS server certificate is valid when the machine receives an IP fax.</on></off></on>
<verify cn=""></verify>	Select <on> or <off>. If you select <on>, the machine checks the CN (Common Name) when the machine receives an IP fax.</on></off></on>

4 Select the key and certificate to use for the TLS encrypted communication of SIP press <Set as Default Key> < OK>.

Example screen:

Rey Name Profest Hay	Taha.	Gef.
ANS	ited	
€ lag1	ibel	22
P Device Signature Rep	iset	100 I I
ir a jetikak ,		
	(DK .

- You cannot select the key and certificate if their status is "Used".
- You can press <Certificate Details> to check detailed information about the certificate.
- You can press <Display Use Location> to check the key/certificate usage.

5 Press <OK>.

6 Press ② (Settings/Registration) ► ③ (Settings/Registration) ► <Apply Setting Changes> ► <Yes>.

The machine restarts, and the settings are applied.

Using the Remote UI

Start the Remote UI.

- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Network Settings] **>** [SIP Settings].

4 Configure the various settings in [TLS Settings] > click [Key and Certificate].

media (1.36) Settings	
T.38 TX Transport :	UDPTL
T.38 Media Type :	image
T.38 RX Port Number :	49152 (1-65535)
RTP RX Port Number :	5004 (1024-65534)
LS Settings	
Key Name	key1 Key and Certificate
RX Settings	
Require Client Authentication	
TX Settings	
Verify Server Certificate	
Add CN to Verification Items	
	Convright CANON INC.

[RX Settings]	
[Require Client Authentication]	If you select this check box, the machine requests client authentication when the machine receives an IP fax.
[TX Settings]	
[Verify Server Certificate]	If you select this check box, the machine checks whether the TLS server certificate is valid when the machine receives an IP fax.
[Add CN to Verification Items]	Select [On] or [Off]. If you select this check box, the machine checks the CN (Common Name) when the machine receives an IP fax.

5 Click [Use] for the key to use in the list.

y and	I Certificate to Use			
legist	ered Key and Certificate			
Key N	lame	Key Usage	Certificate	
۶	Default Key		63	Use
۶	AMS	[Access Control]	(12)	Use
۶	key1	[TLS] [IEEE 802.1X] [IPSec] [SIP]	E3	Use
۶	Device Signature Key	[Device Signature]		Use

6 Click [OK].

7 Click [Apply Setting Changes] to restart the machine.

The machine restarts, and the settings are applied.

Step 4: Deleting a Key/Certificate Generated in the Past (for SIP)

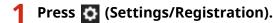
You may not be able to perform operations from the control panel, depending on the model of your machine. In this case, perform operations from the Remote UI.

NOTE

You may need to convey information to the certificate authority when disabling the certificate. See C
 Checking whether You Must Perform the Additional Procedures(P. 5) , and make a note of the required information before deleting the key/certificate.

Using the Control Panel(P. 74)Using the Remote UI(P. 75)

Using the Control Panel



- Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Key and Certificate List> ► <Key and Certificate List for This Device>.
- <Key and Certificate List for This Device> does not appear unless the user signature function is enabled on the machine. In this case, proceed to the next step.

Select the key and certificate > press <Delete> > <Yes>.

Example screen:



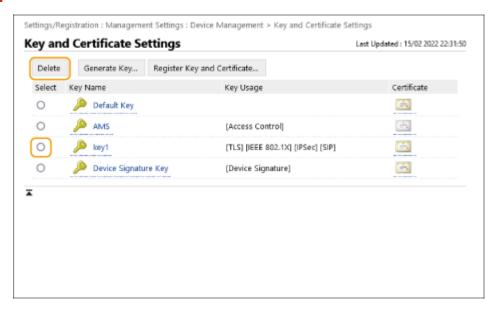
NOTE:

- If \chi appears, the key is corrupt or invalid.
- If 🛅 does not appear, the certificate for the key does not exist.
- If you select a key and certificate and press <Certificate Details>, detailed information about the certificate appears. You can also press <Verify Certificate> on this screen to check whether the certificate is valid.

Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- 3 Click [Device Management] > [Key and Certificate Settings].

4 Select the key and certificate > click [Delete] > [OK].



NOTE

- If \chi appears, the key is corrupt or invalid.
- If 🔄 appears, the certificate for the key does not exist.
- Click a key name to display detailed information about the certificate. You can also click [Verify Certificate] on this screen to check whether the certificate is valid.

Step 5: Disabling the Certificate (for SIP)

Disable a certificate generated in the past. The procedure differs according to the type of certificate.

For a Self-Signed Certificate

If a certificate including a key that requires the additional procedures is registered to another IP fax machine as a trusted certificate, delete the registered certificate. After deleting the registered certificate, register the certificate of the regenerated key.

■ For a CSR Certificate

Request the certificate authority that has issued the certificate to revoke the certificate. Refer to [Issuer] in the certificate for the certificate authority to request.

NOTE

- If you are checking certificate revocation using the other IP fax machine, register the updated CRL to the computer or Web browser after the certificate is revoked.
- If you are using a method other than a CRL (for example, OCSP) to check certificate revocation, perform the procedure for that method.

Step 6: Enabling the New Certificate (for SIP)

Enable the certificate.

■ For a Self-Signed Certificate

Register the new certificate to the other IP fax machine as a trusted certificate.

■ For a CSR Certificate

You do not need to perform the additional procedures.

Procedure for Device Signatures

Step 1: Checking the S/MIME Settings (for Device Signatures)(P. 79)

Step 2: Regenerating the Key and Certificate (for Device Signatures)(P. 81)

Step 3: Disabling the Certificate (for Device Signatures)(P. 82)

Step 4: Enabling the New Certificate (for Device Signatures)(P. 83)

Step 1: Checking the S/MIME Settings (for Device Signatures)

Check whether you need to perform the additional procedures for S/MIME and the device signatures.

Follow the procedure below to check the S/MIME settings.

Using the Control Panel(P. 79)Using the Remote UI(P. 79)

■ Using the Control Panel



Press <Function Settings> > <Send> > <E-Mail/I-Fax Settings> > <S/MIME Settings>.

3 Check <Encryption Settings> and <Add Digital Signatures>.

Example screen:

 Encryption Settings 	Always Encopt	Only liverage If Certificate	Die Het Georget
 Add Digital Signatures 		On	or
 Encryption Higorithm 		Verily Synature u	pon Heceipt
	w.	Dn	or
 Signature Algorithm 		Frint Signature up	un Receipt
	-	0n	OF 1

- If <Encryption Settings> is set to <Do Not Encrypt> and <Add Digital Signatures> is set to <Off>, perform the subsequent procedures for the device signatures only.
- If other settings are specified, perform the subsequent procedures for both S/MIME and the device signatures.

Using the Remote UI

Start the Remote UI.

2 Click [Settings/Registration] on the portal page.

Click [Send] > [S/MIME Settings].

4 Check [Encryption Settings] and [Add Digital Signatures].

	OK	Cancel
		Cancel
 Always Encrypt Only Encrypt If Certificate Do Not Encrypt 		
J.		
3DES Y		
SHA1 Y		
	Only Encrypt If Certificate Do Not Encrypt	Only Encrypt If Certificate Do Not Encrypt 3DES

- If [Do Not Encrypt] is selected for [Encryption Settings] and [Add Digital Signatures] is deselected, perform the subsequent procedures for the device signatures only.
- If other settings are specified, perform the subsequent procedures for both S/MIME and the device signatures.

Step 2: Regenerating the Key and Certificate (for Device Signatures)

Using the Control Panel(P. 81)Using the Remote UI(P. 81)

■ Using the Control Panel

- 1 Press 🔯 (Settings/Registration).
- 2 Press <Management Settings> ► <Device Management> ► <Certificate Settings> ► <Generate Key>.
- Press <Generate/Update Device Signature Key> < Yes> < OK>.

■ Using the Remote UI

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] **>** [Key and Certificate Settings].
- **4** Click [Generate Key] ▶ [Device Signature].
- **5** Click [Generate/Update] ▶ [OK].

Step 3: Disabling the Certificate (for Device Signatures)

Disable a certificate generated in the past.

If a Certificate for Device Signatures Is Registered to Acrobat

If a certificate for device signatures is registered in Acrobat, delete the registered certificate.

■ If an S/MIME Certificate Exported from this Machine Has Been Imported to Another Machine

If you have exported the public key certificate (S/MIME certificate) used for encrypting e-mail/I-faxes via S/MIME from this machine and imported the certificate to another machine, follow the procedure below to delete the certificate from the machine where the certificate has been imported.

1 Start the Remote UI.

2 Click [Settings/Registration] on the portal page.

3 Click [Device Management] > [S/MIME Certificate Settings].

4 Select the corresponding certificate > click [Delete] > [OK].

Step 4: Enabling the New Certificate (for Device Signatures)

Enable the certificate.

If a Certificate for Device Signatures Is Registered to Acrobat

If a certificate for device signatures is registered in Acrobat, export the regenerated certificate for device signatures and register the new certificate to Acrobat.

Exporting the Certificate from the Machine(P. 83)

■ If an S/MIME Certificate Exported from this Machine Has Been Imported to Another Machine

If you have exported the public key certificate (S/MIME certificate) used for encrypting e-mail/I-faxes via S/MIME from this machine and imported the certificate to another machine, export the regenerated certificate and register it to the other machine.

Exporting the Certificate from the Machine(P. 83) Registering the Certificate to the Other Machine(P. 83)

Exporting the Certificate from the Machine

Perform the following procedure to export the certificate.

- Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.
- **3** Click [Device Management] > [Export Device Signature].
- **4** Click [Start Exporting] **>** save the file to a location of your choice.

Registering the Certificate to the Other Machine

Perform the following procedure to register the certificate to the other machine.

- **1** Start the Remote UI.
- **2** Click [Settings/Registration] on the portal page.

- **3** Click [Device Management] > [S/MIME Certificate Settings].
- **4** Click [Register S/MIME Certificate].

5 Register the S/MIME certificate.

• Click [Browse...] > specify the file (S/MIME certificate) to register > click [Register].

Additional Procedures for Bluetooth Settings

Additional Procedures for Bluetooth Settings	. 86
Procedure for Bluetooth	. 87
Step 1: Deleting the Device Registered in Canon PRINT Business (for Bluetooth)	. 88
Step 2: Registering the Device to Canon PRINT Business Again (for Bluetooth)	. 89

Additional Procedures for Bluetooth Settings

The key for Bluetooth is automatically updated after updating the firmware of the machine. If you are using the Canon PRINT Business app for mobile devices, you must register the device again.

OProcedure for Bluetooth(P. 87)

Procedure for Bluetooth

Step 1: Deleting the Device Registered in Canon PRINT Business (for Bluetooth)(P. 88)
 Step 2: Registering the Device to Canon PRINT Business Again (for Bluetooth)(P. 89)

Step 1: Deleting the Device Registered in Canon PRINT Business (for Bluetooth)

If Bluetooth is set to <On>, follow the procedure below.

Operation for iOS(P. 88)Operation for Android(P. 88)

Operation for iOS

Tap [**a**] on the top left of the home screen of Canon PRINT Business. The [Select Printer] screen appears.

2 Delete a device from the list by tapping [🔵] 🕨 [Delete].

Operation for Android

1 Tap [] on the top left of the home screen of Canon PRINT Business. The [Select Printer] screen appears.

Press and hold the device name > tap [Delete] in the displayed dialog box.

Step 2: Registering the Device to Canon PRINT Business **Again (for Bluetooth)**

If Bluetooth is set to <On>, follow the procedure below.

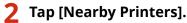
Operation for iOS(P. 89) Operation for Android(P. 89)

Operation for iOS



1 Tap [📑] on the top left of the home screen of Canon PRINT Business.

The [Select Printer] screen appears.



The detected devices appear.

If devices are not detected

Get closer to the machine, and tap [Search]. Bluetooth can detect devices at a distance of up to 2 meters or 80 inches.



Operation for Android

1 Tap [📑] on the top left of the home screen of Canon PRINT Business.

The [Select Printer] screen appears.

Tap [Nearby Printers].

The detected devices appear.

If devices are not detected

Get closer to the machine, and tap [Search]. Bluetooth can detect devices at a distance of up to 2 meters or 80 inches.

Select the device.

Check the device information in the displayed dialog box > tap [Add].

If the Wi-Fi network settings screen appears, follow the instructions on the screen.

Additional Procedures for Access Management System Settings

Additional Procedures for Access Management System Settings	91
Procedure for Access Management System	. 92

Additional Procedures for Access Management System Settings

The key for the Access Management System is automatically updated after updating the firmware of the machine.

Restriction information is automatically retrieved again approximately 30 minutes after the key is automatically updated. Printing can then be performed normally with the Access Management System function.

If you want to print with the Access Management System function of the printer driver immediately after the firmware is updated, it is necessary to manually retrieve the restriction information of the Access Management System again.

Procedure for Access Management System(P. 92)

An error occurs if you try to print without retrieving the restriction information again.

Procedure for Access Management System

If you want to print with the Access Management System function of the printer driver immediately after the firmware is updated, you must manually retrieve the restriction information of the Access Management System.

Follow the procedure below to do so.

The procedure below is not required approximately 30 minutes after the firmware is updated because the restriction information will have been automatically retrieved by that time.

1 Log on to the computer.

2 Display the properties of the printer to use with the printer driver that has the Access Management System function enabled.

For Windows Vista

- Click [Start] > [Control Panel] > [Hardware and Sound] > select [Printers].
- Right-click the printer icon > select [Properties].

For Windows Server 2008

- Click [Start] > [Control Panel] > [Hardware and Sound] > select [Printers].
- Right-click the printer icon > select [Properties].

For Windows Server 2008 R2

- Click [Start] > [Control Panel] > [Hardware] > select [Devices and Printers].
- Right-click the printer icon > select [Printer properties].

For Windows 7

- Click [Start] > [Control Panel] > [Hardware and Sound] > select [Devices and Printers].
- Right-click the printer icon > select [Printer properties].

For Windows 8.1/Windows Server 2012

- Navigate to the desktop and display the charms on the right of the screen.
- Click [Settings] > [Control Panel] > select [View devices and printers].
- Right-click the printer icon > select [Printer properties].

For Windows 10/Windows Server 2016

- Right-click [Start] > select [Control Panel] > [View devices and printers].
- Right-click the printer icon > select [Printer properties].

3 Click the [AMS] tab.

4 Click [Get Restriction Information].

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions: 1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.