RICOH
imagine. change.

User Guide Security Reference
For RICOH IM
C2000/C2000LT/C2500/C2500LT/C3000/C3000LT/C35 00/C3500LT/C4500/C4500LT/C5500/C5500LT/C6000/C 6000LT Enhanced Security Firmware series

For information not found in this manual, see the online manuals available on our web site (https://www.ricoh.com/) or via the control panel.
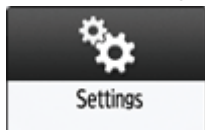
How to Read the Manuals

The [Settings] screen has two different display formats: The Standard type and the Classic type.

You can switch between the two formats on some machines, while other machines support only the Standard type display.

Before reading the manual, check whether your display is the Standard type or the Classic type by pressing [Settings] (

) on the home screen of your machine, and then follow the instructions for your display.

Display format

Standard	Classic

Encryption and Authentication by IPsec

IPsec consists of 2 main functions: the encryption function, which ensures data confidentiality, and the authentication function, which verifies the sender of the data and the data's integrity. This machine's IPsec function supports 2 security protocols: the ESP protocol, which enables both of the IPsec functions at the same time, and the AH protocol, which enables only the authentication function.

ESP protocol

The ESP protocol provides secure transmission through both encryption and authentication. This protocol does not provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH protocol

The AH protocol provides secure transmission through authentication of packets only, including headers.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

AH protocol + ESP protocol

When combined, the ESP and AH protocols provide secure transmission through both encryption and authentication. These protocols provide header authentication.

- For successful encryption, both the sender and receiver must specify the same encryption algorithm and encryption key. If you use the encryption key auto exchange method, the encryption algorithm and encryption key are specified automatically.

- For successful authentication, the sender and receiver must specify the same authentication algorithm and authentication key. If you use the encryption key auto exchange method, the authentication algorithm and authentication key are specified automatically.

- Some operating systems use the term "Compliance" in place of "Authentication".

Copyright © 2020, 2021

Encryption Key Auto Exchange Settings

For key configuration, this machine supports automatic key exchange to specify agreements such as the IPsec algorithm and key for both sender and receiver. Such agreements form what is known as an SA (Security Association). IPsec communication is possible only if the receiver's and sender's SA settings are identical.

If you use the auto exchange method to specify the encryption key, the SA settings are auto configured on both parties' machines. However, before setting the IPsec SA, the ISAKMP SA (Phase 1) settings are auto configured. After this, the IPsec SA (Phase 2) settings, which allow actual IPsec transmission, are auto configured.

Also, for further security, the SA can be periodically auto updated by applying a validity period (time limit) for its settings. This machine only supports IKEv1 for encryption key auto exchange.

Note that it is possible to configure multiple SAs.

Settings 1-4 and default setting

Using the auto exchange method, you can configure four separate sets of SA details (such as different shared keys and IPsec algorithms). In the default settings of these sets, you can include settings that the fields of sets 1 to 4 cannot contain.

When IPsec is enabled, set 1 has the highest priority and set 4 has the lowest. You can use this priority system to target IP addresses more securely. For example, set the broadest IP range at the lowest priority (4), and then set specific IP addresses at a higher priority level (3 and higher). This way, when IPsec transmission is enabled for a specific IP address, the higher level settings will be applied.

Copyright © 2020, 2021

IPsec Settings

IPsec settings for this machine can be made on Web Image Monitor. The following table explains individual setting items.

IPsec settings items

Setting	Description	Setting value
IPsec	Specify whether to enable or disable IPsec.	• Active • Inactive
Exclude HTTPS Communication	Specify whether to enable IPsec for HTTPS transmission.	• Active • Inactive Specify "Active" if you do not want to use IPsec for HTTPS transmission.

The IPsec setting can also be configured from the control panel.

Encryption key auto exchange security level

When you select a security level, certain security settings are automatically configured. The following table explains security level features.

Security level	Security level features
Authentication Only	Select this level if you want to authenticate the transmission partner and prevent unauthorized data tampering, but not perform data packet encryption. Since the data is sent cleartext, data packets are vulnerable to eavesdropping attacks. Do not select this if you are exchanging sensitive information.
Authentication and Low Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping

	attacks. This level provides less security than "Authentication and High Level Encryption".
Authentication and High Level Encryption	Select this level if you want to encrypt the data packets as well as authenticate the transmission partner and prevent unauthorized packet tampering. Packet encryption helps prevent eavesdropping attacks. This level provides higher security than "Authentication and Low Level Encryption".

The following table lists the settings that are automatically configured according to the security level.

Setting	Authentication Only	Authentication and Low Level Encryption	Authentication and High Level Encryption
Security Policy	Apply	Apply	Apply
Encapsulation Mode	Transport	Transport	Transport
IPsec Requirement Level	Use When Possible	Use When Possible	Always Require
Authentication Method	PSK	PSK	PSK
Phase 1Hash Algorithm	MD5	SHA1	SHA256
Phase 1Encryption Algorithm	DES	3DES	AES-128-CBC
Phase 1Diffie-Hellman Group	2	2	2
Phase 2Security Protocol	AH	ESP	ESP
Phase 2Authentication Algorithm	HMAC-SHA1-96/HMAC-SHA256-128/HMAC-SHA384-192/HMAC-SHA512-256	HMAC-SHA1-96/HMAC-SHA256-128/HMAC-SHA384-192/HMAC-SHA512-256	HMAC-SHA256-128/HMAC-SHA384-192/HMAC-SHA512-256
Phase 2Encryption Algorithm Permissions	Cleartext (NULL encryption)	3DES/AES-128/AES-192/AES-256	AES-128/AES-192/AES-256

Phase 2PFS	Inactive	Inactive	2

Encryption key auto exchange settings items

When you specify a security level, the corresponding security settings are automatically configured, but other settings, such as address type, local address, and remote address must still be configured manually.

After you specify a security level, you can still make changes to the auto configured settings. When you change an auto configured setting, the security level switches automatically to "User Setting".

Setting	Description	Setting value
Address Type	Specify the address type for which IPsec transmission is used.	- Inactive - IPv4 - IPv6 - IPv4/IPv6 (Default Settings only)
Local Address	Specify the machine's address. If you are using multiple addresses in IPv6, you can also specify an address range.	The machine's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Remote Address	Specify the address of the IPsec transmission partner. You can also specify an address range.	The IPsec transmission partner's IPv4 or IPv6 address. If you are not setting an address range, enter 32 after an IPv4 address, or enter 128 after an IPv6 address.
Security Policy	Specify how IPsec is handled.	- Apply - Bypass - Discard
Encapsulation Mode	Specify the encapsulation mode. (auto setting)	- Transport - Tunnel If you specify "Tunnel", you must then specify the "Tunnel End Point", which are the beginning and ending IP

		addresses. Set the same address for the beginning point as you set in "Local Address".
IPsec Requirement Level	Specify whether to only transmit using IPsec or to allow cleartext transmission when IPsec cannot be established. (auto setting)	• Use When Possible • Always Require
Authentication Method	Specify the method for authenticating transmission partners. (auto setting)	• PSK • Certificate If you specify "PSK", you must then set the PSK text (using ASCII characters). If you are using "PSK", specify a PSK password using up to 32 ASCII characters. If you specify "Certificate", the certificate for IPsec must be installed and specified before it can be used.
PSK Text	Specify the pre-shared key for PSK authentication.	Enter the pre-shared key required for PSK authentication.
Phase 1 Hash Algorithm	Specify the Hash algorithm to be used in phase 1. (auto setting)	• MD5 • SHA1 • SHA256 • SHA384 • SHA512
Phase 1 Encryption Algorithm	Specify the encryption algorithm to be used in phase 1. (auto setting)	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
Phase 1 Diffie-Hellman Group	Select the Diffie-Hellman group number used for IKE encryption key generation. (auto setting)	• 1 • 2 • 14

Phase 1 Validity Period	Specify the time period for which the SA settings in phase 1 are valid.	Set in seconds from 300 sec. (5 min.) to 172800 sec. (48 hrs.).
Phase 2 Security Protocol	Specify the security protocol to be used in Phase 2. To apply both encryption and authentication to sent data, specify "ESP" or "ESP+AH". To apply authentication data only, specify "AH". (auto setting)	• ESP • AH • ESP+AH
Phase 2 Authentication Algorithm	Specify the authentication algorithm to be used in phase 2. (auto setting)	• HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256
Phase 2 Encryption Algorithm Permissions	Specify the encryption algorithm to be used in phase 2. (auto setting)	• Cleartext (NULL encryption) • DES • 3DES • AES-128 • AES-192 • AES-256
Phase 2 PFS	Specify whether to activate PFS. Then, if PFS is activated, select the Diffie-Hellman group. (auto setting)	• Inactive • 1 • 2 • 14
Phase 2 Validity Period	Specify the time period for which the SA settings in phase 2 are valid.	Specify a period (in seconds) from 300 (5min.) to 172800 (48 hrs.).

Specifying Encryption Key Auto Exchange Settings

To change the transmission partner authentication method for encryption key auto exchange settings to "Certificate", you must first install and assign a certificate. For details about creating and installing a device certificate, see User Guide of your device. For the method of assigning installed certificates to IPsec, see Selecting the certificate for IPsec.

1 **Log in as the network administrator from Web Image Monitor.**

For details on how to log in, see User Guide of your device.

2 **Point to [Device Management], and then click [Configuration].**

3 **Click [IPsec] under "Security".**

4 **Click [Edit] under "Encryption Key Auto Exchange Settings".**

5 **Make encryption key auto exchange settings in [Settings 1].**

If you want to make multiple settings, select the settings number and add settings.

6 **Click [OK].**

7 **Select [Active] for "IPsec" in "IPsec".**

8 **Set "Exclude HTTPS Communication" to [Active] if you do not want to use IPsec for HTTPS transmission.**

`9` **Click [OK].**

`10` **"Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].**

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

`11` **Log out.**

Copyright © 2020, 2021

Selecting the certificate for IPsec

Using Web Image Monitor, select the certificate to be used for IPsec. You must install the certificate before it can be used. For details about creating and installing a device certificate, see User Guide of your device.

1 Log in as the network administrator from Web Image Monitor.

For details on how to log in, see User Guide of your device.

2 Point to [Device Management], and then click [Configuration].

3 Click [Device Certificate] under "Security".

4 Select the certificate to be used for IPsec from the drop-down list box in "IPsec" under "Certification".

5 Click [OK].

The certificate for IPsec is specified.

6 "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

7 Log out.

Copyright © 2020, 2021

Specifying the computer's IPsec settings

Configure the computer's IPsec SA settings, so that they exactly match the machine's security level on the machine. Setting methods differ according to the computer's operating system. The example procedure shown here uses Windows 10 when the "Authentication and Low Level Encryption" security level is selected.

1 Right-click the [Start] button, click [Control Panel], [System and Security], and then [Administrative Tools].

Under Windows 7, click the [Start] button, and click [Control Panel], [System and Security], and then [Administrative Tools].

2 Double-click [Local Security Policy].

If the "User Account Control" dialog box appears, click [Yes].

3 Right-click [IP Security Policies on Local Computer].

Under Windows 7, double-click [IP Security Policies on Local Computer].

4 Click [Create IP Security Policy].

Under Windows 7, click [Create IP Security Policy] in the "Action" menu.

The IP Security Policy Wizard appears.

5 Click [Next].

6 Enter a security policy name in "Name", and then click [Next].

7 Clear the "Activate the default response rule" check box, and then click [Next].

8 Select "Edit properties", and then click [Finish].

9 **In the "General" tab, click [Settings].**

10 **In "Authenticate and generate a new key after every", enter the same validity period (in minutes) that is specified on the machine in "Encryption Key Auto Exchange SettingsPhase 1", and then click [Methods].**

11 **Check that the hash algorithm ("Integrity"), encryption algorithm ("Encryption") and "Diffie-Hellman Group" settings in "Security method preference order" all match those specified on the machine in "Encryption Key Auto Exchange SettingsPhase 1".**

If the settings are not displayed, click [Add].

12 **Click [OK] twice.**

13 **Click [Add] in the "Rules" tab.**

The Security Rule Wizard appears.

14 **Click [Next].**

15 **Select "This rule does not specify a tunnel", and then click [Next].**

16 **Select the type of network for IPsec, and then click [Next].**

17 **Click [Add] in the IP Filter List.**

18 **In [Name], enter an IP Filter name, and then click [Add].**

The IP Filter Wizard appears.

19 **Click [Next].**

20 **If required, enter a description of the IP filter, and then click [Next].**

21 **Select "My IP Address" in "Source address", and then click [Next].**

22 **Select "A specific IP Address or Subnet" in "Destination address", enter the machine's IP address, and then click [Next].**

23 **Select the protocol type for IPsec, and then click [Next].**

If you select "TCP" or "UDP", specify both source and destination ports, and then click [Next].

24 **Click [Finish].**

25 **Click [OK].**

26 **Select the IP filter that was just created, and then click [Next].**

27 **Click [Add].**

Filter action wizard appears.

28 **Click [Next].**

29 **In [Name], enter an IP Filter action name, and then click [Next].**

30 **Select "Negotiate security", and then click [Next].**

31 **Select "Allow unsecured communication if a secure connection cannot be established.", and then click [Next].**

32 **Select "Custom" and click [Settings].**

33 **In "Integrity algorithm", select the authentication algorithm that was specified on the machine in "Encryption Key Auto Exchange SettingsPhase 2".**

34 **In "Encryption algorithm", select the encryption algorithm that specified on the machine in "Encryption Key Auto Exchange SettingsPhase 2".**

35 **In "Session key settings", select "Generate a new key every", and enter the validity period (in seconds) that was specified on the machine in "Encryption Key Auto Exchange SettingsPhase 2".**

36 **Click [OK].**

37 **Click [Next].**

38 **Click [Finish].**

39 **Select the filter action that was just created, and then click [Next].**

If you set "Encryption Key Auto Exchange Settings" to "Authentication and High Level Encryption", select the IP filter action that was just created, click [Edit], and then check "Use session key perfect forward secrecy (PFS)" on the filter action properties dialog box. If using PFS in Windows, the PFS group number used in phase 2 is automatically negotiated in phase 1 from the Diffie-Hellman group number (set in Step 11). Consequently, if you change the security level specified automatic settings on the machine and "User Setting" appears, you must set the same the group number for "Phase 1Diffie-Hellman Group" and "Phase 2PFS" on the machine to establish IPsec transmission.

40 **Select the authentication method, and then click [Next].**

If you select "Certificate" for authentication method in "Encryption Key Auto Exchange Settings" on the machine, specify the device certificate. If you select "PSK", enter the same PSK text specified on the machine with the pre-shared key.

41 Click [Finish].

If you are using IPv6, you must repeat this procedure from Step 13 and add ICMPv6 as an exception.

When you reach step 23, select [58] as the protocol number for the "Other" target protocol type, and then set [Negotiate security] to [Permit].

42 Click [OK].

The new IP security policy (IPsec settings) is specified.

43 Select the security policy that was just created, right-click, and then click [Assign].

The computer's IPsec settings are enabled. If you click [Un-assign], the computer's IPsec settings are disabled.

Copyright © 2020, 2021

Encryption Key Auto Exchange Settings Configuration Flow
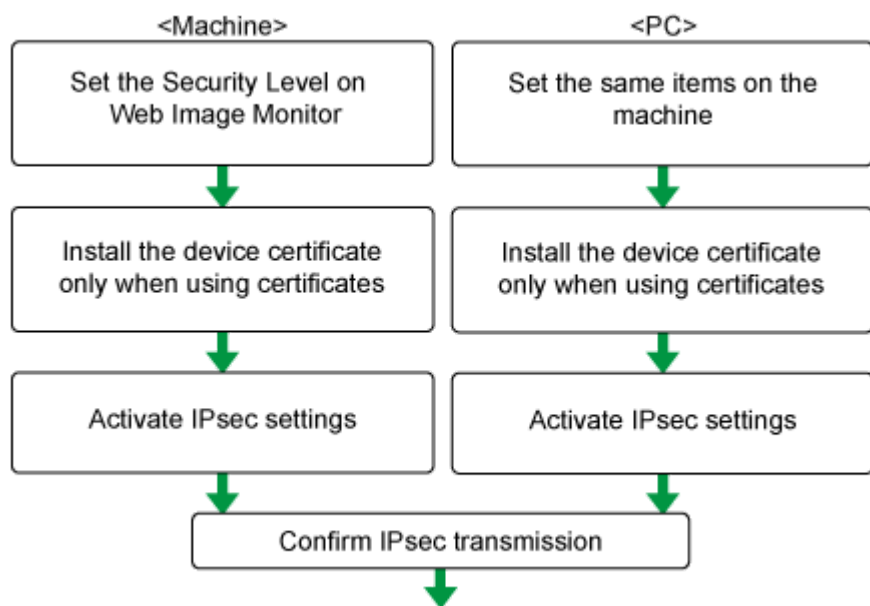
![Important]

- To use a certificate to authenticate the transmission partner in encryption key auto exchange settings, a device certificate must be installed.

- After configuring IPsec, you can use "Ping" command to check if the connection is established correctly. However, you cannot use "Ping" command when ICMP is excluded from IPsec transmission on the computer side. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.

Related topics

Specifying Encryption Key Auto Exchange Settings

Selecting the certificate for IPsec

Specifying the computer's IPsec settings

Copyright © 2020, 2021

ipsec

To display IPsec related settings information, use the "ipsec" command.

Display current settings

```
msh> ipsec
```

Displays the following IPsec settings information:

- IPsec settings values

- Encryption key auto exchange settings, IKE setting 1-4 values

- Encryption key auto exchange settings, IKE default setting values

Display current settings portions

```
msh> ipsec -p
```

- Displays IPsec settings information in portions.

Copyright © 2020, 2021

ipsec exclude

To display or specify protocols excluded by IPsec, use the "ipsec exclude" command.

Display current settings

```
msh> ipsec exclude
```

- Displays the protocols currently excluded from IPsec transmission.

Specify protocols to exclude

```
msh> ipsec exclude {https|dns|dhcp|wins|all} {on|off}
```

- Specify the protocol, and then enter [on] to exclude it, or [off] to include it for IPsec transmission. Entering [all] specifies all protocols collectively.

ipsec ike

To display or specify the encryption key auto exchange settings, use the "ipsec ike" command.

Display current settings

```
msh> ipsec ike {1|2|3|4|default}
```

- To display the settings 1-4, specify the number [1-4].

- To display the default setting, specify [default].

- Not specifying any value displays all of the settings.

Disable settings

```
msh> ipsec ike {1|2|3|4|default} disable
```

- To disable the settings 1-4, specify the number [1-4].

- To disable the default settings, specify [default].

Specify the user-specific local address / remote address.

```
msh> ipsec ike {1|2|3|4} {ipv4|ipv6} "local address" "remote address"
```

- Enter the separate setting number [1-4], and the address type to specify local and remote address.

- To set the local or remote address values, specify masklen by entering [/] and an integer 0-32 when settings an IPv4 address. When setting an IPv6 address, specify masklen by entering [/] and an integer 0-128.

- Not specifying an address value displays the current setting.

Specify the address type in default setting

```
msh> ipsec ike default {ipv4|ipv6|any}
```

- Specify the address type for the default setting.

- To specify both IPv4 and IPv6, enter [any].

Security policy setting

```
msh> ipsec ike {1|2|3|4|default} proc {apply|bypass|discard}
```

- Enter the separate setting number [1-4] or [default] and specify the security policy for the address specified in the selected setting.

- To apply IPsec to the relevant packets, specify [apply]. To not apply IPsec, specify [bypass].

- If you specify [discard], any packets to which IPsec can be applied are discarded.

- Not specifying a security policy displays the current setting.

Security protocol setting

```
msh> ipsec ike {1|2|3|4|default} proto {ah|esp|dual}
```

- Enter the separate setting number [1-4] or [default] and specify the security protocol.

- To specify AH, enter [ah]. To specify ESP, enter [esp]. To specify AH and ESP, enter [dual].

- Not specifying a protocol displays the current setting.

IPsec requirement level setting

```
msh> ipsec ike {1|2|3|4|default} level {require|use}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec requirement level.

- If you specify [require], data will not be transmitted when IPsec cannot be used. If you specify [use], data will be sent normally when IPsec cannot be used. When IPsec can be used, IPsec transmission is performed.

- Not specifying a requirement level displays the current setting.

Encapsulation mode setting

```
msh> ipsec ike {1|2|3|4|default} mode {transport|tunnel}
```

- Enter the separate setting number [1-4] or [default] and specify the encapsulation mode.

- To specify transport mode, enter [transport]. To specify tunnel mode, enter [tunnel].

- If you have set the address type in the default setting to [any], you cannot use [tunnel] in encapsulation mode.

- Not specifying an encapsulation mode displays the current setting.

Tunnel end point setting

```
msh> ipsec ike {1|2|3|4|default} tunneladdr "beginning IP address" "ending IP address"
```

- Enter the separate setting number [1-4] or [default] and specify the tunnel end point beginning and ending IP address.

- Not specifying either the beginning or ending address displays the current setting.

IKE partner authentication method setting

```
msh> ipsec ike {1|2|3|4|default} auth {psk|rsasig}
```

- Enter the separate setting number [1-4] or [default] and specify the authentication method.

- Specify [psk] to use a shared key as the authentication method. Specify [rsasig] to use a certificate at the authentication method.

- You must also specify the PSK character string when you select [psk].

- Note that if you select "Certificate", the certificate for IPsec must be installed and specified before it can be used. To install and specify the certificate use Web Image Monitor.

PSK character string setting

```
msh> ipsec ike {1|2|3|4|default} psk "PSK character string"
```

- If you select PSK as the authentication method, enter the separate setting number [1-4] or [default] and specify the PSK character string.

- Specify the character string in ASCII characters. There can be no abbreviations.

ISAKMP SA (phase 1) hash algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 hash {md5|sha1|sha256|sha384|sha512}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) hash algorithm.
- Not specifying the hash algorithm displays the current setting.

ISAKMP SA (phase 1) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph1 encrypt {des|3des|aes128|aes192|aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) encryption algorithm.
- Not specifying an encryption algorithm displays the current setting.

ISAKMP SA (phase 1) Diffie-Hellman group setting

```
msh> ipsec ike {1|2|3|4|default} ph1 dhgroup {1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) Diffie-Hellman group number.
- Specify the group number to be used.
- Not specifying a group number displays the current setting.

ISAKMP SA (phase 1) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph1 lifetime "validity period"
```

- Enter the separate setting number [1-4] or [default] and specify the ISAKMP SA (phase 1) validity period.
- Enter the validity period (in seconds) from 300 to 172800.
- Not specifying a validity period displays the current setting.

IPsec SA (phase 2) authentication algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 auth {hmac-md5|hmac-sha1|hmac-sha256|hmac-
sha384|hmac-sha512}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) authentication algorithm.

- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.

- Not specifying an authentication algorithm displays the current setting.

IPsec SA (phase 2) encryption algorithm setting

```
msh> ipsec ike {1|2|3|4|default} ph2 encrypt {null|des|3des|aes128|aes192|aes256}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) encryption algorithm.

- Separate multiple encryption algorithm entries with a comma (,). The current setting values are displayed in order of highest priority.

- Not specifying an encryption algorithm displays the current setting.

IPsec SA (phase 2) PFS setting

```
msh> ipsec ike {1|2|3|4|default} ph2 pfs {none|1|2|14}
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) Diffie-Hellman group number.

- Specify the group number to be used.

- Not specifying a group number displays the current setting.

IPsec SA (phase 2) validity period setting

```
msh> ipsec ike {1|2|3|4|default} ph2 lifetime "validity period"
```

- Enter the separate setting number [1-4] or [default] and specify the IPsec SA (phase 2) validity period.

- Enter the validity period (in seconds) from 300 to 172800.

- Not specifying a validity period displays the current setting.

Reset setting values

```
msh> ipsec ike {1|2|3|4|default|all} clear
```

- Enter the separate setting number [1-4] or [default] and reset the specified setting. Specifying [all] resets all of the settings, including default.

telnet Setting Commands

You can use telnet to confirm IPsec settings and make setting changes. This section explains telnet commands for IPsec. For information about the user name and password for logging into telnet, ask the administrator. For details about logging in to telnet and telnet operations, see User Guide of your device.

⭐ Important

- If you are using a certificate as the authentication method in encryption key auto exchange settings (IKE), install the certificate using Web Image Monitor. A certificate cannot be installed using telnet.

Related topics

ipsec

ipsec exclude

ipsec ike

Copyright © 2020, 2021

>Configuring IEEE 802.1X Authentication

Configuring IEEE 802.1X Authentication

IEEE 802.1X is an authentication function that can be used with both wired and wireless networks. Authentication is performed by the authentication server (RADIUS server).

You can select 4 types of EAP authentication method: EAP-TLS, LEAP, EAP-TTLS and PEAP. Note that each EAP authentication method has different configuration settings and authentication procedures.

Types and requirements of certificates are as follows:

EAP type	Required certificates
EAP-TLS	Root certificate, Device certificate (IEEE 802.1X Client Certificate)
LEAP	-
EAP-TTLS	Root certificate
PEAP	Root certificate
PEAP (Phase 2 is for TLS only)	Root certificate, Device certificate (IEEE 802.1X Client Certificate)

Related topics

Installing a Root Certificate

Selecting the Device Certificate

Setting Items of IEEE 802.1X for Ethernet

Setting Items of IEEE 802.1X for Wireless LAN

Copyright © 2020, 2021

Installing a Root Certificate

Install a root certificate (root CA certificate) for verifying the reliability of the authentication server. You need to have at least a certificate issued by the certificate authority who signed the server certificate or a certificate from a higher certificate authority.

Only PEM (Base64-encoded X.509) root certificates can be imported.

1 **Log in as the network administrator from Web Image Monitor.**

For details on how to log in, see User Guide of your device.

2 **Point to [Device Management], and then click [Configuration].**

3 **Click [Root Certificate] under "Security".**

4 **Click [Browse] for "Root Certificate to Import", and then select the CA certificate you obtained.**

5 **Click [Open].**

6 **Click [Import].**

7 **Check that the imported certificate's [Status] shows "Trustworthy".**

If [Root Certificate Check] shows [Active], and the [Status] of the certificate shows [Untrustworthy], communication might not be possible.

8 **Click [OK].**

9 **Log out.**

Copyright © 2020, 2021

Selecting the Device Certificate

Select the certificate you want to use under IEEE 802.1X from among the device certificates created and installed in advance on the machine. For details about creating and installing a device certificate, see User Guide of your device.

1 Log in as the network administrator from Web Image Monitor.

For details on how to log in, see User Guide of your device.

2 Point to [Device Management], and then click [Configuration].

3 Click [Device Certificate] under "Security".

4 Select the certificate to be used for IEEE 802.1X from the drop-down list box in "IEEE 802.1X" under "Certification".

5 Click [OK].

6 "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

7 Log out.

Copyright © 2020, 2021

Setting Items of IEEE 802.1X for Ethernet

1 **Log in as the network administrator from Web Image Monitor.**

For details on how to log in, see User Guide of your device.

2 **Point to [Device Management], and then click [Configuration].**

3 **Click [IEEE 802.1X] under "Security".**

4 **In "User Name", enter the user name set in the RADIUS server.**

5 **Enter the domain name in "Domain Name".**

6 **Select "EAP Type". Configurations differ according to the EAP Type.**

EAP-TLS

- Make the following settings according to the operating system you are using:
    - Select [On] or [Off] in "Authenticate Server Certificate".
    - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
    - Enter the host name of the RADIUS server on "Server ID".
    - Select [On] or [Off] in "Permit Sub-domain".

LEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

EAP-TTLS

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".
  Certain methods might not be available, depending on the RADIUS server you want to use.

- Make the following settings according to the operating system you are using:

    - Select [On] or [Off] in "Authenticate Server Certificate".

    - Select [On] or [Off] in "Trust Intermediate Certificate Authority".

    - Enter the host name of the RADIUS server in "Server ID".

    - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

    If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.

- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.

- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".

    When you select [TLS], you must install "IEEE 802.1X Client Certificate".

- Make the following settings according to the operating system you are using:

    - Select [On] or [Off] in "Authenticate Server Certificate".

    - Select [On] or [Off] in "Trust Intermediate Certificate Authority".

    - Enter the host name of the RADIUS server on "Server ID".

    - Select [On] or [Off] in "Permit Sub-domain".

`7` Click [OK].

`8` "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

`9` Click [Interface Settings] under "Interface".

`10` Select [Active] in "Ethernet Security".

`11` Click [OK].

`12` "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not reappear after you click [OK], wait for a while, and then click the web browser's refresh button.

13 Log out.

![Note]

- If there is a problem with settings, you might not be able to communicate with the machine. In such cases, access the following items on the control panel, and then print the network summary to check the status.

  - Settings screen type: Standard

    [Network/Interface] ▶ [Print List]

  - Settings screen type: Classic

    [Interface Settings] ▶ [Print List]

- If you cannot identify the problem, execute the following item on the control panel, and then repeat the procedure.

  - Settings screen type: Standard

    [Network/Interface] ▶ [IEEE 802.1X Authentication] ▶ [Restore IEEE 802.1X Authentication to Defaults]

  - Settings screen type: Classic

    [Interface Settings] ▶ [Network] ▶ [Restore IEEE 802.1X Authentication to Defaults]

Copyright © 2020, 2021

Setting Items of IEEE 802.1X for Wireless LAN

1 **Log in as the network administrator from Web Image Monitor.**

For details on how to log in, see User Guide of your device.

2 **Point to [Device Management], and then click [Configuration].**

3 **Click [IEEE 802.1X] under "Security".**

4 **In "User Name", enter the user name set in the RADIUS server.**

5 **Enter the domain name in "Domain Name".**

6 **Select "EAP Type". Configurations differ according to the EAP Type.**

EAP-TLS

- Make the following settings according to the operating system you are using:
    - Select [On] or [Off] in "Authenticate Server Certificate".
    - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
    - Enter the host name of the RADIUS server on "Server ID".
    - Select [On] or [Off] in "Permit Sub-domain".

LEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

EAP-TTLS

- Click [Change] in "Password", and then enter the password set in the RADIUS server.
- Click [Change] in "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [CHAP], [MSCHAP], [MSCHAPv2], [PAP], or [MD5] in "Phase 2 Method".
  Certain methods might not be available, depending on the RADIUS server you want to use.

- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server in "Server ID".
  - Select [On] or [Off] in "Permit Sub-domain".

PEAP

- Click [Change] in "Password", and then enter the password set in the RADIUS server.

  If [TLS] is selected for "Phase 2 Method", you do not need to specify a password.
- Click [Change] on "Phase 2 User Name", and then enter the user name set in the RADIUS server.
- Select [MSCHAPv2] or [TLS] in "Phase 2 Method".

  When you select [TLS], you must install "IEEE 802.1X Client Certificate".
- Make the following settings according to the operating system you are using:
  - Select [On] or [Off] in "Authenticate Server Certificate".
  - Select [On] or [Off] in "Trust Intermediate Certificate Authority".
  - Enter the host name of the RADIUS server on "Server ID".
  - Select [On] or [Off] in "Permit Sub-domain".

7 Click [OK].

8 "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

9 Click [Wireless LAN Settings] under "Interface".

10 Select [Wireless LAN] in "LAN Type".

11 Select [Infrastructure Mode] in "Communication Mode".

12 Enter the alphanumeric characters (a-z, A-Z, or 0-9) in [SSID] according to the

access point you want to use.

13 Select [WPA2] in "Security Method".

14 Select [WPA2] in "WPA2 Authentication Method".

15 Click [OK].

16 "Updating..." appears. Wait for about 1 or 2 minutes, and then click [OK].

If the previous screen does not appear again after you click [OK], wait for a while, and then click the web browser's refresh button.

17 Log out.

⬇ Note

- If there is a problem with settings, you might not be able to communicate with the machine. In such cases, access the following items on the control panel, and then print the network summary to check the status.
    - Settings screen type: Standard

      [Network/Interface] ▶ [Print List]
    - Settings screen type: Classic

      [Interface Settings] ▶ [Print List]
- If you cannot identify the problem, execute the following item on the control panel, and then repeat the procedure.
    - Settings screen type: Standard

      [Network/Interface] ▶ [IEEE 802.1X Authentication] ▶ [Restore IEEE 802.1X Authentication to Defaults]
    - Settings screen type: Classic

      [Interface Settings] ▶ [Network] ▶ [Restore IEEE 802.1X Authentication to Defaults]

>How to Read (Settings Screen Type: Standard)

How to Read (Settings Screen Type: Standard)

⭐ Important

- The Manual covers various types of the machines. Descriptions in the Manual may differ from your model.

Understanding headers

- User

  The user administrator has privileges for this operation.

- Mach

  The machine administrator has privileges for this operation.

- N/W

  The network administrator has privileges for this operation.

- File

  The file administrator has privileges for this operation.

- Unset

  The logged in user has privileges for this operation.

  In cases where no settings are selected in [Available Settings] of [Administrator Authentication Management].

- Set

  The logged in user has privileges for this operation.

  Status when settings are selected in [Available Settings] of [Administrator Authentication Management].

- Lv.1

  In cases where the [Menu Protect] setting is set to [Level 1].

- Lv.2

  In cases where the [Menu Protect] setting is set to [Level 2].

Understanding the symbols

R/W: Executing, changing, and reading possible.

R: Reading is possible.

-: Executing, changing, and reading are not possible.

System Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Display/Input]

[Output Tray]

[Machine]

[Date/Time/Timer]

[Sound]

[Network/Interface]

[Send (Email/Folder)]

[Settings for Administrator]

[Machine/Control Panel Information]

[Extended Feature Information]

Copyright © 2020, 2021

[Display/Input]

[Display]

Settings	User	Mach	N/W	File	Unset	Set
[Brightness]	–	R/W	–	–	R/W	–
[Screen Color Setting]	R	R/W	R	R	R/W	R
[Display IP Address]	–	R/W	–	–	–	–
[Function Priority]	–	R/W	–	–	R/W	–
[Select Switchable Languages]	–	R/W	–	–	R/W	–
[Measurement Unit]	R	R/W	R	R	R/W	R
[Application Display Settings by Function]	–	R/W	–	–	R/W	–
[System Bar Settings]	–	R/W	–	–	R/W	–

[Key/Keyboard/Input Assistance]

Settings	User	Mach	N/W	File	Unset	Set
[Function Key Settings]	–	R/W	–	–	R/W	–
[[Back] Key]	–	R/W	–	–	R/W	–
[Word List]	–	R/W	–	–	R/W	–
[Default Keyboard]	–	R/W	–	–	R/W	–
[Switchable Keyboard Settings]	–	R/W	–	–	R/W	–
[Register/Change/Delete User Text]	R	R/W	R	R	R/W	R

[Key Repeat]	R	R/W	R	R	R/W	R

Copyright © 2020, 2021

[Output Tray]

Settings	User	Mach	N/W	File	Unset	Set
[Output Tray: Copier]	R	R/W	R	R	R/W	R
[Output Tray: Document Server]	R	R/W	R	R	R/W	R
[Output Tray: Fax]	R	R/W	R	R	R/W	R
[Specify Tray for Lines]	R	R/W	R	R	R/W	R
[Output Tray: Printer]	R	R/W	R	R	R/W	R

[Machine]

[Print Action/Image Quality Adjustment]

Settings	User	Mach	N/W	File	Unset	Set
[Interleave Print Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[ADF Original Table Elevation]	R	R/W	R	R	R/W	R
[ADF Original Double Feed Detection]	R	R/W	R	R	–	–
[Output Priority When Paper is Fed to Finisher] (IM C6000/C5500/C4500 Series)	R	R/W	R	R	R/W	R
[Allow Logout during Scanning]	R	R/W	R	R	R/W	R

[Power/Energy Saving]

Settings	User	Mach	N/W	File	Unset	Set
[Human Detection Sensor]	R	R/W	R	R	R/W	R
[Energy Saving Recovery for Business Application]	R	R/W	R	R	R/W	R
[Sleep Mode Entry by Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Main Power On by Remote Operation]	R	R/W	R	R	R	R
[Shift to Main Power-Off When Network Disconnected]	R	R/W	R	R	R/W	R
[Control Panel Startup Mode]	–	R/W	–	–	R/W	–

[Recovery by Wireless Connect]	–	R/W	–	–	R/W	–

[Silent]

Settings	User	Mach	N/W	File	Unset	Set
[ADF Operation: Copier / Document Server]	R	R/W	R	R	R/W	R

[External Device]

Settings	User	Mach	N/W	File	Unset	Set
[Register/Change USB Device List]	R	R/W	R	R	R/W	R
[Control Panel SD Card Slot]	–	R/W	–	–	R/W	–
[Control Panel USB Memory Slot]	–	R/W	–	–	R/W	–
[Allow Media Slots Use]	R	R/W	R	R	R	R

[@Remote Service]

Settings	User	Mach	N/W	File	Unset	Set
[Service Test Call]	–	R/W	–	–	R/W	–
[Notify Machine Status]	–	R/W	–	–	R/W	–
[Notify Machine Status to Data Server]	–	R/W	–	–	R/W	–

[Auto Discovery]	–	R/W	–	–	–	–

[Staple]

Settings	User	Mach	N/W	File	Unset	Set
[Erase Margin for Stapleless Stapler]	R	R/W	R	R	R/W	R
[Stapling Method for Stapleless Stapler]	R	R/W	R	R	R/W	R
[Auto Switch Staple/Stapleless Stapler] (When Finisher SR3260 is installed)	R	R/W	R	R	R/W	R

[Fold/Booklet]

Settings	User	Mach	N/W	File	Unset	Set
[Z-fold Position]	R	R/W	R	R	R/W	R
[Half Fold Position]	R	R/W	R	R	R/W	R
[Letter Fold-out Position 1]	R	R/W	R	R	R/W	R
[Letter Fold-out Position 2]	R	R/W	R	R	R/W	R
[Letter Fold-in Position 1]	R	R/W	R	R	R/W	R
[Letter Fold-in Position 2]	R	R/W	R	R	R/W	R

[Others]

Settings	User	Mach	N/W	File	Unset	Set

[Central Management]						
• [Address Book]	R	R/W	R	R	R	R
• [Client Synchronization]^{*1}	R/W	R/W	R	R	R	R
• [Synchronize with Server]^{*2}	R/W	R/W	R	R	R	R
• [Print Volume Use Limitation]^{*3}	R	R/W	R	R	R	R
• [Eco-friendly Counter]^{*3}	R	R/W	R	R	R	R
• [Print Volume Use Limitation If Disconnected]^{*3}	R	R/W	R	R	R	R
[Register/Change/Delete Remote Machine]	–	R/W	–	–	R/W	–
[Support Settings]	–	R/W	–	–	R/W	–
[Compatible ID]	R	R/W	R	R	R/W	R
[Fixed USB Port]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R

*1 This appears if you use the machine as the server.
*2 This appears if you use the machine as a client.
*3 This appears if you use the machine as the server or a client.

[Date/Time/Timer]

[Date/Time]

Settings	User	Mach	N/W	File	Unset	Set
[Daylight Saving Time]	R	R/W	R	R	R/W	R
[Set Date]	R	R/W	R	R	R/W	R
[Set Time]	R	R/W	R	R	R/W	R
[Time Zone]	R	R/W	R	R	R/W	R

[Timer]

Settings	User	Mach	N/W	File	Unset	Set
[Sleep Mode Timer]	R	R/W	R	R	R/W	R
[Auto Logout Timer]	R	R/W	R	R	R/W	R
[Fusing Unit Off Mode (Energy Saving) On/Off]	R	R/W	R	R	R/W	R
[System Auto Reset Timer]	R	R/W	R	R	R/W	R
[Copier/Document Server Auto Reset Timer]	R	R/W	R	R	R/W	R
[Fax Auto Reset Timer]	R	R/W	R	R	R/W	R
[Printer Auto Reset Timer]	R	R/W	R	R	R/W	R
[Scanner Auto Reset Timer]	R	R/W	R	R	R/W	R
[System Status/Job List Display Time]	R	R/W	R	R	R/W	R
[Weekly Timer Detailed Settings]	R	R/W	R	R	R/W	R

[Weekly Timer Easy Settings]	R	R/W	R	R	R/W	R

[Sound]

Settings	User	Mach	N/W	File	Unset	Set
[Volume]	–	R/W	–	–	R/W	–
[Touch/Notification Sound]	–	R/W	–	–	R/W	–
[Invalid Operation Sound]	–	R/W	–	–	R/W	–
[Operation Completed Sound]	–	R/W	–	–	R/W	–
[Copy: Job Done Sound]	–	R/W	–	–	R/W	–
[Fax Printing Ended Sound]	–	R/W	–	–	R/W	–
[Fax Transmission Ended Sound]	–	R/W	–	–	R/W	–
[Fax Reception Ended Sound]	–	R/W	–	–	R/W	–
[Login Sound]	–	R/W	–	–	R/W	–
[Logout Sound]	–	R/W	–	–	R/W	–
[Warm-up Sound]	–	R/W	–	–	R/W	–
[Auto Reset Sound]	–	R/W	–	–	R/W	–
[Caution Sound]	–	R/W	–	–	R/W	–
[Copy: Forgot Original Sound]	–	R/W	–	–	R/W	–
[Scanner: Forgot Original Sound]	–	R/W	–	–	R/W	–
[Fax: Forgot Original Sound]	–	R/W	–	–	R/W	–
[Warning Sound]	–	R/W	–	–	R/W	–
[Blank Page Detected Sound]	–	R/W	–	–	R/W	–

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Adjust Sound Volume]	R	R/W	R	R	R/W	R

Copyright © 2020, 2021

[Network/Interface]

[Machine: LAN Type]

Settings	User	Mach	N/W	File	Unset	Set
[Machine: LAN Type]	R	R	R/W	R	R/W	R

[Wireless LAN]

Settings	User	Mach	N/W	File	Unset	Set
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID Setting]	R	R	R/W	R	R/W	R
[Security Method]	R	R	R/W	R	R/W	R
[Wireless LAN Signal]	R	R	R	R	R	R
[Active/Inactive]	–	–	R/W	–	R/W	–
[Fix SSID]	–	–	R/W	–	R/W	–
[Direct Connection Settings]	–	–	R/W	–	R/W	–
[Ad-hoc Channel]	R	R	R/W	R	R/W	R
[Wireless LAN: Easy Setup/Direct Connection]	–	–	R/W	–	R/W	–
[Restore Factory Defaults for Wireless LAN Settings]	–	–	R/W	–	R/W	–

[IP Address (IPv4)]

Settings	User	Mach	N/W	File	Unset	Set
[IP Address]^{*4}	R	R	R/W	R	R/W	R
[IPv4 Gateway Address]	R	R	R/W	R	R/W	R

*4 When [Auto-Obtain (DHCP)] is set, the data is read-only.

[IP Address (IPv6)]

Settings	User	Mach	N/W	File	Unset	Set
[IP Address]	R	R	R	R	R	R
[IPv6 Gateway Address]	R	R	R	R	R	R
[IPv6 Stateless Address Autoconfiguration]	R	R	R/W	R	R/W	R
[DHCPv6 Configuration]	R	R	R/W	R	R/W	R

[DNS Configuration]

Settings	User	Mach	N/W	File	Unset	Set
[DNS Configuration]^{*5}	R	R	R/W	R	R/W	R

*5 All administrators and users can run [Connection Test].

[DDNS Configuration]

Settings	User	Mach	N/W	File	Unset	Set

	User	Mach	N/W	File	Unset	Set
[DDNS Configuration]	R	R	R/W	R	R/W	R

[WINS Configuration]

Settings	User	Mach	N/W	File	Unset	Set
[WINS Configuration]	R	R	R/W	R	R/W	R

[Machine Name]

Settings	User	Mach	N/W	File	Unset	Set
[Machine Name]	R	R	R/W	R	R/W	R

[Host Name]

Settings	User	Mach	N/W	File	Unset	Set
[Host Name]	R	R	R/W	R	R/W	R

[Domain Name Configuration]

Settings	User	Mach	N/W	File	Unset	Set
[Domain Name Configuration][4]	R	R	R/W	R	R/W	R

*4 When [Auto-Obtain (DHCP)] is set, the data is read-only.

[Ethernet Speed]

Settings	User	Mach	N/W	File	Unset	Set
[Ethernet Speed]	R	R	R/W	R	R/W	R

[Effective Protocol]

Settings	User	Mach	N/W	File	Unset	Set
[Effective Protocol]	R	R	R/W	R	R/W	R

[Optional Network]

Settings	User	Mach	N/W	File	Unset	Set
[IP Address (IPv4)]						
• [IP Address]	R	R	R/W	R	R/W	R
• [IPv4 Gateway Address]	R	R	R/W	R	R/W	R
[IP Address (IPv6)]						
• [IP Address]	R	R	R/W	R	R/W	R
• [IPv6 Gateway Address]	R	R	R/W	R	R	R
• [IPv6 Stateless Address Autoconfiguration]	R	R	R/W	R	R/W	R
[DHCPv6 Configuration]	R	R	R/W	R	R/W	R

[WINS Configuration]	R	R	R/W	R	R/W	R
[Host Name]	R	R	R/W	R	R	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[Effective Protocol]	R	R	R/W	R	R/W	R

[SMB]

Settings	User	Mach	N/W	File	Unset	Set
[SMB Computer Name]	R	R	R/W	R	R/W	R
[SMB Work Group]	R	R	R/W	R	R/W	R
[SMB Client Advanced Settings]	R	R	R/W	R	R/W	R

[Permit SNMPv3 Communication]

Settings	User	Mach	N/W	File	Unset	Set
[Permit SNMPv3 Communication]	R	R	R/W	R	R/W	R

[IEEE 802.1X Authentication]

Settings	User	Mach	N/W	File	Unset	Set
[IEEE 802.1X Authentication for Ethernet]	R	R	R/W	R	R/W	R

[Restore IEEE 802.1X Authentication to Defaults]	–	–	R/W	–	R/W	–

[Communication Security]

Settings	User	Mach	N/W	File	Unset	Set
[Permit SSL / TLS Communication]	R	R	R/W	R	R/W	R
[IPsec]	R	R	R/W	R	R/W	R

[Control Panel: LAN Type]

Settings	User	Mach	N/W	File	Unset	Set
[Control Panel: LAN Type]	–	–	R/W	–	R/W	–

[Control Panel: Port Forwarding]

Settings	User	Mach	N/W	File	Unset	Set
[Control Panel: Port Forwarding]	–	–	R/W	–	R/W	–

[Control Panel: Wireless LAN]

Settings	User	Mach	N/W	File	Unset	Set

Settings	User	Mach	N/W	File	Unset	Set
[Wi-Fi]	–	–	R/W	–	R/W	–
[Wireless Direct]	–	R	R/W	–	R/W	R
[Group Owner Mode]	–	R	R/W	–	R/W	R
[Device Name]	–	R	R/W	–	R/W	R
[Connection Password]	–	R	R/W	–	R/W	R
[DHCP Server IP Address]	–	R	R/W	–	R/W	R
[DHCP IP Address Range]	–	R	R/W	–	R/W	R
[Channel]	–	R	R/W	–	R/W	R
[SSID Header]	–	R	R/W	–	R/W	R
[Available Devices]	–	R/W	R/W	–	R/W	R/W
[Remembered Groups]	–	R/W	R/W	–	R/W	R/W

[Control Panel: Proxy Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Use Proxy]	–	R/W	–	–	R/W	–
[Proxy Address]	–	R/W	–	–	R/W	–
[Port Number]	–	R/W	–	–	R/W	–
[Enable Authentication]	–	R/W	–	–	R/W	–
[Login User Name]	–	R/W	–	–	R/W	–
[Login Password]	–	R/W	–	–	R/W	–
[Proxy Exceptions]	–	R/W	–	–	R/W	–

[Bluetooth]

Settings	User	Mach	N/W	File	Unset	Set
[Bluetooth]	–	R	R/W	–	R/W	R
[Name and Discoverable Settings]	–	R/W	R/W	–	R/W	R/W

[External Interface Software Settings]

Settings	User	Mach	N/W	File	Unset	Set
[External Interface Software Settings]	–	R/W	–	–	R/W	–

[Ping Command]

Settings	User	Mach	N/W	File	Unset	Set
[Ping Command]	–	–	R/W	–	R/W	–

[Print List]

Settings	User	Mach	N/W	File	Unset	Set
[Print List]	–	–	R/W	–	R/W	–

[Restore Factory Defaults for Network/Interface Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Restore Factory Defaults for Network/Interface Settings]	–	–	R/W	–	R/W	–

[Parallel Interface]

Settings	User	Mach	N/W	File	Unset	Set
[Parallel Timing]	R	R/W	R	R	R/W	R
[Parallel Communication Speed]	R	R/W	R	R	R/W	R
[Selection Signal Status]	R	R/W	R	R	R/W	R
[Input Prime]	R	R/W	R	R	R/W	R
[Bidirectional Communication]	R	R/W	R	R	R/W	R
[Signal Control]	R	R/W	R	R	R/W	R

[USB Port]

Settings	User	Mach	N/W	File	Unset	Set
[USB Port]	–	R/W	–	–	R/W	–

[USB Speed]

Settings	User	Mach	N/W	File	Unset	Set

[USB Speed]	–	R/W	–	–	R/W	–

[DIPRINT Timeout Period]

Settings	User	Mach	N/W	File	Unset	Set
[DIPRINT Timeout Period]	R	R	R/W	R	R/W	R

[Unconnected Network Instruction Screen]

Settings	User	Mach	N/W	File	Unset	Set
[Unconnected Network Instruction Screen]	–	–	R/W	–	R/W	R

Copyright © 2020, 2021

[Send (Email/Folder)]

[Email]

Settings	User	Mach	N/W	File	Unset	Set
[SMTP Server]	R	R	R/W	R	R/W	R
[SMTP Authentication][*6]	R	R/W	R	R	R/W	R
[POP before SMTP]	R	R/W	R	R	R/W	R
[Reception Protocol]	R	R/W	R	R	R/W	R
[POP3 / IMAP4 Settings]	R	R/W	R	R	R/W	R
[Administrator's Email Address]	R	R/W	R	R	R/W	R
[Email Communication Port]	R	R	R/W	R	R/W	R
[Email Reception Interval]	R	R	R/W	R	R/W	R
[Maximum Reception Email Size]	R	R	R/W	R	R/W	R
[Email Storage in Server]	R	R	R/W	R	R/W	R
[Register/Change/Delete Email Message]	R	R/W	R	R	R/W	R/W
[Auto Specify Sender Name]	R	R	R/W	R	R/W	R
[Auto Email Notification]	–	R/W	–	–	R/W	–

*6 Passwords cannot be read.

[Folder]

Settings	User	Mach	N/W	File	Unset	Set

[Default User Name / Password (Send)][*6]	R	R/W	R	R	R/W	R

*6 Passwords cannot be read.

[Settings for Administrator]

[Security Pattern/Stamp]

Settings	User	Mach	N/W	File	Unset	Set
[Detect Data Security for Copying]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Copier]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Document Server]	R	R/W	R	R	R/W	R
[Unauthorized Copy Prevention Printing: Printer]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp: Copier]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp: Document Server]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp: Fax]	R	R/W	R	R	R/W	R
[Compulsory Security Stamp: Printer]	R	R/W	R	R	R/W	R

[Data Management]

Settings	User	Mach	N/W	File	Unset	Set
[Auto Erase Memory Setting]	R	R/W	R	R	R	R
[Erase All Memory]	–	R/W	–	–	–	–
[Delete All Logs]	–	R/W	–	–	R/W	–
[Transfer Log Setting][*7]	R	R/W	R	R	R/W	R

[Collect Logs Settings]	R	R/W	R	R	R/W	R
[Allow Log Collection]	R	R/W	R	R	R/W	R
[Device Setting Information: Import Setting (Server)]	–	–	–	–	–	–
[Device Setting Information: Run Import (Server)]	–	–	–	–	–	–
[Device Setting Information: Export (Memory Storage Device)]	–	–	–	–	–	–
[Device Setting Information: Import (Memory Storage Device)]	–	–	–	–	–	–
[Restore Default Control Panel Settings]	–	R/W	–	–	R/W	–

*7 Can only be changed to [Off].

[File Management]

Settings	User	Mach	N/W	File	Unset	Set
[Machine Data Encryption Settings]	–	R/W	–	–	–	–
[Auto Delete File in Document Server]	R	R	R	R/W	R/W	R
[Delete All Files in Document Server]	–	–	–	R/W	R/W	–
[Capture: Delete All Unsent Files]	–	R/W	–	–	R/W	–
[Document Server Function]	–	R/W	–	–	–	–
[Default Privilege for Stored File]	R	R/W	R	R	R/W	R
[Capture Function]	–	R/W	–	–	–	–
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Capture Server IPv4 Address]	R	R/W	R	R	R/W	R

—

[Security]

Settings	User	Mach	N/W	File	Unset	Set
[Extended Security Settings]						
• [Driver Encryption Key]*8 (Permissions: Network Administrator)	–	–	R/W	–	R/W	–
• [Driver Encryption Key: Encryption Strength] (Permissions: Network Administrator)	R	R	R/W	R	R/W	R
• [Restrict Display of User Information]*8 (Permissions: Machine Administrator)	R	R/W	R	R	R/W	R
• [Enhance File Protection] (Permissions: File Administrator)	R	R	R	R/W	R	R
• [Restrict Use of Destinations (Fax)] (Permissions: User Administrator)	R/W	R	R	R	R	R
• [Restrict Use of Destinations (Scanner)] (Permissions: User Administrator)	R/W	R	R	R	R	R
• [Restrict Adding of User Destinations (Fax)] (Permissions: User Administrator)	R/W	R	R	R	R	R
• [Restrict Adding of User Destinations (Scanner)] (Permissions: User Administrator)	R/W	R	R	R	R	R
• [Transfer to Fax Receiver] (Permissions: Machine Administrator)	R	R/W	R	R	R	R
• [Authenticate Current Job]*8 (Permissions: Machine Administrator)	R	R/W	R	R	R/W	R
• [@Remote Service]	R	R/W	R	R	R/W	R

(Permissions: Machine Administrator)						
• [Update Firmware] (Permissions: Machine Administrator)	R	R/W	R	R	–	–
• [Change Firmware Structure] (Permissions: Machine Administrator)	R	R/W	R	R	–	–
• [Password Policy][8] (Permissions: User Administrator)	R/W	–	–	–	–	–
• [Settings by SNMPv1, v2] (Permissions: Network Administrator)	R	R	R/W	R	R/W	R
• [Security Setting for Access Violation] (Permissions: Machine Administrator)	–	R/W	–	–	–	–
• [Password Entry Violation] (Permissions: Machine Administrator)	–	R/W	–	–	–	–
• [Device Access Violation] (Permissions: Machine Administrator)	–	R/W	–	–	–	–
[Network Security Level]	R	R	R/W	R	–	–
[Access Control Function]	R	R	R/W	R	R/W	R
[Register/Delete Device Certificate]	–	–	R/W	–	R/W	–
[Service Mode Lock]	R	R/W	R	R	R/W	R
[HDD Authentication Code]	–	R/W	–	–	–	–
[CCC: Save Standard Values][9]	–	–	–	–	–	–
[CCC: Apply Standard Values][9]	–	–	–	–	–	–
[Credential Storage]	–	R/W	–	–	R/W	–
[Server Settings]	–	R/W	–	–	R/W	–

*8 This is displayed when Basic Authentication, Windows Authentication, or LDAP Authentication is used.

*9 R/W can be performed by the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Remote Panel Operation]

Settings	User	Mach	N/W	File	Unset	Set
[Remote Operation/Monitoring]	R	R/W	R	R	R	R

[Function Restriction]

Settings	User	Mach	N/W	File	Unset	Set
[Menu Protect]	R	R/W	R	R	R	R
[Restrict Functions of Each Application]	R	R/W	R	R	R/W	R

[Authentication/Charge]

[Administrator Authentication/User Authentication/App Auth.]

Settings	User	Mach	N/W	File	Unset	Set
[Administrator Authentication Management]	R/W *10*11	R/W *11	R/W *11	R/W *11	R/W	–
[Register/Change Administrator]	R/W *12	R/W *12	R/W *12	R/W *12	–	–
[User Authentication Management]	R	R/W	R	R	R/W	R
[Setting for Entering Authentication Password]	–	R/W	–	–	R/W	–
[Application Authentication Management]	–	R/W	–	–	–	–
[Application Authentication Settings]	R/W	R/W	–	–	–	–
[User's Own Customization]	–	R/W	–	–	R/W	–

[Register/Change/Delete Realm]	–	R/W	–	–	R/W	R
[Register/Change/Delete LDAP Server][*6]	–	R/W	–	–	R/W	R
[LDAP Search]	R	R/W	R	R	R	R

*6 Passwords cannot be read.

*10 Cannot be changed when the individual authentication function is used.

*11 Only the administrator privilege settings can be changed.

*12 Administrators can only change their own accounts.

[Print Volume Use Limitation]

Settings	User	Mach	N/W	File	Unset	Set
[Machine Action When Limit is Reached]	R	R/W	R	R	R	R
[Volume Use Counter: Scheduled/Specified Reset Settings]	R	R/W	R	R	R	R
[Print Volume Use Limitation: Default Limit Value]	R/W	R	R	R	R	R
[Print Volume Use Limitation: Unit Count Setting]	R	R/W	R	R	R	R
[Enhanced Print Volume Use Limitation]	R	R/W	R	R	R	R

[External Charge Unit Management]

Settings	User	Mach	N/W	File	Unset	Set
[Key Counter Management]	R	R/W	R	R	R/W	R
[External Charge Unit Management]	R	R/W	R	R	R/W	R
[Enhanced External Charge Unit Management]	R	R/W	R	R	R/W	R

[Switch Screen Type]

Settings	User	Mach	N/W	File	Unset	Set
[Switch Screen Type]	–	R/W	–	–	R/W	R

[Machine/Control Panel Information]

[Firmware Version]

Settings	User	Mach	N/W	File	Unset	Set
[Firmware Version]	R	R	R	R	R	R

[About Control Panel]

Settings	User	Mach	N/W	File	Unset	Set
[Status]	–	R	R	–	R	R
[Legal Information]	–	R	R	–	R	R
[Software Version List]	–	R	R	–	R	R
[Software Version History]	–	R	–	–	R	–

Copyright © 2020, 2021

[Extended Feature Information]

[Extended Feature Information]

Settings	User	Mach	N/W	File	Unset	Set
[Extended Feature Information]	R	R/W	R	R	R	R
[Heap/Stack Size Information]	R	R	R	R	R	R

[JavaTM Platform]

Settings	User	Mach	N/W	File	Unset	Set
[Counter]	R	R	R	R	R	R

Address Book (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Management]

[Management]

Settings	User	Mach	N/W	File	Unset	Set
[Print Address Book: Destination List]	R/W	–	–	–	R/W	R/W
[Edit Title]	R/W	–	–	–	R/W	–
[Default Title]	R/W	–	–	–	R/W	–
[Back Up/Restore Address Book]	R/W	–	–	–	R/W	–
[Default Search Conditions]	R	R/W	R	R	R	R
[Data Carry-Over Setting for Address Book Auto-Registration]	R/W	R	R	R	R/W	R
[Auto Delete User in Address Book]	R/W	R	R	R	R	R
[Delete All Data in Address Book]	R/W	–	–	–	–	–

Tray/Paper Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Tray/Paper Settings]

Copyright © 2020, 2021

[Tray/Paper Settings]

[Paper Size/Paper Type]

[Bypass Tray]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size: Printer]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R
[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[Tray 1]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R
[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[Tray 2]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R

[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[Tray 3]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R
[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[Tray 4]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R
[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[LCT]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Size]	R	R/W	R	R	R/W	R
[Paper Type/Thickness]	R	R/W	R	R	R/W	R
[Apply Duplex]	R	R/W	R	R	R/W	R
[Apply Auto Paper Select/Auto Tray Select]	R	R/W	R	R	R/W	R

[Paper Tray Priority]

Settings	User	Mach	N/W	File	Unset	Set
[Paper Tray Priority: Copier]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Fax]	R	R/W	R	R	R/W	R
[Paper Tray Priority: Printer]	R	R/W	R	R	R/W	R

[Common Settings/Others]

Settings	User	Mach	N/W	File	Unset	Set
[Cover Sheet Tray]	R	R/W	R	R	R/W	R
[Slip Sheet Tray]	R	R/W	R	R	R/W	R
[Size Entry Screen if Using Small Paper Unit]	R	R/W	R	R	R/W	R
[Auto Detect: Switch Paper Size Detected Legal/Oficio]	R	R/W	R	R	R/W	R

[Copy]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Paper Display] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R
[Auto Tray Switching]	R	R/W	R	R	R	R
[Display Bypass Tray Paper Settings]	R	R/W	R	R	R	R

[Display Paper Settings for Bypass Tray]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R

[Printer]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Sub Paper Size]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R

[Fax]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Paper Tray]	R	R/W	R	R	R/W	R

Copier/Document Server Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Scan]

[Paper/Paper Input]

[Finishing]

[Edit / Stamp]

[2 Sided / Combine]

[Reduce / Enlarge]

[Others]

[Scan]

[Original]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Original Type Priority]	R	R/W	R	R	R	R
[Original Photo Type Priority]	R	R/W	R	R	R	R
[Original Type Display] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R

[Batch/SADF]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switch to Batch]	R	R/W	R	R	R/W	R
[SADF Auto Reset]	R	R/W	R	R	R	R

[Color/Density]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Auto Image Density Priority]	R	R/W	R	R	R	R
[Background Density of ADS (Full Color / Two-color)]	R	R/W	R	R	R/W	R
[Color Sensitivity]	R	R/W	R	R	R/W	R

| [Auto Color Select Sensitivity] | R | R/W | R | R | R/W | R |
| [Auto Color Select Priority] | R | R/W | R | R | R/W | R |

[Paper/Paper Input]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Paper Display] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R
[Auto Tray Switching]	R	R/W	R	R	R	R
[Display Bypass Tray Paper Settings]	R	R/W	R	R	R	R
[Display Paper Settings for Bypass Tray]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R

[Finishing]

[Sort]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Memory Full Auto Scan Restart]	R	R/W	R	R	R	R

[Staple]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stapleless Position] (This item is enabled only when the [Copier (Classic)] is used.)	R	R/W	R	R	R/W	R
[Staple Position] (This item is enabled only when the [Copier (Classic)] is used.)	R	R/W	R	R	R/W	R

[Punch]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Punch Type] (This item is enabled only when the [Copier (Classic)] is used.)	R	R/W	R	R	R/W	R

[Fold]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Z-fold/Half Fold Output Tray Settings]	R	R/W	R	R	R	R
[Half Fold]	R	R/W	R	R	R	R
[Letter Fold-in]	R	R/W	R	R	R	R
[Letter Fold-out]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[Edit / Stamp]

[Margin]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Front Margin: Left / Right]	R	R/W	R	R	R	R
[Back Margin: Left / Right]	R	R/W	R	R	R	R
[Front Margin: Top / Bottom]	R	R/W	R	R	R	R
[Back Margin: Top / Bottom]	R	R/W	R	R	R	R
[1 Sided➔2 Sided Auto Margin: Left/Right]	R	R/W	R	R	R	R
[1 Sided➔2 Sided Auto Margin: Top to Bottom]	R	R/W	R	R	R	R

[Erase]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Erase Border Width]	R	R/W	R	R	R	R
[Erase Original Shadow in Combine]	R	R/W	R	R	R/W	R
[Erase Center Width]	R	R/W	R	R	R	R

[Stamp]

[Background Numbering]

Settings	User	Mach	N/W	File	Lv.1	Lv.2

	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Size Setting]	R	R/W	R	R	R/W	R
[Density Setting]	R	R/W	R	R	R/W	R
[Stamp Color Priority]	R	R/W	R	R	R	R

[Preset Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Language]	R	R/W	R	R	R/W	R
[Stamp Language Priority]	R	R/W	R	R	R	R
[Stamp Format]	R	R/W	R	R	R/W *1	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[User Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Program / Delete User Stamp]	R	R/W	R	R	R/W	R

[Date Stamp]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Format]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color]	R	R/W	R	R	R	R
[Stamp Setting]	R	R/W	R	R	R/W *1	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[Page Numbering]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stamp Format Priority]	R	R/W	R	R	R	R
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Duplex Back Page Stamp Position: Left/Right]	R	R/W	R	R	R/W	R
[Duplex Back Page Stamp Position: Top to Bottom]	R	R/W	R	R	R/W	R
[Page Numbering in Combine]	R	R/W	R	R	R/W	R
[Stamp on Designating Slip Sheet] (This item is enabled only when the [Copier (Classic)] is used.)	R	R/W	R	R	R/W	R
[Stamp Position]	R	R/W	R	R	R/W *1	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color Priority]	R	R/W	R	R	R/W	R

*1 Only adjustments to print position can be set. The print position itself cannot be configured.

[Stamp Text]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Font]	R	R/W	R	R	R/W	R
[Size]	R	R/W	R	R	R/W	R
[Superimpose]	R	R/W	R	R	R/W	R
[Stamp Color Priority]	R	R/W	R	R	R	R
[Stamp Setting]	R	R/W	R	R	R/W	R

| [Change Job Serial No. for First Job] | R | R/W | R | R | R | R |

[Edit Image]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Image Repeat Separation Line]	R	R/W	R	R	R/W	R
[Double Copies Separation Line]	R	R/W	R	R	R/W	R

Copyright © 2020, 2021

[2 Sided / Combine]

[2 Sided]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Original Orientation in Duplex Mode] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R
[Copy Orientation in Duplex Mode] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R

[Combine]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Copy Order in Combine]	R	R/W	R	R	R/W	R
[Separation Line in Combine]	R	R/W	R	R	R/W	R
[Front Cover Copy in Combine] (This item is enabled only when the[Copier (Classic)] is used.)	R	R/W	R	R	R/W	R
[Copy on Designating Page in Combine] (This item is enabled only when the [Copier (classic)] is used.)	R	R/W	R	R	R/W	R

[Book]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Orientation: Booklet, Magazine]	R	R/W	R	R	R/W	R

Copyright © 2020, 2021

[Reduce / Enlarge]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Shortcut Key : Copy Ratio]	R	R/W	R	R	R	R
[Copy Ratio Setting]	R	R/W	R	R	R	R
[Copy Ratio Priority Setting] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R	R
[Ratio for Create Margin]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[Others]

[Quantity]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Maximum Copy Quantity]	R	R/W	R	R	R	R

Settings	User	Mach	N/W	File	Unset	Set
[Copy Count Display]	R	R/W	R	R	R/W	R

[Customize Function]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Customize Function: Copy (Classic Mode)] (This is available only when [Copier (Classic)] is used.)	R	R/W	R	R	R/W	R
[Customize Func.: Document Srvr Storage]	R	R/W	R	R	R/W	R
[Customize Function: Copy (Standard Mode)]	R	R/W	R	R	R/W	R
[Customize Function: Copy (All View Mode)]	R	R/W	R	R	R/W	R
[Simplified Screen: Finishing Types]	R	R/W	R	R	R/W	R

[Number Keys / Preview]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switching: Number Keys / Preview]	R	R/W	R	R	R	R

Copyright © 2020, 2021

Fax Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Frequently Used Settings]

[Scan Settings]

[Send Settings]

[Reception Settings]

[Detailed Initial Settings]

[Others]

[Frequently Used Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Register Fax Information]	R	R/W	R	R	R	R
[Fax Records]	R	R/W	R	R	R	R
[Adjust Sound Volume]	R	R/W	R	R	R/W	R
[Reception Mode Settings]	R	R/W	R	R	R	R
[Action on Receiving File]	R	R/W	R	R	R	R
[Internet Fax/Email/Folder]	R	R/W	R	R	R	R
[Select Dial/Push Phone]	R	R/W	R	R	R	R
[IP-Fax Use Settings]	R	R	R/W	R	R	R

Copyright © 2020, 2021

[Scan Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register/Change/Delete Scan Size]	R	R/W	R	R	R/W	R
[Wait Time for Next Original: Exposure Glass]	R	R/W	R	R	R/W	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Maximum Email Size]	R	R	R/W	R	R	R
[Register/Change/Delete Standard Message]	R	R/W	R	R	R	R
[Memory File Transfer (If Unable to Print)]	–	R/W	–	–	–	–
[Backup File Transmission Setting]	R	R/W	R	R	R	R
[Number of Resends Settings]	R	R/W	R	R	R	R
[Prevent Incorrect Transmissions]	R	R/W	R	R	R	R
[Stored Fax File Auto Delete] (This setting item is valid only when using [Fax (Classic)].)	R	R	R	R/W	R	R
[Email address/Folder Path on Communication Log]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[Reception Settings]

[Reception File Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Action on Receiving File]	R	R/W	R	R	R	R
[Output Mode Switch Timer]	R	R/W	R	R	R	R
[Prohibit Auto Print]	R	R/W	R	R	R	R
[Print Standby to Print Files]	–	R/W	–	–	–	–
[Reception File Storing Error Setting]	R	R/W	R	R	R	R
[Reception File Storage Location]	R	R/W	R	R	R	R

[Reception Mode Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switch Reception Mode]	R	R/W	R	R	R	R

[Register Special Sender]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register/Change/Delete]	–	R/W	–	–	–	–
[Register Special Sender: Print List]	–	R/W	–	–	–	–
[Authorized Reception]	R	R/W	R	R	R	R

[Special Reception Function]	R	R/W	R	R	R	R
[Print/Store on Forwarding Special Sender]	R	R/W	R	R	R	R
[Receive Fax (Caller ID Blocked)]	R	R/W	R	R	R	R
[Bypass Tray Paper Size]	R	R/W	R	R	R	R

[Box Setting]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register/Change/Delete Box]	–	R/W	–	–	R	–
[Box Setting: Print List]	–	R/W	–	–	R/W	–

[Stored Reception File User Setting]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Stored Reception File User Setting]	R	R	R	R/W	R	R

[SMTP Reception File Delivery Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[SMTP Reception File Delivery Settings]	R	R/W	R	R	R	R

[Reception File Print Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[2 Sided Print]	R	R/W	R	R	R/W	R
[Combine Two Originals]	R	R/W	R	R	R/W	R
[Checkered Mark]	R	R/W	R	R	R/W	R
[Center Mark]	R	R/W	R	R	R/W	R
[Print Reception Time]	R	R/W	R	R	R/W	R
[Reception File Print Quantity]	R	R/W	R	R	R/W	R
[Paper Tray]	R	R/W	R	R	R/W	R
[Just Size Printing]	R	R/W	R	R	R	R
[Specify Tray for Lines]	R	R/W	R	R	R/W	R

[Folder Transfer Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Folder Transfer Result Report]	R	R/W	R	R	R	R
[Email address/Folder Path on Communication Log]	R	R/W	R	R	R	R
[File Name Setting in Folder Transfer]	R	R/W	R	R	R	R

[Remote Reception Setting per Line]

Settings	User	Mach	N/W	File	Lv.1	Lv.2

[Remote Reception Setting per Line]	R	R/W	R	R	R	R

[Delivery per Line]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Delivery per Line]	R	R/W	R	R	R	R

[Maximum Reception Size]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Maximum Reception Size]	R	R/W	R	R	R	R

[Trays for Paper Tray Selection]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Trays for Paper Tray Selection]	R	R/W	R	R	R	R

[Light Response after Receiving Fax]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Light Response after Receiving Fax]	R	R/W	R	R	R	R

[Detailed Initial Settings]

[Parameter Setting]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Parameter Setting]	R	R/W	R	R	R	R
[Parameter Setting: Print List]	–	R/W	–	–	R/W	–

[Register Closed Network Code]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register Closed Network Code]	–	R/W	–	–	R	–

[Register Memory Lock ID]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register Memory Lock ID]	–	R/W	–	–	R	–

[Internet Fax/Email/Folder]

Settings	User	Mach	N/W	File	Lv.1	Lv.2

[Internet Fax/Email/Folder]	R	R/W	R	R	R	R

[Select Dial/Push Phone]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Select Dial / Push Phone]	R	R/W	R	R	R	R

[Register Fax Information]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Register Fax Information]	R	R/W	R	R	R	R

[IP-Fax Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[IP-Fax Use Settings]	R	R	R/W	R	R	R
[H.323 Settings]	R	R	R/W	R	R	R
[SIP Settings]	R	R	R/W	R	R	R
[Register/Change/Delete Gateway]	R	R	R/W	R	R	R
[Server Use Settings]	R	R	R/W	R	R	R

[Security for Email Transmission Results]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Security for Email Transmission Results]	R	R/W	R	R	R	R

[Fax Email Account]

Settings	User	Mach	N/W	File	Unset	Set
[Fax Email Account]	R	R/W	R	R	R/W	R

[Destination List per Line]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Destination List per Line]	R	R/W	R	R	R	R
[Group Destination Display Style]	R	R/W	R	R	R	R

[G3 FAX Line Connection Check]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[G3 FAX Line Connection Check]	R	R/W	R	R	R	R

[Super G3 Communication Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Super G3 Communication Settings]	R	R/W	R	R	R	R

[Notification Email Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Notification Email Settings]	R	R/W	R	R	R	R

[Display Network Error]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Display Network Error]	R	R/W	R	R	R	R

[Destination Type Priority]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Destination Type Priority]	R	R/W	R	R	R	R

[Others]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Quick Operation Key] (This item is enabled only when the [Fax (Classic)] is used.)	R	R/W	R	R	R/W	R
[Switch Title]	R	R/W	R	R	R/W	R
[Search Destination]	R	R/W	R	R	R/W	R
[Communication Page Count]	R	R	R	R	R	R
[Adjust Sound Volume]	R	R/W	R	R	R/W	R
[On Hook Mode Release Time]	R	R/W	R	R	R/W	R
[Delete Recent Destinations]	–	R/W	–	–	–	–
[Report Auto Print Settings]	R	R/W	R	R	R	R
[Report Contents Settings]	R	R/W	R	R	R	R

Copyright © 2020, 2021

Printer Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[List/Test Print]

[Data Management/Maintenance]

[System]

[Host Interface]

[PCL Menu]

[PS Menu]

[PDF Menu]

[XPS Menu]

Copyright © 2020, 2021

[List/Test Print]

[Machine Information]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Multiple Lists]	–	R/W	–	–	R/W	R/W
[Configuration Page]	–	R/W	–	–	R/W	R/W
[Error Log]	–	R/W	–	–	R/W	R/W

[PDL Information]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PCL Config./Font Page]	–	R/W	–	–	R/W	R/W
[PS Config./Font Page]	–	R/W	–	–	R/W	R/W
[PDF Config./Font Page]	–	R/W	–	–	R/W	R/W

[Sample Pages]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Color Test Chart]	–	R/W	–	–	R/W	R/W

[Change Modes]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Hex Dump]	–	R/W	–	–	R/W	R/W

[Print Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Side(s) to Print of List/Test Print]	–	R/W	–	–	R/W	R/W

Copyright © 2020, 2021

[Data Management/Maintenance]

[Print Jobs]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Delete All Temporary Print Jobs]	–	–	–	R/W	–	–
[Delete All Stored Print Jobs]	–	–	–	R/W	–	–
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R
[Print Job Function]	R	R/W	R	R	R	R
[Jobs Not Printed as Machine Was Off]	R	R/W	R	R	R	R
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Auto Store Jobs Without User Authentication Information]	R	R/W	R	R	R	R
[Switch Initial Screen]	R	R/W	R	R	R	R

[Image Adjustment]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[4 Color Graphic Mode]	R	R/W	R	R	R	R

[Administrator Tools]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Prohibit List/Test Print]	R	R/W	R	R	R	R
[Stapleless Stapler and Staple Display Setting]	R	R/W	R	R	R	R
[Auto Cancel Print if Card Removed/No Units]	R	R/W	R	R	R	R

[System]

[Error Action]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Error Display Setting]	R	R/W	R	R	R	R
[Auto Cancel Confirmation for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[When Exceeded Max. Number of Sheets for Stapling]	R	R/W	R	R	R	R
[When Exceeded Max. Number of Sheets for Booklet]	R	R/W	R	R	R	R

[Paper In/Out]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Sub Paper Size]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R

[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Job Separation]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R

[Emulation]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Printer Language]	R	R/W	R	R	R	R
[Default Printer Language]	R	R/W	R	R	R	R

[Print Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Copies]	R	R/W	R	R	R	R
[2 Sided Print]	R	R/W	R	R	R	R
[Blank Page Print]	R	R/W	R	R	R	R
[Page Size]	R	R/W	R	R	R/W	R
[Edge to Edge Print]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R

[Memory]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Memory Usage]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[Host Interface]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[I/O Buffer]	R	R/W	R	R	R	R
[I/O Timeout]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[PCL Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Orientation]	R	R/W	R	R	R	R
[Form Lines]	R	R/W	R	R	R	R
[Font Source]	R	R/W	R	R	R	R
[Font Number]	R	R/W	R	R	R	R
[Point Size]	R	R/W	R	R	R	R
[Font Pitch]	R	R/W	R	R	R	R
[Symbol Set]	R	R/W	R	R	R	R
[Nimbus Mono Font]	R	R/W	R	R	R	R
[Extend A4 Width]	R	R/W	R	R	R	R
[Append CR to LF]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Tray Parameters (PCL)]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[PS Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Job Timeout]	R	R/W	R	R	R	R
[Wait Timeout]	R	R/W	R	R	R	R
[Paper Selection Method]	R	R/W	R	R	R	R
[Switching between 1 & 2 Sided Print]	R	R/W	R	R	R	R
[Data Format]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Color Setting]	R	R/W	R	R	R	R
[Color Profile]	R	R/W	R	R	R	R
[Process Color Model]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R
[Gray Reproduction]	R	R/W	R	R	R	R
[Font Change Confirmation]	R	R/W	R	R	R	R
[Tray Parameters (PS)]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[PDF Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Change PDF Password]	R	R/W	R	R	R	R
[PDF Group Password]	R	R/W	R	R	R	R
[Reverse Order Printing]	R	R/W	R	R	R	R
[Resolution]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Color Setting]	R	R/W	R	R	R	R
[Color Profile]	R	R/W	R	R	R	R
[Process Color Model]	R	R/W	R	R	R	R
[Orientation Auto Detect]	R	R/W	R	R	R	R

[XPS Menu]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Resolution]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Color Profile]	R	R/W	R	R	R	R
[Process Color Model]	R	R/W	R	R	R	R
[Gray Reproduction]	R	R/W	R	R	R	R

Scanner Settings (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Scan]

[Sending Settings]

[Others]

Copyright © 2020, 2021

[Scan]

[Color/Density]

Settings	User	Mach	N/W	File	Unset	Set
[Auto Color Select Sensitivity Level]	R	R/W	R	R	R	R
[Background Density of ADS (Full Color)]	R	R/W	R	R	R	R

[Size/Reduce/Enlarge]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Program/Edit/Delete Scan Size]	R	R/W	R	R	R	R
[Scan Ratio Setting]	R	R/W	R	R	R	R
[Mixed Sizes Mode]	R	R/W	R	R	R	R

[Blank Page Detection]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Blank Page Detection]	R	R/W	R	R	R	R
[Blank Page Detection Level]	R	R/W	R	R	R	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R

[Timer Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Wait Time for Next Original(s): Exposure Glass]	R	R/W	R	R	R	R
[Wait Time for Next Original(s): SADF]	R	R/W	R	R	R	R
[PC Scan Command Standby Time]	R	R/W	R	R	R	R

Copyright © 2020, 2021

[Sending Settings]

[File Name]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Number of Digits for Single Page Files]	R	R/W	R	R	R/W	R

[Compression Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression Method (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale/Full Color)]	R	R/W	R	R	R/W	R
[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[High Compression PDF Level]	R	R/W	R	R	R/W	R

[Email (Subject/Text)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Default Email Subject]	R	R/W	R	R	R	R
[Insert Additional Email Information]	R	R/W	R	R	R/W	R

[Email (Size)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Maximum Email Size]	R	R	R/W	R	R	R
[Divide & Send Email]	R	R	R/W	R	R	R

[Email (URL Link)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[File Emailing Method]	R	R/W	R	R	R/W	R
[Download File Directly From URL Link]	R	R/W	R	R	R/W	R
[URL File Storage Period]	R	R/W	R	R	R/W	R

[Resend Settings]

Settings	User	Mach	N/W	File	Unset	Set
[Scanner Resend]	R	R	R/W	R	R/W	R
[Scanner Resend Interval Time]	R	R	R/W	R	R/W	R

Copyright © 2020, 2021

[Others]

[Address Book Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Switch Title]	R	R/W	R	R	R	R
[Search Destination]	R	R/W	R	R	R	R
[Destination List Display Priority 1] (This setting item becomes valid only when using [Scanner (Classic)].)	R	R/W	R	R	R	R
[Destination List Display Priority 2]	R	R/W	R	R	R	R
[Login User Address Priority]	R	R/W	R	R	R/W	R
[Program Setting for Destinations]	R	R/W	R	R	R	R
[External Authentication: Folder Path Overwrite Setting]	R	R/W	R	R	R	R

[History Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print & Delete Scanner Records]	R	R/W	R	R	R	R
[Print Scanner Records]	R	R/W	R	R	R	R
[Delete Scanner Records]	R	R/W	R	R	R	R
[Delete Recent Destinations]	R	R/W	R	R	R	R
[Scanner Records with no Privileges]	R	R/W	R	R	R	R

(This setting item is invalid when using [Scanner (Classic)].)					

[WSD/DSM Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Use WSD or DSM] (This setting item is invalid when using [Scanner (Classic)].)	R	R/W	R	R	R/W	R
[Use a Destination List that is not DSM] (This setting item is invalid when using [Scanner (Classic)].)	R	R/W	R	R	R/W	R
[Display WSD Destination List] (This setting item is invalid when using [Scanner (Classic)].)	R	R/W	R	R	R	R
[Prohibit WSD Scan Command]	R	R/W	R	R	R	R

Copyright © 2020, 2021

Maintenance (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

Settings	User	Mach	N/W	File	Unset	Set
[Auto Color Calibration]	–	R/W	–	–	R/W	–
[Color Registration]	–	R/W	–	–	R/W	–

Copyright © 2020, 2021

Counter (Settings Screen Type: Standard)

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Related topics

[Counter]

[Counter]

Settings	User	Mach	N/W	File	Unset	Set
[Display/Print Counter]	–	R/W	–	–	R/W	R/W
[Display/Clear/Print Counter per User]	R/W *1	R/W *2	R	R	R/W	–
[Display/Clear Eco-friendly Counter per User]	–	R/W	–	–	–	–
[Eco-friendly Counter Period/Administrator Message]	R	R/W	R	R	R	R
[Display/Clear Eco-friendly Counter]	–	R/W	–	–	–	–

*1 Can only be cleared.
*2 Can only be printed.

Copyright © 2020, 2021

How to Read (Other than Initial Settings)

⭐ Important

- The Manual covers various types of the machines. Descriptions in the Manual may differ from your model.

Understanding headers

- User

  The user administrator has privileges for this operation.

- Mach

  The machine administrator has privileges for this operation.

- N/W

  The network administrator has privileges for this operation.

- File

  The file administrator has privileges for this operation.

- Unset

  The logged in user has privileges for this operation.

  In cases where no settings are selected in [Available Settings] of [Administrator Authentication Management].

- Set

  The logged in user has privileges for this operation.

  Status when settings are selected in [Available Settings] of [Administrator Authentication Management].

- Lv.1

  In cases where the [Menu Protect] setting is set to [Level 1].

- Lv.2

  In cases where the [Menu Protect] setting is set to [Level 2].

Understanding the symbols

R/W: Executing, changing, and reading possible.

R: Reading is possible.

-: Executing, changing, and reading are not possible.

Printer Functions

This section lists the printer functions that appear if [Printer] or [Printer (Classic)] on the Home screen is pressed.

When administrator authentication is set, the restrictions to user operations differ depending on the [Menu Protect] setting.

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Job List]	R	R	R	R	R	R
[Print Jobs]	R	R	R	R/W	R/W	R/W
[Print from Memory Storage Device]	–	–	–	–	R/W	R/W
[Job Reset]	R/W	R/W	R/W	R/W	R/W	R/W
[Job Operation]	R/W	R/W	R/W	R/W	R/W	R/W
[Form Feed]	R/W	R/W	R/W	R/W	R/W	R/W
[Spooling Job List]	R	R/W	R	R	R	R
[Error Log]	–	R	–	–	R	R

Copyright © 2020, 2021

>Edit Home

Edit Home

When administrator authentication is set, the restrictions to user operations differ depending on the configurations in [Available Settings].

Settings	User	Mach	N/W	File	Unset	Set
Adding Icon/Widget/Folder	–	R/W	–	–	R/W	–
Rearranging Icon/Widget/Folder	–	R/W	–	–	R/W	–
Deleting Icon/Widget/Folder	–	R/W	–	–	R/W	–
Changing the Wallpaper	–	R/W	–	–	R/W	–

Copyright © 2020, 2021

Quick Card Authentication Config.

Settings	User	Mach	N/W	File
[Use Authentication]/[Do not Use Authentication]	–	R/W	–	–
[Address Book Management]	R/W	–	–	–
[User Priority Settings]	R/W	–	–	–
[Proximity Card Rdr. Settng.]	–	R/W	–	–
[NFC Card Reader Settings]	–	R/W	–	–
[Bluetooth Settings]	–	R/W	–	–

Copyright © 2020, 2021

>Web Image Monitor: Display Eco-friendly Counter

Web Image Monitor: Display Eco-friendly Counter

These settings are in [Status/Information].

A user can only view their own counter.

Settings	User	Mach	N/W	File	Unset	Set
[Download]	–	R/W	–	–	–	–
[Device Total Counter]	–	R	–	–	–	–
[Counter per User]	–	R	–	–	R	R

Copyright © 2020, 2021

Web Image Monitor: Job

These settings are in [Status/Information].

Users can only change jobs they executed themselves.

When administrator authentication is set, the restrictions to user operations differ depending on the Available Settings setting.

[Job List]

Settings	User	Mach	N/W	File	Unset	Set
[Current/Waiting Jobs]: [Delete Reservation]	–	R/W	–	–	–	R/W
[Current/Waiting Jobs]: [Suspend Printing]/[Resume Printing]	–	R/W	–	–	–	–
[Current/Waiting Jobs]: [Change Order]	–	R/W	–	–	–	–
[Job History]	–	R/W	–	–	R	R[*1]

*1 Can be viewed when [User Code Authentication] is enabled for the user authentication method.

[Printer]

Settings	User	Mach	N/W	File	Unset	Set
[Spool Printing]: [Delete]	R	R/W	R	R	R	R
[Job History]	R	R/W	R	R	R	R
[Error Log]	–	R	–	–	R	R

[Fax History]

Settings	User	Mach	N/W	File	Unset	Set
[All items]	–	R	–	–	R	R^{*2}

*2 Can be viewed when user code authentication is enabled for the user authentication method.

[Document Server]

Settings	User	Mach	N/W	File	Unset	Set
[All items]	–	R	–	–	R	R^{*3}

*3 Can be viewed when [User Code Authentication] is enabled for the user authentication method.

Copyright © 2020, 2021

Web Image Monitor: Screen

These settings are in [Configuration] in [Device Management].

[Screen]

Settings	User	Mach	N/W	File	Unset	Set
All items	R/W	R/W	R/W	R/W	–	–

Copyright © 2020, 2021

Web Image Monitor: Device Settings

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

[System]

Settings	User	Mach	N/W	File	Unset	Set
[Device Name]	R	R	R/W	R	R/W	R
[Comment]	R	R	R/W	R	R/W	R
[Location]	R	R	R/W	R	R/W	R
[Spool Printing]	R	R/W	R	R	R/W	R
[Protect Printer Display Panel]	R	R/W	R	R	–	–
[Interleave Priority]	R	R/W	R	R	R/W	R
[Function Reset Timer]	R	R/W	R	R	R/W	R
[Stop Key to Suspend Print Job]	R	R/W	R	R	R/W	R
[Display IP Address on Device Display Panel]	R	R/W	R	R	–	–
[Media Slot Use]	R	R/W	R	R	R	R
[Compatible ID]	R	R/W	R	R	R/W	R
[PDF File Type: PDF/A Fixed]	R	R/W	R	R	R/W	R
[Stapleless Stapler Settings]	R	R/W	R	R	R/W	R
[Prohibit printing stored files from Web Image Monitor]	R	R/W	R	R	R	R
[Human Detection Sensor]	R	R/W	R	R	R/W	R

[Energy Saving Recovery for Business Application]	R	R/W	R	R	R/W	R
[Silent Mode]	R	R/W	R	R	R/W	R
[Main Power On by Remote Operation]	R/W	R/W	R/W	R/W	R/W	R/W
[Ready State After Printing]	R	R/W	R	R	R/W	R
[ADF Operation]	R	R/W	R	R	R/W	R
[Screen display function when network is not connected]	R	R/W	R	R	R/W	R
[Shift to Main Power-Off When Network Disconnected]	R	R/W	R	R	R/W	R
[Output Priority When Paper is Fed to Finisher]	R	R/W	R	R	R/W	R
[Ability to log out while scanning]	R	R/W	R	R	R/W	R
[Allow Log Collection]	R	R/W	R	R	R	R
[Output Tray]	R	R/W	R	R	R/W	R
[Paper Tray Priority]	R	R/W	R	R	R/W	R
[Cover Sheet Tray]	R	R/W	R	R	R/W	R
[Slip Sheet Tray]	R	R/W	R	R	R/W	R

[Paper]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Date/Time]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Timer]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Logs]

Settings	User	Mach	N/W	File	Unset	Set
All items[*1]	R	R/W	R	R	R/W	R

*1 [Transfer Logs] is enabled to change to [Inactive] only.

[Download Logs]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

[SYSLOG Transfer Setting]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Email]

Settings	User	Mach	N/W	File	Unset	Set
[Administrator Email Address]	–	R/W	–	–	R/W	R
[Auto Specify Sender Name]	–	R/W	–	–	R/W	R
[Signature]	–	R/W	–	–	R/W	R
[Image of Signature]	–	R/W	–	–	R/W	R
[Signature Image Preview]	–	R/W	–	–	R/W	R
[Reception Protocol]	–	R/W	–	–	R/W	R
[Email Reception Interval]	–	–	R/W	–	R/W	R
[Max. Reception Email Size]	–	–	R/W	–	R/W	R
[Email Storage in Server]	–	–	R/W	–	R/W	R
[SMTP Server Name]	–	–	R/W	–	R/W	R
[SMTP Port No.]	–	–	R/W	–	R/W	R
[Use Secure Connection (SSL)]	–	–	R/W	–	R/W	R
[SMTP Authentication]	–	R/W	–	–	R/W	R
[SMTP Auth. Email Address]	–	R/W	–	–	R/W	R
[SMTP Auth. User Name]	–	R/W	–	–	R/W	–
[SMTP Auth. Password][*2]	–	R/W	–	–	R/W	–

[SMTP Auth. Encryption]	–	R/W	–	–	R/W	R
[POP before SMTP]	–	R/W	–	–	R/W	R
[POP Email Address]	–	R/W	–	–	R/W	R
[POP User Name]	–	R/W	–	–	R/W	–
[POP Password][*2]	–	R/W	–	–	R/W	–
[Timeout setting after POP Auth.]	–	R/W	–	–	R/W	R
[POP3/IMAP4 Server Name]	–	R/W	–	–	R/W	R
[POP3/IMAP4 Encryption]	–	R/W	–	–	R/W	R
[POP3 Reception Port No.]	–	–	R/W	–	R/W	R
[IMAP4 Reception Port No.]	–	–	R/W	–	R/W	R
[Fax Email Address]	–	R/W	–	–	R/W	R
[Receive Fax Email]	–	R/W	–	–	R/W	–
[Fax Email User Name]	–	R/W	–	–	R/W	–
[Fax Email Password][*2]	–	R/W	–	–	R/W	–
[Email Notification E-mail Address]	–	R/W	–	–	R/W	R
[Receive Email Notification]	–	R/W	–	–	R/W	–
[Email Notification User Name]	–	R/W	–	–	R/W	–
[Email Notification Password][*2]	–	R/W	–	–	R/W	–

*2 Passwords cannot be read.

[Auto Email Notification]

Settings	User	Mach	N/W	File	Unset	Set

[All items]	R	R/W	R	R	R/W	R

[On-demand Email Notification]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[File Transfer]

Settings	User	Mach	N/W	File	Unset	Set
[SMB User Name]	–	R/W	–	–	R/W	–
[SMB Password]*2	–	R/W	–	–	R/W	–
[FTP User Name]	–	R/W	–	–	R/W	–
[FTP Password]*2	–	R/W	–	–	R/W	–

*2 Passwords cannot be read.

[Conditions to Search Address Book]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

[User Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Administrator Authentication Management]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator Authentication]	R/W	R	R	R	R	R
[Machine Administrator Authentication]	R	R/W	R	R	R	R
[Network Administrator Authentication]	R	R	R/W	R	R	R
[File Administrator Authentication]	R	R	R	R/W	R	R

[Program/Change Administrator]

Settings	User	Mach	N/W	File	Unset	Set
[User Administrator]	R/W	R	R	R	–	–
[Machine Administrator]	R	R/W	R	R	–	–
[Network Administrator]	R	R	R/W	R	–	–
[File Administrator]	R	R	R	R/W	–	–
[Login User Name][*3]	R/W	R/W	R/W	R/W	–	–
[Login Password][*3]	R/W	R/W	R/W	R/W	–	–
[Encryption Password][*3]	R/W	R/W	R/W	R/W	–	–

*3 Administrators can only change their own accounts.

[Print Volume Use Limitation]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R	R

[LDAP Server]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	R/W	–

[Firmware Update]

Settings	User	Mach	N/W	File	Unset	Set
[Update]	–	R/W	–	–	–	–
[Firmware Version]	–	R	–	–	–	–
[Application Version]	–	R	–	–	–	–

[Kerberos Authentication]

Settings	User	Mach	N/W	File	Unset	Set

Settings						
All items	–	R/W	–	–	–	–

[Program/Change/Delete Remote Machine]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

[Device Setting Information: Import Setting (Server)]

Settings	User	Mach	N/W	File	Unset	Set
All items[*4]	–	–	–	–	–	–

*4 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Import Test]

Settings	User	Mach	N/W	File	Unset	Set
[Start][*4]	–	–	–	–	–	–

*4 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Import/Export Device Setting Information]

Settings	User	Mach	N/W	File	Unset	Set

Settings	User	Mach	N/W	File	Unset	Set
All items[4]	–	–	–	–	–	–

*4 R/W is the administrator with all privileges that include user administrator, machine administrator, network administrator, and file administrator privileges.

[Eco-friendly Counter Period/Administrator Message]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R/W	R

[Compulsory Security Stamp]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Copier]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Document Server]

Settings	User	Mach	N/W	File	Unset	Set

All items	R	R/W	R	R	R	R

[Unauthorized Copy Prevention: Printer]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R	R

[Program/Change USB Device List]

Settings	User	Mach	N/W	File	Unset	Set
[Device 1-10]	R	R/W	R	R	R/W	R

[Restrict Application Functions]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R/W	R	R	R	R

Web Image Monitor: Printer

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the [Menu Protect] setting.

[Basic Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Print Error Report]	R	R/W	R	R	R	R
[Auto Continue]	R	R/W	R	R	R	R
[Memory Overflow]	R	R/W	R	R	R	R
[Error Display Setting]	R	R/W	R	R	R	R
[Auto Cancel Confirmation for PDL Error Job]	R	R/W	R	R	R	R
[Auto Cancel for Print Job(s) on Error]	R	R/W	R	R	R	R
[Rotate Sort: Auto Paper Continue]	R	R/W	R	R	R	R
[Auto Delete Temporary Print Jobs]	R	R	R	R/W	R	R
[Auto Delete Stored Print Jobs]	R	R	R	R/W	R	R
[Print Job Function]	R	R/W	R	R	R	R
[Stapleless Stapler and Staple Display Setting]	R	R/W	R	R	R	R
[Jobs Not Printed As Machine Was Off]	R	R/W	R	R	R	R
[Rotate by 180 Degrees]	R	R/W	R	R	R	R
[Print Compressed Data]	R	R/W	R/W	R	R	R
[Memory Usage]	R	R/W	R	R	R	R

[Copies]	R	R/W	R	R	R	R
[Toner Saving]	R	R/W	R	R	R	R
[Reserved Job Waiting Time]	R	R/W	R	R	R	R
[Printer Language]	R	R/W	R	R	R	R
[Sub Paper Size]	R	R/W	R	R	R	R
[Letterhead Setting]	R	R/W	R	R	R	R
[Tray Setting Priority]	R	R/W	R	R	R	R
[Paper Weight by Paper Type if Command selected for Tray Setting Priority]	R	R/W	R	R	R	R
[Paper Mismatch Alert for Bypass Tray]	R	R/W	R	R	R	R
[Store and Skip Errored Job]	R	R/W	R	R	R	R
[Tray Switching]	R	R/W	R	R	R	R
[List/Test Print Lock]	R	R/W	R	R	R	R
[Extended Auto Tray Switching]	R	R/W	R	R	R	R
[Virtual Printer]	R	R/W	R	R	R	R
[Gray Reproduction (Expand Gray Recognition)]	R	R/W	R	R	R	R
[Restrict Direct Print Jobs]	R	R/W	R	R	R	R
[Initial screen switch setting]	R	R/W	R	R	R	R
[When Exceeded Max. Number of Sheets for Stapling]	R	R/W	R	R	R	R
[When Exceeded Max. Number of Sheets for Booklet]	R	R/W	R	R	R	R
[Host Interface]	R	R/W	R	R	R	R
[PCL Menu]	R	R/W	R	R	R	R
[PS Menu]	R	R/W	R	R	R	R

[PDF Menu]	R	R/W	R	R	R	R
[XPS Menu]	R	R/W	R	R	R	R

[Tray Parameters (PCL)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Tray Parameters (PCL)]	–	R/W	–	–	–	–

[Tray Parameters (PS)]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Tray Parameters (PS)]	–	R/W	–	–	–	–

[PDF Temporary Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Temporary Password]	–	–	–	–	R/W	R/W

[PDF Group Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2

[PDF Group Password]	–	R/W	–	–	–	–

[PDF Fixed Password]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[PDF Fixed Password]	–	R/W	–	–	–	–

[Virtual Printer Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Virtual Printer Name]	R	R/W	R	R	R	R
[Protocol]	R	R/W	R	R	R	R
[RHPP Settings][*1]	R	R/W	R	R	R/W	R/W

*1 For details about the operation privileges of the other settings, see [Basic Settings].

[Permissions for Printer Language to Operate File System]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	R	R/W	R	R	R	R

[Google Cloud Print Settings]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	R/W	–	–	–

Copyright © 2020, 2021

Web Image Monitor: Fax

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the [Menu Protect] setting.

[Initial Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	R/W	–	–	–	–

[Send / Reception Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Maximum Email Size]	–	–	R/W	–	–	–
[Switch Reception Mode]	–	R/W	–	–	–	–
[SMTP RX File Delivery Settings]	–	R/W	–	–	–	–
[2 Sided Print]	–	R/W	–	–	R/W	–
[Checkered Mark]	–	R/W	–	–	R/W	–
[Center Mark]	–	R/W	–	–	R/W	–
[Print Reception Time]	–	R/W	–	–	R/W	–
[Reception File Print Quantity]	–	R/W	–	–	R/W	–
[Paper Tray]	–	R/W	–	–	R/W	–

| [Memory Lock Reception] | – | R/W | – | – | – | – |

[Reception File Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	R/W	–	–	–	–

[IP-Fax Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	–	R/W	–	–	–

[IP-Fax Gateway Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	–	R/W	–	–	–

[Parameter Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	R/W	–	–	–	–

>Web Image Monitor: Scanner

Web Image Monitor: Scanner

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the [Menu Protect] setting.

[General Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	R	R/W	R	R	R	R

[Scan Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	R	R/W	R	R	R	R

[Send Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
[Compression (Black & White)]	R	R/W	R	R	R/W	R
[Compression (Gray Scale/Full Color)]	R	R/W	R	R	R/W	R
[OCR Scanned PDF: Blank Page Sensitivity]	R	R/W	R	R	R/W	R
[High Compression PDF Level]	R	R/W	R	R	R/W	R

[Compression Method for High Compression PDF]	R	R/W	R	R	R/W	R
[Max. Email Size]	R	R	R/W	R	R[*1]	R[*1]
[Divide & Send Email]	R	R	R/W	R	R[*1]	R[*1]
[Insert Additional Email Info]	R	R/W	R	R	R/W	R
[No. of Digits for Single Page Files]	R	R/W	R	R	R/W	R
[Default Email Subject]	R	R/W	R	R	R	R
[File Emailing Method]	R	R/W	R	R	R/W	R
[URL File Storage Period]	R	R/W	R	R	R/W	R

*1 When [Network Management] in [Administrator Authentication Management] is set to [Off], users are assigned with R/W privileges.

[Initial Settings]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	R	R/W	R	R	R	R

[Default Settings for Normal Screens(Classic) on Device]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	R/W	–	–	R	R

[Default Settings for Simplified Screens(Classic) on Device]

Settings	User	Mach	N/W	File	Lv.1	Lv.2
All items	–	R/W	–	–	R	R

Copyright © 2020, 2021

Web Image Monitor: Interface

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

[Interface Settings]

Settings	User	Mach	N/W	File	Unset	Set
[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Ethernet Security]	R	R	R/W	R	R/W	R
[Ethernet Speed]	R	R	R/W	R	R/W	R
[Bluetooth]	R	R	R/W	R	R/W	R
[Operation Mode]	R	R	R/W	R	R/W	R
[USB]	R	R/W	R	R	R/W	R
[USB Host]	R	R/W	R	R	R/W	R
[PictBridge]	R	R/W	R	R	R/W	R
[Parallel Interface]	R	R/W	R	R	R/W	R

[Wireless LAN Settings]

Settings	User	Mach	N/W	File	Unset	Set

[LAN Type]	–	–	R/W	–	R	–
[Network]	R	R	R	R	R	R
[Firmware Version]	R	R	R	R	R	R
[MAC Address]	R	R	R	R	R	R
[Available Wireless LAN]	R	R	R	R	R	R
[Wireless Signal Status]	R	R	R	R	R	R
[Communication Mode]	R	R	R/W	R	R/W	R
[SSID]	R	R	R/W	R	R/W	R
[Channel]	R	R	R/W	R	R/W	–
[Security Method]	R	R	R/W	R	R/W	R
[WEP Settings]	R	R	R/W	R	R/W	R
[WPA2 Settings]	R	R	R/W	R	R/W	R
[Direct Connection Settings]	R	R	R/W	R	R/W	R

Copyright © 2020, 2021

Web Image Monitor: Network

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

[IPv4]

Settings	User	Mach	N/W	File	Unset	Set
[IPv4]	R	R	R/W *1	R	R/W *1	R
[Host Name]	R	R	R/W	R	R/W	R
[DHCP]	R	R	R/W	R	R/W	R
[Domain Name]	R	R	R/W	R	R/W	R
[IPv4 Address]	R	R	R/W	R	R/W	R
[Subnet Mask]	R	R	R/W	R	R/W	R
[DDNS]	R	R	R/W	R	R/W	R
[WINS]	R	R	R/W	R	R/W	R
[Primary WINS Server]	R	R	R/W	R	R/W	R
[Secondary WINS Server]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Scope ID]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

*1 You cannot disable IPv4 when using Web Image Monitor through an IPv4 connection.

[IPv6]

Settings	User	Mach	N/W	File	Unset	Set
[IPv6]	R	R	R/W *2	R	R/W *2	R
[Host Name]	R	R	R/W	R	R/W	R
[Domain Name]	R	R	R/W	R	R/W	R
[Link-local Address]	R	R	R	R	R	R
[Stateless Address]	R	R	R/W	R	R/W	R
[Manual Configuration Address]	R	R	R/W	R	R/W	R
[DHCPv6]	R	R	R/W	R	R/W	R
[DHCPv6 Address]	R	R	R	R	R	R
[DDNS]	R	R	R/W	R	R/W	R
[LLMNR]	R	R	R/W	R	R/W	R
[Details]	R	R	R/W	R	R/W	R

*2 You cannot disable IPv6 when using Web Image Monitor through an IPv6 connection.

[SMB]

Settings	User	Mach	N/W	File	Unset	Set
[SMB]	R	R	R/W	R	R/W	R
[Protocol]	R	R	R	R	R	R
[Workgroup Name]	R	R	R/W	R	R/W	R
[Computer Name]	R	R	R/W	R	R/W	R

[Comment]	R	R	R/W	R	R/W	R
[Share Name]	R	R	R	R	R	R
[Advanced Settings]	R	R	R/W	R	R/W	R

[SNMP]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[SNMPv3]

Settings	User	Mach	N/W	File	Unset	Set
[SNMP]	–	–	R/W	–	–	–
[Protocol]	–	–	R/W	–	–	–
[SNMPv3 Setting]	–	–	R/W	–	–	–
[SNMPv3 Trap Communication Setting]	–	–	R/W	–	–	–
[Account(User)]	–	–	R/W	–	–	–
[Account(Network Administrator)]	–	–	R/W	–	–	–
[Account(Machine Administrator)]	–	R/W	–	–	–	–

[SSDP]

Settings	User	Mach	N/W	File	Unset	Set
[SSDP]	–	–	R/W	–	–	R/W
[UUID]	–	–	R	–	–	R
[Profile Expires]	–	–	R/W	–	–	R/W
[TTL]	–	–	R/W	–	–	R/W

[Bonjour]

Settings	User	Mach	N/W	File	Unset	Set
[Bonjour]	R	R	R/W	R	R/W	R
[Local Hostname]	R	R	R	R	R	R
[Details]	R	R	R/W	R	R/W	R
[Print Order Priority]	R	R	R/W	R	R/W	R

[AirPrint]

Settings	User	Mach	N/W	File	Unset	Set
All items	R	R	R/W	R	R/W	R

[Option Network Interface]

Settings	User	Mach	N/W	File	Unset	Set

| All items | R | R | R/W | R | R/W | R |

[System Log]

Settings	User	Mach	N/W	File	Unset	Set
[System Log]	R	R	R	R	R	R

Copyright © 2020, 2021

Web Image Monitor: Security

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the [Available Settings] setting.

[To use this machine safely]

Settings	User	Mach	N/W	File	Unset	Set
All items	R/W	R/W	R/W	R/W	–	–

[Network Security]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[Access Control]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[IPP Authentication]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[SSL/TLS]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[Root Certificate]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[Device Certificate]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[S/MIME]

Settings	User	Mach	N/W	File	Unset	Set

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[IPsec]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[User Lockout Policy]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

[IEEE 802.1X]

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	R/W	–	–	–

[Extended Security]

Settings	User	Mach	N/W	File	Unset	Set
[Driver Encryption Key]	–	–	R/W	–	R/W	–
[Driver Encryption Key: Encryption Strength]	R	R	R/W	R	R/W	R

[Restrict Display of User Information]	R	R/W	R	R	R/W	R
[Enhance File Protection]	R	R	R	R/W	R	R
[Restrict Use of Destinations (Fax)]	R/W	R	R	R	R	R
[Restrict Use of Destinations (Scanner)]	R/W	R	R	R	R	R
[Transfer to Fax Receiver]	R	R/W	R	R	R	R
[Authenticate Current Job]	R	R/W	R	R	R/W	R
[@Remote Service]	R	R/W	R	R	R/W	R
[Update Firmware]	R	R/W	R	R	–	–
[Change Firmware Structure]	R	R/W	R	R	–	–
[Password Policy]	R/W	–	–	–	–	–
[Settings by SNMPv1, v2]	R	R	R/W	R	R/W	R
[Security Setting for Access Violation]	–	R/W	–	–	–	–
[Password Entry Violation]	–	R/W	–	–	–	–
[Device Access Violation]	–	R/W	–	–	–	–

Copyright © 2020, 2021

Web Image Monitor: @Remote

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

Copyright © 2020, 2021

Web Image Monitor: Webpage

These settings are in [Configuration] in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

[Webpage]

Settings	User	Mach	N/W	File	Unset	Set
[Webpage Language]	R	R	R/W	R	R/W	R
[Web Image Monitor Auto Logout]	R	R	R/W	R	R/W	R
[Personal Information Concealment]	R	R	R/W	R	R/W	R
[Set URL Target of Link Page]	R	R	R/W	R	R/W	R
[Set Help URL Target]	R	R	R/W	R	R/W	R
[WSD/UPnP Setting]	R	R	R/W	R	R/W	R
[Download Help File]	R/W	R/W	R/W	R/W	R/W	R/W

Copyright © 2020, 2021

Web Image Monitor: Extended Feature Settings

These settings are in [Configuration] in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Startup Setting]	–	R/W	–	–	–	–
[Extended Feature Info]	R	R	R	R	R	R
[Install]	–	R/W	–	–	–	–
[Uninstall]	–	R/W	–	–	–	–
[Administrator Tools]	–	R/W	–	–	–	–
[Additional Program Startup Setting]	–	R/W	–	–	–	–
[Install Additional Program]	–	R/W	–	–	–	–
[Uninstall Additional Program]	–	R/W	–	–	–	–
[Copy Extended Features]	–	R/W	–	–	–	–
[Copy Card Save Data]	–	R/W	–	–	–	–

Copyright © 2020, 2021

Web Image Monitor: Address Book

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the [Available Settings] setting.

Settings	User	Mach	N/W	File	Unset	Set
[Add User]	R/W	–	–	–	R/W *1	R/W *1
[Change]	R/W	–	–	–	R/W *1	R/W *1
[Delete]	R/W	–	–	–	R/W *1	R/W *1
[Add Group]	R/W	–	–	–	R/W *1	R/W *1
[Data Carry-over Setting for Address Book Auto-program]	R/W	–	–	–	R/W	R
[Maintenance]	R/W	–	–	–	–	–
[Central Management]	R/W	–	–	–	–	–

*1 If you set the machine as follows, each user can only change the password for his or her account when basic authentication is set.

- Settings screen type: Standard

  [Security] ▶ [Extended Security Settings] ▶ [Restrict Adding of User Destinations (Fax)] or [Restrict Adding of User Destinations (Scanner)] ▶ [On]

- Settings screen type: Classic

  [Extended Security] ▶ [Restrict Adding of User Destinations (Fax)] or [Restrict Adding of User Destinations (Scanner)] ▶ [On]

>Web Image Monitor: Central Management

Web Image Monitor: Central Management

These settings are in [Device Management].

This does not appear if you have user administrator privilege. In this case, specify it by accessing [Device Management] > [Address Book].

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

Copyright © 2020, 2021

Web Image Monitor: Main Power Off

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

Copyright © 2020, 2021

Web Image Monitor: Reset Printer Job

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
All items	–	R/W	–	–	–	–

Copyright © 2020, 2021

>Web Image Monitor: Reset the Machine

Web Image Monitor: Reset the Machine

These settings are in [Device Management].

When administrator authentication is set, the restrictions to user operations differ depending on the configuration in [Available Settings].

Settings	User	Mach	N/W	File	Unset	Set
[Reset the Machine]	–	R/W	–	–	R/W	–

Copyright © 2020, 2021

Web Image Monitor: Screen Monitoring

These settings are in [Device Management].

Settings	User	Mach	N/W	File	Unset	Set
[Display Device's Screen]	–	R/W	–	–	–	–

Copyright © 2020, 2021

>Web Image Monitor: Document Server

Web Image Monitor: Document Server

These settings are in [Print Job/Stored File].

What users can do with stored files depends on their access privileges. For details, see List of Operation Privileges for Stored Files.

Settings	User	Mach	N/W	File	Unset	Set
[New Folder]	–	–	–	R/W	R/W	R/W
[Edit Folder]	–	–	–	R/W	R/W	R/W
[Delete Folder]	–	–	–	R/W	R/W	R/W
[Unlock Folder]	–	–	–	R/W	–	–
[Print]	–	–	–	–	R/W	R/W
[Send]	–	–	–	–	R/W	R/W
[Delete]	–	–	–	R/W	R/W	R/W
[🔲 Edit detailed information]	–	–	–	R/W	R/W	R/W
[Download]	–	–	–	–	R/W	R/W
[Unlock File]	–	–	–	R/W	–	–

Copyright © 2020, 2021

>Web Image Monitor: Fax Received File

Web Image Monitor: Fax Received File

These settings are in [Print Job/Stored File].

Settings	User	Mach	N/W	File	Unset	Set
All items	–	–	–	–	R/W *1	R/W *1

*1 Only specified users can print, delete, or download documents when the machine is configured with [Fax Settings]→[Reception Settings]→[Stored Reception File User Setting] set to [On].

Copyright © 2020, 2021

Web Image Monitor: Printer: Print Jobs

These settings are in [Print Job/Stored File].

The printer documents users can manage are those users stored themselves or when user authentication is disabled.

The printer documents stored by other users are not displayed.

Settings	User	Mach	N/W	File	Unset	Set
[Print]	–	–	–	–	R/W *1	R/W *1
[Delete]	–	–	–	R/W	R/W *1	R/W *1
[🗒 Edit detailed information]	–	–	–	R/W	R/W *1	R/W *1
[Unlock Job]	–	–	–	R/W	–	–

*1 Access to saved documents may be restricted, depending on the user's access privileges.

Copyright © 2020, 2021

List of Operation Privileges for Stored Files

Understanding headers

- Read

  Users assigned with read privileges.

- Edit

  Users assigned with editing privileges.

- E/D

  Users assigned with edit/delete privileges.

- Full

  Users assigned with full control privileges.

- Owner

  Indicates either the user who registered a document or a user specified as the owner.

- File

  Indicates the file administrator.

Understanding the symbols

R/W: Can execute

–: Cannot execute

Settings	Read	Edit	E/D	Full	Owner	File
[To Printing Screen]	R/W	R/W	R/W	R/W	R/W	–
[Details]	R/W	R/W	R/W	R/W	R/W	R/W
[Preview]	R/W	R/W	R/W	R/W	R/W	–
[Change Access Priv.]: [Owner]	–	–	–	–	–	R/W
[Change Access Priv.]: [Permissions for Users/Groups]	–	–	–	R/W	R/W[*1]	R/W

[Change File Name]	–	R/W	R/W	R/W	R/W[*1]	–
[Change Password]	–	–	–	–	R/W	R/W
[Unlock Files]	–	–	–	–	–	R/W
[Delete File]	–	–	R/W	R/W	R/W[*1]	R/W
[Print Specified Page]	R/W	R/W	R/W	R/W	R/W[*1]	–

*1 The owner can change operation privileges.

List of Operation Privileges for Address Books

Understanding headers

- Read

  Users assigned with read privileges.

- Edit

  Users assigned with editing privileges.

- E/D

  Users assigned with edit/delete privileges.

- Full

  Users assigned with full control privileges.

- Entry

  Indicates a user whose personal information is registered in the Address Book. Also, it indicates any user who knows his or her user login name and password.

- User

  Indicates the user administrator.

Understanding the symbols

R/W: Executing, changing, and reading are possible.

R: Reading is possible.

–: Executing, changing, and reading are not possible.

[Name]

Settings	Read	Edit	E/D	Full	Entry	User
All items	R	R/W	R/W	R/W	R/W	R/W

[Destinations]

[Fax]

Settings	Read	Edit	E/D	Full	Entry	User
All items	R	R/W	R/W	R/W	R/W	R/W

[Email Address]

Settings	Read	Edit	E/D	Full	Entry	User
[Email Address]	R	R/W	R/W	R/W	R/W	R/W
[Use as Sender]	R	R/W	R/W	R/W	R/W	R/W
[Send via SMTP Server]	R	R/W	R/W	R/W	R/W	R/W
[SMTP Authentication Info]	–	–	–	–	R/W[*1]	R/W[*1]
[Use Email Address As]	R	R/W	R/W	R/W	R/W	R/W

*1 Passwords cannot be read.

[Folder]

Settings	Read	Edit	E/D	Full	Entry	User
All items	R	R/W[*2]	R/W[*2]	R/W[*2]	R/W[*2]	R/W[*2]

*2 The Login Password for [Folder Authentication Info] cannot be read.

[User Management / Others][User Management]

Settings	Read	Edit	E/D	Full	Entry	User
[Login User Name]	–	–	–	–	R	R/W

[Login Password]	–	–	–	–	R/W *1	R/W *1
[User Code]	–	–	–	–	–	R/W
[LDAP Authentication Info]	–	–	–	–	R/W *1	R/W *1
[Available Functions / Applications]	–	–	–	–	R	R/W
[Print Vol. Use Limitation]	–	–	–	–	R	R/W
[Access Privileges for Destination]	–	–	–	R/W	R/W	R/W
[Access Privileges for Stored Files]	–	–	–	R/W	R/W	R/W

*1 Passwords cannot be read.

[Registration Destination Group]

Settings	Read	Edit	E/D	Full	Entry	User
[Select Group]	R	R/W	R/W	R/W	R/W	R/W
[Delete]	–	–	–	R/W	R/W	R/W

[Display Priority]

Settings	Read	Edit	E/D	Full	Entry	User
[Display Priority]	R	R/W	R/W	R/W	R/W	R/W

[Destination Protection]

Settings	Read	Edit	E/D	Full	Entry	User
[Protect]	–	R/W	R/W	R/W	R/W	R/W
[Protection Code]	–	–	–	R/W*3	R/W*3	R/W*3

*3 The code for [Protection Code] cannot be read.

↓ Note

- For the following items, when [Restrict Adding of User Destinations (Fax)] and/or [Restrict Adding of User Destinations (Scanner)] is set to [On], regardless of a user's operation privileges, only the user administrator can access the Address Book.

  - Settings screen type: Standard

    [Security] ▶ [Extended Security Settings]

  - Settings screen type: Classic

    [Extended Security]

Copyright © 2020, 2021