RICOH
imagine. change.

User Guide Security Reference

For RICOH IM C300/C300F/C400F/C400SRF series

Author: RICOH COMPANY, LTD.
Date: 2022.07
Part Number: D0C97304

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 (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.

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]

Top Page>Web Image Monitor: Address Book

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]

[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

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

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

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

[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

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

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	–	–	–	–

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

[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

[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

[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

[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

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

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.

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.).