


IPsec Setting Guide



Definitions of notes

We use the following icon throughout this user's guide:

 Note	Notes tell you how you should respond to a situation that may arise or give tips about how the operation works with other features.
---	---

Trademarks

The Brother logo is a registered trademark of Brother Industries, Ltd.

Any trade names and product names of companies appearing on Brother products, related documents and any other materials are all trademarks or registered trademarks of those respective companies.

©2012 Brother Industries, Ltd. All rights reserved.

Table of Contents

1	Introduction	1
	Overview.....	1
	Configuration using Web Based Management (web browser)	2
2	IPsec Settings	5
	Address Template.....	5
	Service Template.....	7
	IPsec Service Template.....	7
	Setup Service	8
	IPsec Template.....	12
A	Appendix A	20
	Service Templates	20
	Type/Code	22

1 Introduction

Overview

IPsec (Internet Protocol Security) is a security protocol that uses an optional Internet Protocol function to prevent manipulation and ensure the confidentiality of data transmitted as IP packets. IPsec encrypts data carried over the network, such as print data sent from computers to a printer. Because the data is encrypted at the network layer, applications that use a higher-level protocol use IPsec even if the user is not aware of its use.

IPsec supports the following functions:

■ IPsec transmissions

According to the IPsec setting conditions, the network-connected computer sends data to and receives data from the specified device using IPsec. When the devices start communicating using IPsec, keys are exchanged using IKE (Internet Key Exchange) first, and then the encrypted data is transmitted using the keys.

In addition, IPsec has two operation modes: the Transport mode and Tunnel mode. The Transport mode is used mainly for communication between devices and the Tunnel mode is used in environments such as a VPN (Virtual Private Network).



Note

- For IPsec transmissions, the following conditions are necessary:
 - A computer that can communicate using IPsec is connected to the network.
 - The printer or MFC is configured for IPsec communication.
 - The computer connected to the printer or MFC is configured for IPsec connections.
 - IPsec does not support broadcast or multicast communication.
-

■ IPsec settings

The settings that are necessary for connections using IPsec. These settings can be configured using Web Based Management. (See *Configuration using Web Based Management (web browser)* >> page 2.)



Note


To configure the IPsec settings, a computer that can operate the browser must be connected to the network.

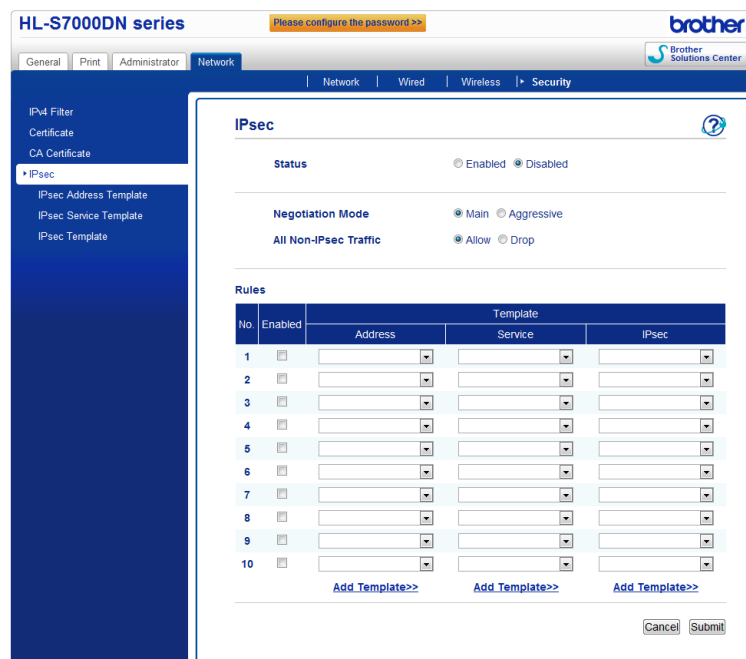
Configuration using Web Based Management (web browser)

1

Use the IPsec setting screen for Web Based Management to specify the IPsec connection conditions.

The IPsec connection conditions are comprised of three **Template** types: **Address**, **Service**, and **IPsec**, and a maximum of 10 connection conditions can be configured.

- 1 Start your web browser.
- 2 Type "http://machine's IP address/" into your browser (where "machine's IP address" is the machine's IP address).
 - For example:
http://192.168.1.2/
- 3 No password is required by default. Enter a password if you have set one and press .
- 4 Click the **Network** tab.
- 5 Click **Security**.
- 6 Click **IPsec**.
- 7 You can configure the IPsec settings from the screen below.



HL-S7000DN series Please configure the password >> brother

General | Print | Administrator | Network Brother Solutions Center

Network | Wired | Wireless | Security

IPsec

Status Enabled Disabled

Negotiation Mode Main Aggressive

All Non-IPsec Traffic Allow Drop

Rules

No.	Enabled	Template		
		Address	Service	IPsec
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Add Template>>](#) [Add Template>>](#) [Add Template>>](#)

- **Status**
Select **Enabled** or **Disabled** for IPsec.
- **Negotiation Mode**
Select the mode for IKE Phase 1.

- **Main:** The main mode is used.
- **Aggressive:** The aggressive mode is used.

**Note**

IKE is a protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec.

If the **Main** mode is selected, the processing speed is slow, but the security is high. If the **Aggressive** mode is selected, the processing speed is faster than when the **Main** mode is selected, but the security is lower.

■ All Non-IPsec Traffic

Select the action to be taken for non-IPsec packets.

- **Allow:** All packets are allowed to be received.
- **Drop:** Non-IPsec packets are discarded.

**Note**

When using Web Services, you must select **Allow** for **All Non-IPsec Traffic**. If **Drop** is selected, Web Services cannot be used.

■ Rules

A maximum of 10 IPsec connection conditions (template set) can be configured.

■ Enabled

When this check box is selected, the template set for that number is enabled.

**Note**

When multiple check boxes are selected, the check boxes with the lower numbers are given priority if the settings for the selected check boxes conflict.

■ Template - Address

Select the **Address Template** that is used for the IPsec connection conditions.

To add an **Address Template**, click **Add Template**. (See *Address Template* >> page 5.)

■ Template - Service

Select the **Service Template** that is used for the IPsec connection conditions.

To add a **Service Template**, click **Add Template**. (See *Service Template* >> page 7.)

**Note**

If you want to use DNS for the name resolution when using service templates 2, 3, and 4 in *Appendix A*, the DNS settings must be configured separately.

■ Template - IPsec

Select the **IPsec Template** that is used for the IPsec connection conditions.

To add an **IPsec Template**, click **Add Template**. (See *IPsec Template* >> page 12.)

■ **Submit**

Click this button to register the settings. If the computer must be restarted to change the settings, the restart confirmation screen will be displayed when this button is clicked.



Note


If you select the **Enabled** check box and click **Submit**, an error will occur if there is a blank item for the selected template.

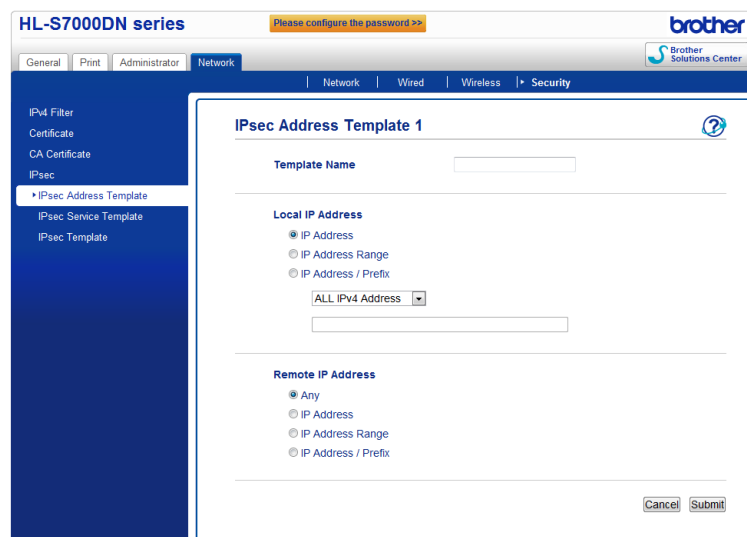
2

IPsec Settings

Address Template

Specify the IP addresses that will be used for the IPsec connection conditions. A maximum of 10 **Address Template** can be used.

- 1 Start your web browser.
- 2 Type “http://machine’s IP address/” into your browser (where “machine’s IP address” is the machine’s IP address).
 - For example:
http://192.168.1.2/
- 3 No password is required by default. Enter a password if you have set one and press .
- 4 Click the **Network** tab.
- 5 Click **Security**.
- 6 Click **IPsec Address Template**.
10 **Address Template** will be displayed. If the **Address Template** has not been configured, **Not Configured** will be displayed.
 - **Delete**
Click this button to delete the selected **Address Template**. However, the currently used **Address Template** cannot be deleted.
- 7 Click the number for the **Address Template** that you want to create. Specify the IP address that you want to use IPsec in the screen below, and create the **IPsec Address Template**.



The screenshot shows the Brother HL-S7000DN series web interface. The top navigation bar includes 'General', 'Print', 'Administrator', and 'Network'. The 'Network' tab is selected, and the 'Security' sub-tab is active. The left sidebar lists various settings, with 'IPsec Address Template' selected. The main content area is titled 'IPsec Address Template 1' and contains the following fields:

- Template Name:** A text input field.
- Local IP Address:** Radio buttons for 'IP Address', 'IP Address Range', and 'IP Address / Prefix'. A dropdown menu is set to 'ALL IPv4 Address' with an associated text input field.
- Remote IP Address:** Radio buttons for 'Any', 'IP Address', 'IP Address Range', and 'IP Address / Prefix'.
- Buttons for 'Cancel' and 'Submit' at the bottom right.

■ Template Name

Enter a name for the template in this box. (Maximum of 16 characters)

■ Local IP Address

Specify the IP address conditions for the sender.

• IP Address

Specify the IP address. Select **ALL IPv4 Address**, **ALL IPv6 Address**, **All Link Local IPv6**, or **Custom**.

If **Custom** is selected, enter the specified IP address (IPv4 or IPv6) in the text box.

• IP Address Range

Enter the starting and ending IP addresses for the IP address range. If the starting and ending IP addresses are not standardized to IPv4 or IPv6, or the ending IP address is smaller than the starting address, an error will occur.

• IP Address / Prefix

Specify the IP address using a prefix.

For example: 192.168.1.1/24

Because the prefix is specified in the form of a 24-bit subnet mask (255.255.255.0) for 192.168.1.1, the addresses 192.168.1.xx are valid.

■ Remote IP Address

Specify the IP address conditions for the recipient.

• Any

When **Any** is selected, all IP addresses are enabled.

• IP Address

Enter the specified IP address (IPv4 or IPv6) in the text box.

• IP Address Range

Enter the starting and ending IP addresses for the IP address range. If the starting and ending IP addresses are not standardized to IPv4 or IPv6, or the ending IP address is smaller than the starting address, an error will occur.

• IP Address / Prefix

Specify the IP address using a prefix.

For example: 192.168.1.1/24

Because the prefix is specified in the form of a 24-bit subnet mask (255.255.255.0) for 192.168.1.1, the addresses 192.168.1.xx are valid.

■ Submit

Click this button to register the settings.

**Note**


When you change the settings of the currently used template, the IPsec setting screen for Web Based Management will close and open again.

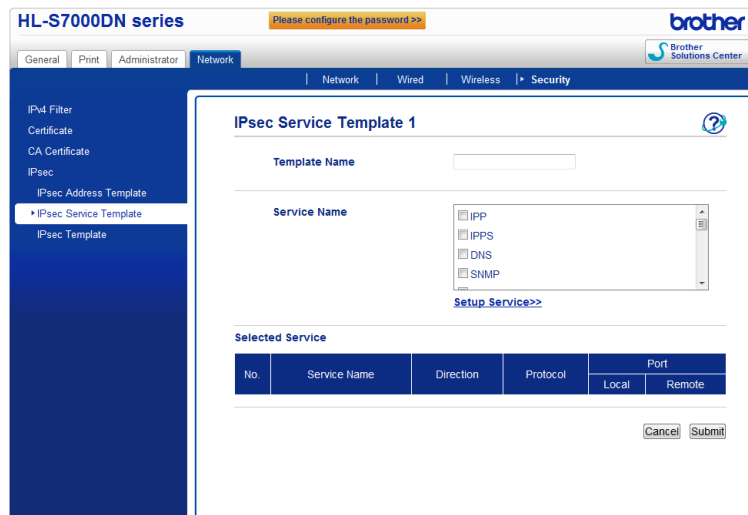
Service Template

IPsec Service Template

2

Specify the protocol and the port number to use for IPsec connections. A maximum of 10 **Service Template** can be used.

- 1 Start your web browser.
- 2 Type "http://machine's IP address/" into your browser (where "machine's IP address" is the machine's IP address).
 - For example:
http://192.168.1.2/
- 3 No password is required by default. Enter a password if you have set one and press .
- 4 Click the **Network** tab.
- 5 Click **Security**.
- 6 Click **IPsec Service Template**.
10 **Service Template** will be displayed. If the **Service Template** has not been configured, **Not Configured** will be displayed.
 - **Delete**
Click this button to delete the selected **Service Template**. However, the currently used **Service Template** cannot be deleted.
- 7 Click the number for the **Service Template** that you want to create. Select the services that you want to use for IPsec in the screen below, and create the **IPsec Service Template**.
In addition, if you want to create original services, click **Setup Service**. (See *Setup Service* >> page 8.)



HL-S7000DN series Please configure the password >> brother

General | Print | Administrator | Network | **Network** | Wired | Wireless | Security

IPv4 Filter
Certificate
CA Certificate
IPsec
IPsec Address Template
IPsec Service Template
IPsec Template

IPsec Service Template 1

Template Name

Service Name

- IPP
- IPPS
- DNS
- SNMP

[Setup Service>>](#)

Selected Service

No.	Service Name	Direction	Protocol	Port	
				Local	Remote

■ Template Name

Enter a name for the template in this box. (Maximum of 16 characters)

■ Service Name

The default service names and previously created service names are displayed. Select the services that you want to add to the template.

■ Setup Service

Click **Setup Service** to configure the template by adding services. (See *Setup Service* >> page 8.)

■ Selected Service

The service information (**Service Name**, **Direction**, **Protocol**, and **Port**) selected for **Service Name** is displayed.

**Note**

- A maximum of 32 services can be added at one time.
- For details about the protocols that you can specify in **IPsec Service Template**, see *Appendix A*.

■ Submit

Click this button to register the settings.

**Note**

When you change the settings of the currently used template, the IPsec setting screen for Web Based Management will close and open again.

Setup Service

Create a new service.

1

In the **IPsec Service Template** screen, click **Setup Service**.

60 **Service Name** will be displayed. If the **Service Name** has not been configured, **Not Configured** will be displayed.

■ Delete

Click this button to delete the selected **Service Name**. However, the currently used **Service Name** cannot be deleted.

■ IPsec Service Template

Click this button to return to the **IPsec Service Template** screen.

- Click the number for the **Service Name** that you want to create. Select the services that you want to use for IPsec in the screen below. The setting items are different depending on the selected **Protocol**.

(Protocol:ALL)

The screenshot shows the Brother HL-S7000DN series web interface. The left sidebar contains a navigation menu with the following items: IPv4 Filter, Certificate, CA Certificate, IPsec, IPsec Address Template, IPsec Service Template (highlighted), and IPsec Template. The main content area is titled 'Setup Service 1' and includes the following fields:

- Service Name:** An empty text input field.
- Direction:** Radio buttons for Initiator, Responder, and Both. The 'Both' option is selected.
- Protocol:** A dropdown menu set to 'ALL'.
- Buttons:** 'Setup Service>>', 'Cancel', and 'Submit'.

(Protocol:TCP or UDP)

The screenshot shows the Brother HL-S7000DN series web interface. The left sidebar contains the same navigation menu as the previous screenshot. The main content area is titled 'Setup Service 1' and includes the following fields:

- Service Name:** An empty text input field.
- Direction:** Radio buttons for Initiator, Responder, and Both. The 'Both' option is selected.
- Protocol:** A dropdown menu set to 'TCP'.
- Local Port:** Radio buttons for Single and Range. The 'Range' option is selected, with a value of '1' in the input field and '65535' in the adjacent field.
- Remote Port:** Radio buttons for Single and Range. The 'Range' option is selected, with a value of '1' in the input field and '65535' in the adjacent field.
- Buttons:** 'Setup Service>>', 'Cancel', and 'Submit'.

(Protocol: ICMP)

The screenshot shows the 'Setup Service 1' configuration page for ICMP. The page is titled 'Setup Service 1' and includes a 'Service Name' field. The 'Direction' section has radio buttons for 'Initiator', 'Responder', and 'Both', with 'Both' selected. The 'Protocol' is set to 'ICMP'. Under 'ICMP(Local)', there is a checkbox for 'Any' and input fields for 'Type' and 'Code', both set to '0'. Similarly, under 'ICMP(Remote)', there is a checkbox for 'Any' and input fields for 'Type' and 'Code', both set to '0'. At the bottom, there is a 'Setup Service>>' button and 'Cancel' and 'Submit' buttons.

■ **Service Name**

Enter a name for the service in this box. (Maximum of 16 characters)

■ **Direction**

Specify the communication direction. Select **Initiator**, **Responder**, or **Both**.

■ **Protocol**

Specify the protocol that is enabled. Select **ALL**, **TCP**, **UDP**, or **ICMP**. The setting items are different depending on the selected **Protocol**.

- When **TCP** or **UDP** is selected, register the **Local Port/Remote Port**.
- When **ICMP** is selected, register the **Type/Code**.



Note

ICMP is a protocol that is used to send IP error messages and control messages. This protocol is used by computers and network devices connected using TCP/IP in order to carry out mutual status confirmation.

■ **Local Port/Remote Port** (When **TCP** or **UDP** is selected in **Protocol**.)

Enter the local port number. If **Single** is selected, enter one port number. If **Range** is selected, enter the starting port number, and then enter the ending port number. When you want to enable all port numbers, select **Range** and enter "1-65535" without the double quotation marks.

■ **ICMP(Local)/ICMP(Remote)** (When **ICMP** is selected in **Protocol**.)

Configure the ICMP settings. Select **Any** or enter the **Type/Code**. For details about the **Type/Code**, see *Appendix A*.

■ **Setup Service**

Click this button to return to the **Setup Service** screen.

■ **Submit**

Click this button to register the settings.




Note

When you change the settings of the currently used template, the IPsec setting screen for Web Based Management will close and open again.

IPsec Template

Configure the IKE/IPsec settings. A maximum of 10 **IPsec Template** can be used.

- 1 Start your web browser.
- 2 Type “http://machine’s IP address/” into your browser (where “machine’s IP address” is the machine’s IP address).
 - For example:
http://192.168.1.2/
- 3 No password is required by default. Enter a password if you have set one and press .
- 4 Click the **Network** tab.
- 5 Click **Security**.
- 6 Click **IPsec Template**.
10 **IPsec Template** will be displayed. If the **IPsec Template** has not been configured, **Not Configured** will be displayed.
 - **Delete**
Click this button to delete the selected **IPsec Template**. However, the currently used **IPsec Template** cannot be deleted.

- Click the number for the **IPsec Template** that you want to create. Configure the IPsec settings in the screen below, and create the **IPsec Template**. The setting items are different depending on the selected **Use Prefixed Template** and **Internet Key Exchange (IKE)**.

(IKE: Preset)

The screenshot shows the configuration page for 'IPsec Template 1' on a Brother HL-S7000DN series device. The interface includes a top navigation bar with 'General', 'Print', 'Administrator', and 'Network' tabs. The 'Security' section is active, showing options for 'Network', 'Wired', 'Wireless', and 'Security'. A left sidebar lists various security settings, with 'IPsec Template' selected. The main configuration area is titled 'IPsec Template 1' and contains the following settings:

- Template Name:** [Empty text field]
- Use Prefixed Template:** IKEV1 High Security (dropdown menu)
- Internet Key Exchange (IKE):** IKEV1 (radio button selected)
- Authentication Type:**
 - Diffie-Hellman Group: Group5, Group14
 - Encryption: AES-CBC 128, AES-CBC 256
 - Hash: SHA1, SHA256, SHA512
 - SA Lifetime: 26800 second(s) (240 – 63072000), 32768 KByte (10 – 2097152)
- Encapsulating Security:**
 - Protocol: ESP
 - Encryption: AES-CBC 128, AES-CBC 256

(IKE: IKEv1)

The screenshot shows the configuration page for 'IPsec Template 1' on a Brother HL-S7000DN series device, similar to the previous one but with different settings. The interface and navigation are identical. The main configuration area is titled 'IPsec Template 1' and contains the following settings:

- Template Name:** [Empty text field]
- Use Prefixed Template:** Custom (dropdown menu)
- Internet Key Exchange (IKE):** IKEV1 (radio button selected), IKEV2, Manual
- Authentication Type:**
 - Diffie-Hellman Group: Group1 (dropdown menu)
 - Encryption: DES (dropdown menu)
 - Hash: MD5 (dropdown menu)
 - SA Lifetime: 86600 second(s) (240 – 63072000), 32768 KByte (10 – 2097152)
- Encapsulating Security:**
 - Protocol: ESP (radio button selected), AH
 - Encryption: DES (dropdown menu)
 - Hash: MD5 (dropdown menu)
 - SA Lifetime: 43200 second(s)

(IKE:IKEv2)

■ Template Name

Enter a name for the template in this box. (Maximum of 16 characters)

■ Use Prefixed Template

Select **Custom**, **IKEv1 High Security**, **IKEv1 Medium Security**, **IKEv2 High Security**, or **IKEv2 Medium Security**. The setting items are different depending on the selected template.



Note

The default template differs depending on whether you chose Main or Aggressive in Negotiation Mode on the IPsec setting screen. For details about the IPsec setting screen, see *Configuration using Web Based Management (web browser)* >> page 2.

■ Internet Key Exchange (IKE)

IKE is a communication protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec. In order to carry out encrypted communication for that time only, the encryption algorithm that is necessary for IPsec is determined and the encryption keys are shared. For IKE, the encryption keys are exchanged using the Diffie-Hellman key exchange method, and encrypted communication that is limited to IKE is carried out.

If **Custom** is selected in **Use Prefixed Template**, select **IKEv1**, **IKEv2**, or **Manual**.

If a setting other than **Custom** is selected, the authentication type selected in **Use Prefixed Template** will be displayed.

■ Authentication Type

Configures the IKE authentication and encryption.

- **Diffie-Hellman Group**

This key exchange method allows secret keys to be securely exchanged over an unprotected network. The Diffie-Hellman key exchange method uses a discrete logarithm problem, not the secret key, to send and receive open information that was generated using a random number and the secret key.

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **IKEv2** is selected in **IKE**) Select **Group1**, **Group2**, **Group5**, or **Group14**. If **IKEv2** is selected, multiple selections are possible.

(If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**) The group will not be displayed.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled group will be displayed.

- **Encryption**

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **IKEv2** is selected in **IKE**) Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**. If **IKEv2** is selected, multiple selections are possible.

(If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**) The encryption will not be displayed.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled encryption will be displayed.

- **Hash**

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **IKEv2** is selected in **IKE**) Select **MD5**, **SHA1**, **SHA256**, or **SHA512**. If **IKEv2** is selected, multiple selections are possible.

(If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**) The hash algorithm type will not be displayed.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled hash algorithm type will be displayed.

- **SA Lifetime**

Specify the IKE SA lifetime.

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **IKEv2** is selected in **IKE**) Enter the time (seconds) and number of kilobytes (KByte).

(If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**) The SA Lifetime information will not be displayed.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The time (seconds) and number of kilobytes (KByte) will be displayed.

- **Encapsulating Security**

- **Protocol**

(If **Custom** is selected in **Use Prefixed Template**) Select **ESP** or **AH**. If **IKEv2** is selected in **IKE**, only **ESP** can be selected.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled protocol will be displayed.

**Note**

- ESP is a protocol for carrying out encrypted communication using IPsec. ESP encrypts the payload (communicated contents) and adds additional information. The IP packet is comprised of the header and the encrypted payload, which follows the header. In addition to the encrypted data, the IP packet also includes information regarding the encryption method and encryption key, the authentication data, and so on.
- AH is part of the IPsec protocol that authenticates the sender and prevents manipulation of the data (ensures the completeness of the data). In the IP packet, the data is inserted immediately after the header. In addition, the packets include hash values, which are calculated using an equation from the communicated contents, secret key, and so on, in order to prevent the falsification of the sender and manipulation of the data. Unlike ESP, the communicated contents are not encrypted, and the data is sent and received as plain text.

- **Encryption**

(If **Custom** is selected in **Use Prefixed Template**) Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**. The encryption can be selected only when **ESP** is selected in **Protocol**. If **IKEv2** is selected in **IKE**, multiple selections are possible.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled encryption will be displayed.

- **Hash**

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **Manual** is selected in **IKE**) Select **None**, **MD5**, **SHA1**, **SHA256**, or **SHA512**. **None** can be selected only when **ESP** is selected in **Protocol**.

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv2** is selected in **IKE**) Select **MD5**, **SHA1**, **SHA256**, or **SHA512**. Multiple selections are possible.

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The above-mentioned enabled hash algorithm type will be displayed.

- **SA Lifetime**

Specify the IKE SA lifetime.

(If **Custom** is selected in **Use Prefixed Template**, and **IKEv1** or **IKEv2** is selected in **IKE**) Enter the time (seconds) and number of kilobytes (KByte).

(If a setting other than **Custom** is selected in **Use Prefixed Template**) The time (seconds) and number of kilobytes (KByte) will be displayed.

- **Encapsulation Mode**

Select **Transport** or **Tunnel**.

- **Remote Router IP-Address**

Specify the IP address (IPv4 or IPv6) of the connection destination. Enter only when the **Tunnel** mode is selected.

**Note**

SA (Security Association) is an encrypted communication method using IPsec or IPv6 that exchanges and shares information, such as the encryption method and encryption key, in order to establish a secure

communication channel before communication begins. SA may also refer to a virtual encrypted communication channel that has been established. The SA used for IPsec establishes the encryption method, exchanges the keys, and carries out mutual authentication according to the IKE (Internet Key Exchange) standard procedure. In addition, the SA is updated periodically.

■ Perfect Forward Secrecy (PFS)

PFS does not derive keys from previous keys, which were used to encrypt messages. In addition, if a key that is used to encrypt a message was derived from a parent key, that parent key is not used to derive other keys. Therefore, even if a key is compromised, the damage will be limited only to the messages that were encrypted using that key.

Select **Enabled** or **Disabled**. If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**, the PFS information will not be displayed.

■ Authentication Method

Select the authentication method. Select **Pre-Shared Key**, **Certificates**, **EAP - MD5**, or **EAP - MS-CHAPv2**.

EAP - MD5 and **EAP - MS-CHAPv2** can be selected only when **IKEv2** is selected in **IKE**. If **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**, the authentication method information will not be displayed.

■ Pre-Shared Key

When encrypting communication, the encryption key is exchanged and shared beforehand using another channel.

If **Pre-Shared Key** is selected in **Authentication Method**, enter the **Pre-Shared Key**. (Maximum of 32 characters)

• Local ID Type/ID

Select the ID type of the sender, and enter the ID.

Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.

If **Certificate** is selected, enter the common name of the certificate in **ID**.

• Remote ID Type/ID

Select the ID type of the recipient, and enter the ID.

Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.

If **Certificate** is selected, enter the common name of the certificate in **ID**.

■ Certificates

If **Certificates** is selected in **Authentication Method**, select the certificate.



Note

You can select only the certificates that were created using the **Certificate** page of the Web Based Management Security features. For details, see Network User's Guide: Using Certificates for device security.

■ EAP

EAP is an authentication protocol that is an extension of PPP. By using EAP together with IEEE802.1x, a different key is used for user authentication and each session.

The following settings are necessary only when **EAP - MD5** or **EAP - MS-CHAPv2** is selected in **Authentication Method**.

- **Mode**

Select **Server-Mode** or **Client-Mode**.

- **Certificate**

Select the certificate.

- **User Name**

Enter the user name. (Maximum of 32 characters)

- **Password**

Enter the password. The password must be entered two times for confirmation. (Maximum of 32 characters)

- **Certificate>>**

Click this button to move to the certificate setting screen.

(IKE:Manual)

The screenshot displays the 'IPsec Template 1' configuration interface. The left sidebar contains navigation options: IPv4 Filter, Certificate, CA Certificate, IPsec, IPsec Address Template, IPsec Service Template, and IPsec Template (selected). The main content area is titled 'IPsec Template 1' and includes the following fields:

- Template Name:** An empty text input field.
- Use Prefixed Template:** A dropdown menu set to 'Custom'.
- Internet Key Exchange (IKE):** Radio buttons for IKEV1, IKEV2, and Manual (selected).
- Authentication Key (ESP, AH):** Two pairs of text input fields labeled 'In' and 'Out'.
- Code key (ESP):** Two pairs of text input fields labeled 'In' and 'Out'.
- SPI:** Two text input fields labeled 'In' (value: 256) and 'Out' (value: 256).
- Encapsulating Security:**
 - Protocol:** Radio buttons for ESP (selected) and AH.
 - Encryption:** A dropdown menu set to 'DES'.
 - Hash:** A dropdown menu set to 'MD5'.

■ Authentication Key (ESP,AH)

Specify the key to use for authentication. Enter the **In/Out** values.

These settings are necessary when **Custom** is selected in **Use Prefixed Template**, **Manual** is selected in **IKE**, and a setting other than **None** is selected in **Hash** in **Encapsulating Security**.

**Note**

The number of characters you can set differs depending on the setting you chose in Hash in Encapsulating Security.

If the length of the specified authentication key is different from the selected hash algorithm, an error will occur.

- **MD5**: 128 bits (16 bytes)
- **SHA1**: 160 bits (20 bytes)
- **SHA256**: 256 bits (32 bytes)
- **SHA512**: 512 bits (64 bytes)

When you specify the key in ASCII Code, enclose the characters in double quotation marks.

■ Code key (ESP)

Specify the key to use for encryption. Enter the **In/Out** values.

These settings are necessary when **Custom** is selected in **Use Prefixed Template**, **Manual** is selected in **IKE**, and **ESP** is selected in **Protocol** in **Encapsulating Security**.

**Note**

The number of characters you can set differs depending on the setting you chose in Encryption in Encapsulating Security.

If the length of the specified code key is different from the selected encryption algorithm, an error will occur.

- **DES**: 64 bits (8 bytes)
- **3DES**: 192 bits (24 bytes)
- **AES-CBC 128**: 128 bits (16 bytes)
- **AES-CBC 256**: 256 bits (32 bytes)

When you specify the key in ASCII Code, enclose the characters in double quotation marks.

■ SPI

These parameters are used to identify the security information. Generally, a host has multiple SAs (Security Associations) for several types of IPsec communication. Therefore, it is necessary to identify the applicable SA when an IPsec packet is received. The SPI parameter, which identifies the SA, is included in the AH (Authentication Header) and ESP (Encapsulating Security Payload) header.

These settings are necessary when **Custom** is selected in **Use Prefixed Template**, and **Manual** is selected in **IKE**.

Enter the **In/Out** values. (3-10 characters)

■ Submit

Click this button to register the settings.

**Note**

When you change the settings of the currently used template, the IPsec setting screen for Web Based Management will close and open again.

Service Templates

You can use the following services by selecting the templates.

1 All Services

IPsec is used for all protocols.

2 Print Services

Service Name	Protocol	Local Port	Remote Port
IPP	TCP	631	Any
IPPS	TCP	443	Any
FTP (Control)	TCP	21	Any
FTP (Data)	TCP	20	Any
P9100	TCP	9100	Any
Web Services	TCP	80	Any
LPD	TCP	515	Any

3 Management Services

Service Name	Protocol	Local Port	Remote Port
SNMP	UDP	161	Any
Telnet	TCP	23	Any
HTTP	TCP	80	Any
HTTPS	TCP	443	Any
Remote Setup	TCP	54922	Any

4 Printer/MFC Services ¹

Service Name	Protocol	Local Port	Remote Port
CIFS	TCP	Any	445
SMB	TCP	Any	139
LDAP	TCP	Any	389
SMTP	TCP	Any	25
POP3	TCP	Any	110
SNTP	UDP	Any	123
Network Scan	TCP	54921	Any
PC-FAX	TCP	54923	Any

Service Name	Protocol	Local Port	Remote Port
Kerberos (TCP)	TCP	Any	88
Kerberos (UDP)	UDP	Any	88

¹ If you want to use Kerberos authentication, you must enable the DNS settings accordingly.

Type/Code

The following types and codes are supported when **ICMP** is selected in **Protocol**.

IPv4		
Type		Supported Codes
0	Echo Reply	0
3	Destination Unreachable	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Source Quench	0
5	Redirect	0,1,2,3
8	Echo Request	0
9	Router Advertisement	0
10	Router Solicitations	0

IPv4 Code

0,1,2,3,4,5,6,7,8,9,10,11,12

IPv6		
Type		Supported Codes
1	Destination Unreachable	0,1,2,3,4
3	Time Exceeded	0,1
4	Parameter Problem	0,1,2
128	Echo Request	0
129	Echo Reply	0
133	Router Solicitation	0
134	Router Advertisement	0
135	Neighbor Solicitation	0
136	Neighbor Advertisement	0
137	Redirect	0

IPv6 Code

0,1,2,3,4

brother[®]

**Visit us on the World Wide Web
<http://www.brother.com/>**



www.brotherearth.com