Functions and Network Settings Available in an IPv6 Environment

The functions and network settings of this machine that are available in an IPv6 environment differ from those available in an IPv4 environment. Make sure the functions you require are supported in an IPv6 environment, and then configure the necessary network settings.

Available Functions

♦ **Print via FTP**

Prints documents via FTP using the EPRT and EPSV commands. Windows Vista/7 and an FTP application that supports IPv6 are required to use these commands.

♦ **Printer**

Prints documents on this machine using the printer driver.

♦ **Scan to FTP**

Delivers files that have been scanned using the control panel to an FTP server.

This function is only available on models that have a control panel display.

♦ **Scan to Email**

Sends files scanned using the control panel via e-mail.

This function is only available on models that have a control panel display.

♦ **Scan to Folder**

Sends files scanned using the control panel to a shared folder on a computer on the network.

This function is only available on models that have a control panel display.

This function is not available on Macintosh OS.

♦ **Network Twain Server**

Controls the scanning function from a computer on the network, and delivers scanned data to the computer directly. This function is available only to computers that have a TWAIN-supporting application. The IP address of the multi-cast group supported by IPv6 is ff12::fb88:1.

This function is only available on models that have a control panel display.

♦ **Bonjour**

Allows the machine to communicate with Bonjour protocol-supported computers on the network. The IP address of the multi-cast group supported by IPv6 is ff02::fb.

♦ **PC-FAX**

Sends a document created in an application as a fax and without printing it.

This function is only available on models that have a control panel display.

♦ **Web Image Monitor**

Allows you to check the machine's status and configure its settings using a Web browser.

♦ **Configuration Page**

Prints a configuration page that shows you the machine's configuration, IP address, and other details.

IPv6-Related Settings

This section explains the settings specific to IPv6 that can be configured on this machine. To use this machine in an IPv6 environment, specify each setting as necessary. If your model has a control panel display, you can use the control panel or Web Image Monitor to change the IPv6 settings. If your model does not have a control panel display, use Web Image Monitor or Smart Organizing Monitor to change the IPv6 settings.

Web Image Monitor

Configure the IPv6 settings under **[Network Settings]**.

[IPv6 Setup] tab

Setting	Description
IPv6	Select whether to enable or disable IPv6. This setting becomes effective after the machine has been restarted. If IPv6 is already set to **[Enable]**, it cannot be changed to **[Disable]**. Default: **[Enable]** • **Enable** • **Disable**
IPv6 DHCP	Select whether or not the machine obtains its IPv6 address from a DHCP server. To specify the machine's IPv6 address manually, select **[Disable]** and enter the machine's IP address in **[Manual Address]**. This setting becomes effective after the machine has been restarted. Default: **[Disable]** • **Enable** • **Disable**
Address from DHCP	The IPv6 address obtained from the DHCP server appears when **[IPv6 DHCP]** is set to **[Enable]**.
Stateless Auto Address	Displays up to four stateless auto addresses.
Default Gateway Address	Displays the machine's default gateway address.

Setting	Description
Link Local Address	Displays the link local address of the machine. The link local address is an address that is valid only inside the local network (local segment). It starts with "fe80::", followed by an identifier that is derived from the physical address of the currently active interface board.
Manual Address	Manually enter the machine's IPv6 address. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered. The default is blank. This setting becomes effective after the machine has been restarted.
Prefix Length	If you have selected **[Manual Address]**, you must enter a prefix length using a value between 1 and 128. If **[Manual Address]** is not entered (blank), this box will be automatically cleared. The default is blank. This setting becomes effective after the machine has been restarted.
Default Gateway Address	To specify the IP address of the default gateway manually, enter it here. The default gateway address is the IP address of the host or router used as the gateway when the machine is communicating with a computer on another network. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered. The default is blank. This setting becomes effective after the machine has been restarted.

[DNS] tab

Setting	Description
IPv6 DNS Method	Select whether to specify the domain server manually or have the machine obtain its DNS information automatically. Default: **[Auto]** • **Auto** • **Manual** **[Primary IPv6 DNS Server]**, **[Secondary IPv6 DNS Server]**, and **[IPv6 Domain Name]** can be set only when this setting is set to **[Manual]**. This setting becomes effective after the machine has been restarted.

Setting	Description
Primary IPv6 DNS Server	Enter the IPv6 address of the primary IPv6 DNS server. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered.
Secondary IPv6 DNS Server	Enter the IPv6 address of the secondary IPv6 DNS server. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered.
IPv6 Domain Name	Enter the domain name of the machine. Up to 32 characters can be entered.
DNS Resolve Priority	Select whether to give priority to IPv4 or IPv6 for DNS name resolution. Default: **[IPv4]** • **IPv4** • **IPv6**

For details about each setting, see Web Image Monitor Help.

Control Panel (models with a control panel display)

Configure the IPv6 settings under **[Network Settings]**.

[IPv6 Configuration] menu

Setting	Description
IPv6 Activated	Select whether to enable or disable IPv6. Default: **[On]** • **On** • **Off**
DHCPv6 Activated	Select whether to enable or disable DHCPv6. Default: **[Off]** • **On** • **Off**
Link local Address	Displays up to four link local address.
Stateless Address	Displays the stateless auto address.

Setting	Description
Manual Address	• **Manual Address** Manually enter the machine's IPv6 address. Up to 39 characters can be entered. • **Prefix Length** If you have selected **[Manual Address]**, you must enter a prefix length using a value between 1 and 128. • **Gateway** To specify the IP address of the default gateway manually, enter it here. The default gateway address is the IP address of the host or router used as the gateway when the machine is communicating with a computer on another network. Up to 39 characters can be entered. The default is blank. This setting becomes effective after the machine has been restarted.
DHCPv6 Address	Displays the IPv6 address obtained from the DHCP server.

[IPsec] menu

Setting	Description
IPsec Activated	Select whether to enable or disable IPsec. Default: **[Off]** • **On** • **Off** This function is available only when a password is specified under **[Admin Menu Lock]**.

Smart Organizing Monitor (models without a control panel display)

Configure the IPv6 settings on the **[IPv6]** tab of Printer Configuration.

Setting	Description
IPv6 DHCP	Select whether or not the machine obtains its IPv6 address from a DHCP server. This setting becomes effective after the machine has been restarted. Default: **[Disable]** • **Disable** • **Enable**
Address from DHCP	Displays the IPv6 address obtained from the DHCP server.
Stateless Auto Address	Displays the stateless auto address and the default gateway address.
Link local Address	Displays the link local address. The link local address is an address that is valid only inside the local network (local segment). It starts with "fe80::", followed by an identifier that is derived from the physical address of the currently active interface board.
IPv6 default router (Gateway)	Displays the default gateway address.
Manual address	Manually enter the machine's IPv6 address. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered. The default is blank. This setting becomes effective after the machine has been restarted.
Prefix length	If you have set **[IPv6 DHCP]** to **[Disable]**, you must enter a prefix length. If you have selected **[Manual address]**, you must enter a prefix length using a value between 1 and 128. The default is blank. This setting becomes effective after the machine has been restarted.
Gateway	Enter the default gateway address. The default gateway address is the IP address of the host or router used as the gateway when the machine is communicating with a computer on another network. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered. The default is blank. This setting becomes effective after the machine has been restarted.

Setting	Description
IPv6	Select whether to enable or disable IPv6. This setting becomes effective after the machine has been restarted. Default: **[Enable]** • **Disable** • **Enable** The following settings can be changed only when **[Enable]** is selected for this setting: **[IPv6 DHCP]**, **[Manual address**], **[Prefix length]**, and **[Gateway]**.
DNS method	Select whether to specify the domain server manually or have the machine obtain its DNS information automatically from the network. Default: **[Auto]** • **Manual** • **Auto** **[IPv6 Primary DNS Server]**, **[IPv6 Secondary DNS Server]**, and **[IPv6 Domain Name]** can not be set only when this setting is set to **[Manual]**. This setting becomes effective after the machine has been restarted.
IPv6 Primary DNS Server	This setting can be modified only when **[DNS method]** is set to **[Manual]**. Enter the IPv6 address of the primary IPv6 DNS server. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered.
IPv6 Secondary DNS Server	This setting can be modified only when **[DNS method]** is set to **[Manual]**. Enter the IPv6 address of the secondary IPv6 DNS server. Usable characters are 0-9, A-F, a-f, and: (0x3a). Up to 39 characters can be entered.
IPv6 Domain Name	This setting can be modified only when **[DNS method]** is set to **[Manual]**. Enter the domain name of this machine. Up to 32 characters can be entered.

For details about each setting item, see Smart Organizing Monitor Help.

Transmission Using IPsec

For securer communications, this machine supports the IPsec protocol. When applied, IPsec encrypts data packets at the network layer using shared key encryption. The machine uses encryption key exchange to create a shared key for both sender and receiver. To achieve even higher security, you can also renew the shared key on a validity period basis.

Important

- IPsec is not applied to data obtained through DHCP, DNS, or WINS.
- IPsec compatible operating systems are Windows XP SP2, Windows Vista/7, Windows Server 2003/2003 R2/2008/2008 R2, and Mac OS X 10.4.8 or later. However, some setting items are not supported depending on the operating system. Make sure the IPsec settings you specify are consistent with the operating system's IPsec settings.

Encryption and Authentication by IPsec

IPsec consists of two main functions: the encryption function, which ensures the confidentiality of data, and the authentication function, which verifies the sender of the data and the data's integrity. This machine's IPsec function supports two 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. 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. 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. 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. 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. The authentication algorithm and authentication key are specified automatically.

Note

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

Security Association

This machine uses encryption key exchange as the key setting method. With this method, agreements such as the IPsec algorithm and key must be specified for both sender and receiver. Such agreements form an "SA" (Security Association). IPsec communication is possible only if the receiver's and sender's SA settings are identical.

The SA settings are auto configured on both parties' machines. However, before the IPsec SA can be established, the ISAKMP SA (Phase 1) settings must be auto configured. When this is done, the IPsec SA (Phase 2) settings, which allow actual IPsec transmission, will be 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 exchange.

Multiple settings can be configured in the SA.

♦ **Settings 1-10**

You can configure ten separate sets of SA details (such as different shared keys and IPsec algorithms).

Policies are searched through one by one, starting at **[No.1]**.

IPsec Settings

The IPsec settings for this machine can be made through Web Image Monitor. The following table explains each setting.

Important

- This function is available only when an administrator password is specified.

[IPsec Global Settings] tab

Setting	Description
IPsec Function	Select whether to enable or disable IPsec. Default: **[Disable]** • **Enable** • **Disable**
Default Policy	Select the default IPsec policy. Default: **[Allow]** • **Allow** • **Drop**
Broadcast and Multicast Bypass	Select the services that you do not want to encrypt with IPsec. • **DHCPv4** • **DHCPv6** • **SNMP** • **mDNS** • **NetBIOS** • **UDP Port 53550** By default, none of the above listed services are IPsec-encrypted.
All ICMP Bypass	Select whether to enable or disable the bypass method for ICMP. Default: **[Disable]** • **Disable** Only certain types of ICMP traffic will be bypassed. • **Enable** All ICMP traffic (IPv4 and IPv6) will be bypassed. The response request sent by the "ping" command, and the corresponding response packets will not be encapsulated.

[IPsec Policy List] tab

Displays the list of the registered IP sec policies.

Select **[No.]** for any setting that you want to edit, and then click **[Edit]** to open the **[IPsec Policy Settings]** screen. The following settings can be made on the **[IPsec Policy Settings]** screen.

IP Policy Settings

Setting	Description
No.	Specify a number between 1 and 10 for the IPsec policy. The number you specify will determine the position of the policy in the IPsec Policy List. Policy searching is performed according to the order of the list. If the number you specify is already assigned to another policy, the policy you are configuring will take the number of the earlier policy, and the earlier policy and any subsequent policies will be renumbered accordingly.
Activity	Select whether to enable or disable the policy.
Name	Enter the name of the policy. Up to 16 characters can be entered.
Address Type	Select IPv4 or IPv6 as the type of IP address to be used in IPsec communication.
Local Address	You can specify the IP address of this machine.
Remote Address	Enter the IPv4 or IPv6 address of the device with which to communicate. Up to 39 characters can be entered.
Prefix Length	Enter the prefix length of the Remote Address, using a value between 1 and 128. If this setting is left blank, "32" (IPv4) or "128" (IPv6) will be automatically selected.
Action	Specify how the IP packets are processed. • **Allow** IP packets are both sent and received without IPsec applied to them. • **Drop** IP packets are discarded. • **Require Security** IPsec is applied to IP packets that are both sent and received. If you have selected **[Require Security]**, you must configure **[IPsec Settings]** and **[IKE Settings]**.

IPsec Settings

Setting	Description
Encapsulation Type	Specify the encapsulation type. • **Transport** Select this mode to secure only the payload section of each IP packet when communicating with IPsec compliant devices. • **Tunnel** Select this mode to secure every section of each IP packet. We recommend this type for communication between security gateways (such as VPN devices).
Security Protocol	Select the security protocol. • **AH** Establishes secure communication that supports authentication only. • **ESP** Establishes secure communication that supports both authentication and data encryption. • **ESP&AH** Establishes secure communication that supports both data encryption and authentication of packets, including packet headers. Note that you cannot specify this protocol when **[Tunnel]** is selected for **[Encapsulation Type]**.
Authentication Algorithm for AH	Specify the authentication algorithm to be applied when **[AH]** is selected for **[Security Protocol]**. • **MD5** • **SHA1**

Setting	Description
Encryption Algorithm for ESP	Specify the encryption algorithm to be applied when **[ESP]** is selected for **[Security Protocol]**. • **None** • **DES** • **3DES** • **AES-128** • **AES-192** • **AES-256**
Authentication Algorithm for ESP	Specify the authentication algorithm to be applied when **[ESP]** is selected for **[Security Protocol]**. • **MD5** • **SHA1**
Life Time	Specify the life time of the IPsec SA (Security Association) as a time period or data volume. The SA will expire when the time period you specify elapses or the volume of data carried reaches the volume you specify. If you specify both a time period and a data volume, the SA will expire as soon as either is reached, and a new SA will then be obtained by negotiation. To specify the life time of the SA as a time period, enter a number of seconds. To specify the life time of the SA as a data volume, enter a number of KBs.
Key Perfect Forward Secrecy	Select whether to enable or disable PFS (Perfect Forward Secrecy). • **Enable** • **Disable**

IKE Settings

Setting	Description
IKE Version	Displays the IKE version.
Encryption Algorithm	Specify the encryption algorithm. • **DES** • **3DES** • **AES-128** • **AES-192** • **AES-256**
Hash Algorithm	Specify the hash algorithm. • **MD5** • **SHA1**
IKE Life Time	Specify the life time of the ISAKMP SA as a time period. Enter a number of seconds.
IKE Diffie-Hellman Group	Select the IKE Diffie-Hellman Group to be used in the generation of the IKE encryption key. • **DH1** • **DH2**
Pre-Shared Key	Specify the PSK (Pre-Shared Key) to be used for authentication of a communicating device. Up to 32 characters can be entered.
Key Perfect Forward Secrecy	Select whether to enable or disable PFS (Perfect Forward Secrecy). • **Enable** • **Disable**

For details about each setting item, see Web Image Monitor Help.

Encryption Key Exchange Settings Configuration Flow

This section explains the procedure for specifying encryption key exchange settings.

Machine	PC
1. Set the IPsec Settings on Web Image Monitor	1. Set the same Items as on the machine
2. Activate IPsec settings	2. Activate IPsec Settings
3. Confirm IPsec Transmission	

Note

- After configuring IPsec, you can use "ping" command to check if the connection is established correctly. Also, because the response is slow during initial key exchange, it may take some time to confirm that transmission has been established.
- If communication with the machine becomes impossible after enabling IPsec, disable IPsec and then reconfigure the settings.

Reference

- P20."Deactivating IPsec"

Specifying Encryption Key Exchange Settings

1. **Access Web Image Monitor, and then click [IPsec Policy List] on the [IPsec Settings] page.**
2. **Select the number of the setting you want to modify in the list, and then click [Edit].**
3. **Modify the IPsec related settings as necessary.**
4. **Enter the administrator password, and then click [Submit].**
5. **Click the [IPsec Global Settings] tab, and then select [Enable] in [IPsec Function].**
6. **If necessary, select [Default Policy] and [Broadcast and Multicast Bypass] also.**
7. **Enter the administrator password, and then click [Submit].**

Specifying IPsec Settings on the Computer

Specify exactly the same settings for IPsec SA settings on your computer as are specified for the IPsec Settings on the machine. Setting methods differ according to the computer's operating system. The example procedure shown here uses Windows XP under IPv4 environment.

1. **On the [Start] menu, click [Control Panel], [Performance and Maintenance], and then click [Administrative Tools].**
2. **Double-click [Local Security Policy].**
3. **Click [IP Security Policies on Local Computer].**
4. **In the "Action" menu, click [Create IP Security Policy].**
   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 [Advanced].**
10. **In "Authenticate and generate a new key after every", enter the same validity period (in minutes) that is specified on the machine in [IKE Life Time], and then click [Methods].**
11. **Confirm that the Encryption Algorithm ("Encryption"), Hash Algorithm ("Integrity"), and IKE Diffie-Hellman Group ("Diffie-Hellman Group") settings in "Security method preference order" all match those specified on the machine in [IKE Settings].**
    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. **Select "Use this string to protect the key exchange (preshared key)", and then enter the same PSK text specified on the machine with the pre-shared key.**
18. **Click [Next].**
19. **Click [Add] in the IP Filter List.**

20. **In [Name], enter an IP Filter name, and then click [Add].**
    The IP Filter Wizard appears.
21. **Click [Next].**
22. **Select "My IP Address" in "Source address", and then click [Next].**
23. **Select "A specific IP Address" in "Destination address", enter the machine's IP address, and then click [Next].**
24. **For the IPsec protocol type, select "Any", and then click [Next].**
25. **Click [Finish].**
26. **Click [OK].**
27. **Select the IP filter that you have just created, and then click [Next].**
28. **Select the IPsec security filter, and then click [Edit].**
29. **In the "Security Methods" tab, check "Negotiate security" and then click [Add].**
30. **Select "Custom" and click [Settings].**
31. **When [ESP] is selected for the machine in [Security Protocol] under [IPsec Settings], select [Data integrity and encryption (ESP)], and configure the following settings:**
    Set the value of **[Integrity algorithm]** to the same value as the **[Authentication Algorithm for ESP]** specified on the machine.
    Set the value of **[Encryption algorithm]** to the same value as the **[Encryption Algorithm for ESP]** specified on the machine.
32. **When [AH] is selected for the machine in [Security Protocol] under [IPsec Settings], select [Data and address integrity without encryption (AH)], and configure the following settings:**
    Set the value of **[Integrity algorithm]** to the same value as the **[Authentication Algorithm for AH]** specified on the machine.
    Clear the **[Data integrity and encryption (ESP)]** check box.
33. **When [ESP&AH] is selected for the machine in [Security Protocol] under [IPsec Settings], select [Data and address integrity without encryption (AH)], and configure the following settings:**
    Set the value of **[Integrity algorithm]** under **[Data and address integrity without encryption (AH)]** to the same value as **[Authentication Algorithm for AH]** specified on the machine.
    Set the value of **[Integrity algorithm]** under **[Data integrity and encryption (ESP)]** to the same value as **[Authentication Algorithm for ESP]** specified on the machine.
    Set the value of **[Encryption algorithm]** under **[Data integrity and encryption (ESP)]** to the same value as **[Encryption Algorithm for ESP]** specified on the machine.

34. **In the Session key settings, select "Generate a new key every", and enter the same validity period (in seconds or Kbytes) as that specified for [Life Time] on the machine.**

35. **Click [OK] three times.**

36. **Click [Next].**

37. **Click [Finish].**
    If you are using IPv6 under Windows Vista or a newer version of Windows, you must repeat this procedure from step 13 and specify ICMPv6 as an exception. When you reach step 24, select **[58]** as the protocol number for the **"Other"** target protocol type, and then set **[Negotiate security]** to **[Permit]**.

38. **Click [OK].**

39. **Click [Close].**
    The new IP security policy (IPsec settings) is specified.

40. **Select the security policy that you have just created, right click on it, and then click [Assign].**
    IPsec settings on the computer are enabled**.**

Note

- To disable the computer's IPsec settings, select the security policy, right click, and then click **[Unassign]**.

Deactivating IPsec

Using the Control Panel (models with a control panel display)

1. **Press the [User Tools] key.**
2. **Press the [▲] or [▼] key to select [Network Setting], and then press the [OK] key.**
3. **Press the [▲] or [▼] key to select [IPSec Activated], and then press the [OK] key.**
4. **Press the [▲] or [▼] key to select [Off], and then press the [OK] key.**
   IPsec is now deactivated.
5. **Press the [User Tools] key.**

Using Smart Organizing Monitor (models without a control panel display)

1. **Access Smart Organizing Monitor, and open [Printer Configuration].**
2. **Click the [Network2] tab.**
3. **In [IPsec Activated], select [Disable].**
4. **Click [OK].**
5. **Close the Smart Organizing Monitor window.**

Note

- The **[IPsec Activated]** setting can be modified only when **[Use]** is set in **[Access Code]** on the **[System]** tab.