Network User’s Guide

Version C

ENG

Table of Contents

1 Introduction

Network Features

Your Brother machine can be shared on an IEEE 802.11b/g/n wireless Ethernet network using the internal network scan server. The scan server supports various functions and connection methods, depending on your operating system and network configuration. The following chart shows the network features and connections that are supported by each operating system:

Operating Systems	**Windows® XP 32 bit (SP3)** **Windows Vista®** **Windows® 7** **Windows® 8** **Windows® 8.1** **Windows® 10** **Windows Server® 2003 R2 32 bit (SP2)** **Windows Server® 2008** **Windows Server® 2008 R2** **Windows Server® 2012** **Windows Server® 2012 R2** **Server OS supports scanning only**	**OS X v10.8.5, 10.9.x, 10.10.x, 10.11.x**
Scanning See the *User's Guide*.	✔	✔
BRAdmin Light [1] See *Using BRAdmin Light (Windows®)* on page 3.	✔	
BRAdmin Professional 3 [2] See *BRAdmin Professional 3 (Windows®)* on page 6.	✔	
Web Based Management (web browser) See *Web Based Management* on page 38.	✔	✔
Remote Setup See the *User's Guide*.	✔	✔
Status Monitor See the *User's Guide*.	✔	
Vertical Pairing See *Network Scanning Installation for Infrastructure Mode When Using Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)* on page 99.	✔	

[1] BRAdmin Light is available as a download from support.brother.com

[2] BRAdmin Professional 3 is available as a download from support.brother.com

Other Features

LDAP (ADS-2800W / ADS-3600W)

The LDAP protocol allows you to search for information, such as email addresses on your computer. When you use the Scan to E-mail server function, you can use the LDAP search to find email addresses. (See *Changing LDAP Configuration Using Your Machine's Control Panel (ADS-2800W / ADS-3600W)* on page 45.)

Scan to E-mail Server (ADS-2800W / ADS-3600W)

The Scan to E-mail Server function allows you to send scanned documents using the Internet. (See *Scan to E-mail Server (ADS-2800W / ADS-3600W)* on page 59.)

Before using this function, you have to configure the necessary machine settings using the machine's control panel, BRAdmin Professional 3, or Web Based Management.

Security

Your Brother machine employs some of the latest network security and encryption protocols available. (See *Security Features* on page 63.)

Wi-Fi Direct® (ADS-2800W / ADS-3600W)

Wi-Fi Direct® is one of the wireless configuration methods developed by the Wi-Fi Alliance®. This type of connection is a Wi-Fi standard that allows devices to connect with each other without a wireless access point, using a secured method. (See *Use Wi-Fi Direct®* on page 31.)

2 Changing Your Network Settings

Change Your Machine’s Network Settings

The machine’s network settings can be changed using the control panel, BRAdmin Light, Web Based Management, or BRAdmin Professional 3.

Using the Machine’s Control Panel (ADS-2800W / ADS-3600W)

You can configure your machine for a network using the Network control panel menu.

How to Check the Network Status (ADS-2800W / ADS-3600W)

1. On your machine’s LCD, press 🛠.
2. Press `Network`.
3. Press `Wired LAN`.
4. Press `Wired Status`.
5. Press `Status`.

Using BRAdmin Light (Windows®)

The BRAdmin Light utility is designed for initial setup of Brother network-connected devices. It also can search for Brother products in a TCP/IP environment, view the status, and configure basic network settings, such as IP address.

Installing BRAdmin Light

1. Make sure your machine is ON.
2. Turn on your computer. Close any open applications.
3. Put the installation DVD-ROM into your DVD-ROM drive.
4. Double click **(DVD Drive):\Tools\BRAdminLight\xxx\disk1\setup.exe**.

Setting the IP address, Subnet Mask and Gateway Using BRAdmin Light

NOTE

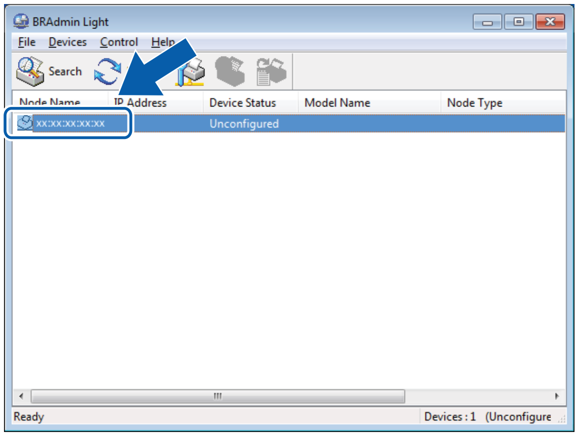
- Go to your model's **Downloads** page on the Brother Solutions Center at support.brother.com to download the latest version of Brother's BRAdmin Light.
- If you require more advanced machine management, use the latest version of BRAdmin Professional 3. Go to your model's **Downloads** page on the Brother Solutions Center at support.brother.com to download BRAdmin Professional 3. This utility is available only for Windows® users.
- If you are using the firewall function of an anti-spyware or antivirus application, temporarily disable the application. When you are sure that you can scan, re-enable the application.
- Node name: The Node name appears in the current BRAdmin Light window. The default node name of the scan server in the machine is "BRWxxxxxxxxxxxx" for a wireless network (where "xxxxxxxxxxxx" is your machine's MAC Address / Ethernet Address).
- No password is required by default. Type a password if you have set one and press **OK**.

1. Start BRAdmin Light.
   - Windows® XP, Windows Vista® and Windows® 7

     Click (**Start**) > **All Programs** > **Brother** > **BRAdmin Light** > **BRAdmin Light**.
   - Windows® 8, Windows® 8.1, and Windows® 10

     Click (**BRAdmin Light**) in the task tray.
2. BRAdmin Light automatically searches for new devices.

3 Double-click your Brother machine.



Node Name	IP Address	Device Status	Model Name	Node Type
xx:xx:xx:xx:xx:xx		Unconfigured		

Ready Devices : 1 (Unconfigure

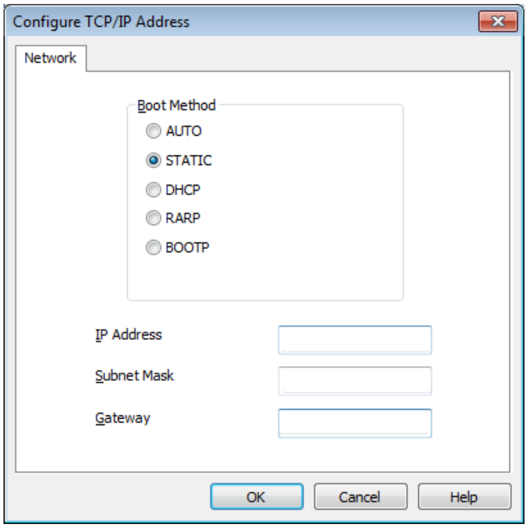
NOTE

- If the scan server is set to its factory settings (and you do not use a DHCP/BOOTP/RARP server), the device appears as **Unconfigured** in the BRAdmin Light utility window.
- You can display your machine's MAC Address (Ethernet Address) and Node Name using the machine's LCD (ADS-2800W / ADS-3600W).

  To find the MAC Address, press 🛠 > `Network` > `WLAN` > `MAC Address`.

  To find the Node Name, press 🛠 > `Network` > `WLAN` > `TCP/IP` > `Node Name`.

4 Select **STATIC** from the **Boot Method** list. Type the **IP Address**, **Subnet Mask** and **Gateway** (if needed) for your machine.



Boot Method
○ AUTO
● STATIC
○ DHCP
○ RARP
○ BOOTP

IP Address
Subnet Mask
Gateway

5 Click **OK**.

6 Your Brother machine appears in the device list. If it does not, check your IP Address in step 4.

Other Management Utilities

Web Based Management

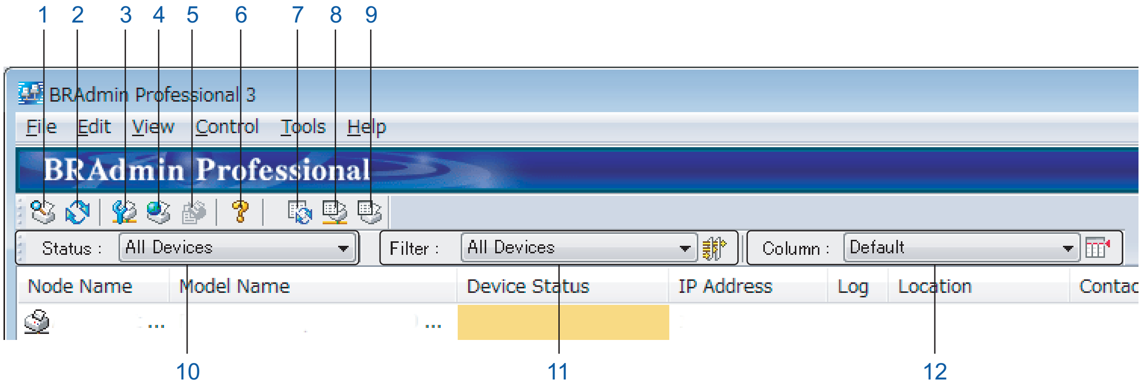
A standard web browser can be used to change your scan server settings using the HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol Secure). (See *Configure Your Machine Settings* on page 39.)

BRAdmin Professional 3 (Windows®)

BRAdmin Professional 3 is a utility for more advanced management of network-connected Brother devices. This utility can search for Brother products on your network and display them in an easy-to-read, Explorer-style window. Icons change color to show the status of each device. You can configure network and device settings and can update device firmware from a Windows® computer on your network. BRAdmin Professional 3 can also log the activity of Brother devices on your network and export the log data in HTML, CSV, TXT, or SQL format.

NOTE

- Use the latest version of the BRAdmin Professional 3 utility. Go to your model's **Downloads** page on the Brother Solutions Center at support.brother.com to download Brother's BRAdmin Professional 3. This utility is available only for Windows® users.
- If you are using the firewall function of an anti-spyware or antivirus application, temporarily disable the application. When you are sure that you can scan, re-enable the application.
- Node name: The Node name for each Brother device on the network appears in BRAdmin Professional 3. The default Node name is "BRWxxxxxxxxxxxx" for a wireless network (where "xxxxxxxxxxxx" is your machine's MAC Address/Ethernet Address).



1 **Search Network**

Searches for devices on your network.

By default, BRAdmin Professional is configured to view all supported network devices in your local network that have been configured with a valid IP address.

2 **Get Device Status (ALL)**

Refreshes the status of the devices that BRAdmin Professional is communicating with.

3 **Set up Unconfigured Devices**

If your network-connected Brother device does not have a valid IP address, BRAdmin Professional allows you to set your device’s IP address, subnet mask, gateway address and boot method.

4 **Device Home Page (Web Based Management)**

Connects to the embedded web server within the machine (note that not all devices have an embedded web server).

5 **Send File**

Sends a file to a device.

6 **Help Topics**

Shows the Help File for BRAdmin Professional 3.

7 **Log Refresh**

Refreshes the log history.

8 **View Network Devices Log**

Shows the log information of all devices on the network.

9 **View Local Devices Log**

Shows the log information of all devices that are connected to the client computers registered in Local Devices Log Settings.

10 **Status**

Select a status from the drop-down list.

11 **Filter**

Select a filter from the drop-down list.

To select a filter from the drop-down list, you must add menus by clicking in advance.

12 **Column**

The Column Settings option allows you to select which columns are displayed within BRAdmin Professional’s main view screen.

NOTE

For more information about BRAdmin Professional 3, click ? .

3 Configuring Your Machine for a Wireless Network (ADS-2800W / ADS-3600W)

Overview

To connect your machine to your wireless network, we recommend following one of the setup methods outlined in the *Quick Setup Guide*. Go to your model's page on the Brother Solutions Center at solutions.brother.com/manuals to download the *Quick Setup Guide*.

For more information about additional wireless configuration methods and settings, read this chapter. For information on TCP/IP settings, see *Change Your Machine's Network Settings* on page 3.

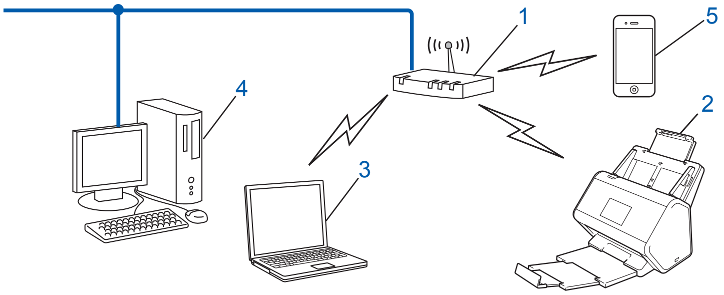
NOTE

- To achieve optimum results with everyday document scanning, place the Brother machine as close to the WLAN access point/router as possible with minimal obstructions. Large objects and walls between the two devices and interference from other electronic devices can affect the data transfer speed of your documents.

  Due to these factors, wireless may not be the best method of connection for all types of documents and applications. If you are scanning large files, such as multi-page documents with mixed text and large graphics, consider using a USB cable for a faster throughput speed.
- Before configuring wireless settings, you need to know your Network Name (SSID) and Network Key.

Confirm Your Network Environment

Connected to a Computer with a WLAN Access Point/Router in the Network (Infrastructure Mode)



1 WLAN access point/router [1]

[1] If your computer supports Intel® My WiFi Technology (MWT), you can use your computer as a Wi-Fi Protected Setup™ (WPS) supported access point.

2 Wireless network machine (your machine)

3 Wireless-capable computer connected to the WLAN access point/router

4 Wired computer (that is not wireless-capable) connected to the WLAN access point/router with a network cable

5 Mobile Device connected to the WLAN access point/router

Configuration Method

The following are different methods for configuring your Brother machine in a wireless network environment. Choose the method you prefer for your environment:

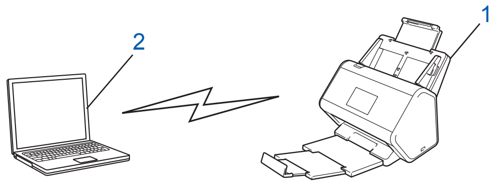
- Wireless configuration, temporarily (Recommended). See the *Quick Setup Guide*.
- One push wireless configuration using WPS (Wi-Fi Protected Setup™). See page 18.
- PIN Method wireless configuration using WPS. See page 19.
- Configure for a wireless network using the Setup Wizard. See page 29.

How to Check the WLAN Status (ADS-2800W / ADS-3600W)

1. On your machine’s LCD, press 🛠.
2. Press `Network`.
3. Press `WLAN`.
4. Press ▲ or ▼ and then press `WLAN Status`.
5. Press `Status`.

Connected to a Wireless Capable Computer without a WLAN Access Point/Router in the Network (Ad-hoc Mode)

This type of network does not have a central WLAN access point/router. Each wireless client communicates directly with the other. When the Brother wireless machine (your machine) is part of this network, it receives all scan jobs directly from the computer sending the scan data.



1 Wireless network machine (your machine)

2 Wireless-capable computer

We do not guarantee the wireless network connection in Ad-hoc mode. To set up your machine in Ad-hoc mode, see *Configuration in Ad-hoc Mode* on page 22.

Configuration

When the SSID Is Not Broadcasting

1 Before configuring your machine, we recommend writing down your wireless network settings. You will need this information to proceed with the configuration.
Check and write down the current wireless network settings.

Network name (SSID)

Communication Mode	Authentication Method	Encryption Mode	Network Key
Infrastructure	Open system	NONE	—
		WEP	
	Shared key	WEP	
	WPA/WPA2-PSK	AES	
		TKIP [1]	

[1] TKIP is supported for WPA-PSK only.

For example:

Network name (SSID)
HELLO

Communication Mode	Authentication method	Encryption mode	Network key
Infrastructure	WPA2-PSK	AES	12345678

NOTE

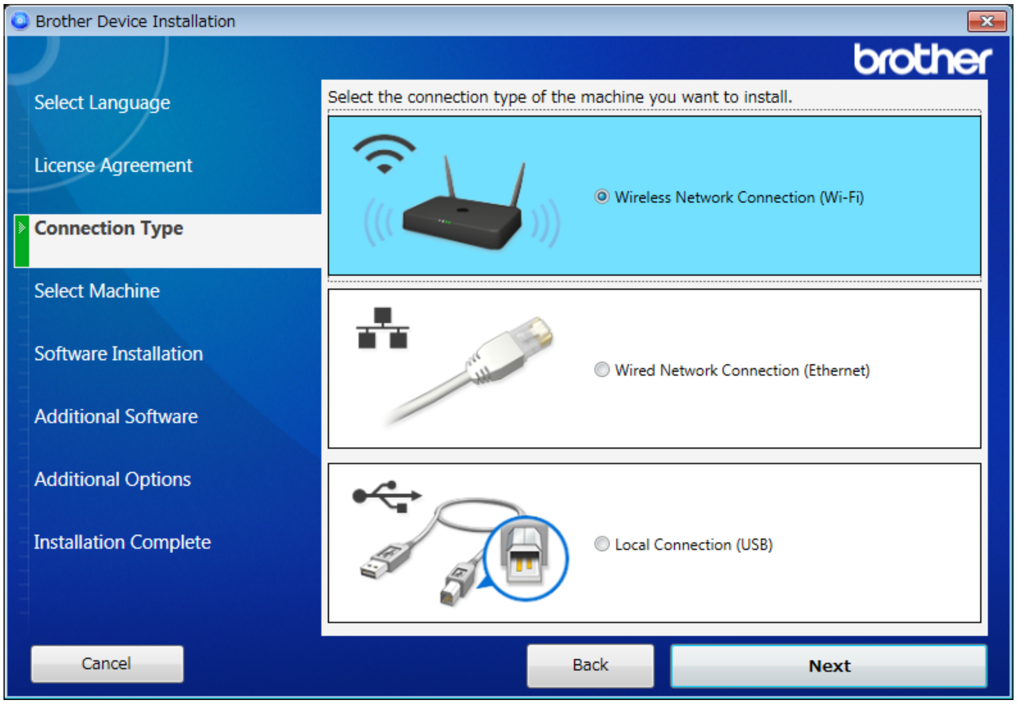
If your router uses WEP encryption, enter the key used as the first WEP key. Your Brother machine supports the use of the first WEP key only.

2 Do one of the following:

- Windows®

a Insert the supplied DVD-ROM into your DVD-ROM drive.

b Select **Wireless Network Connection (Wi-Fi)**, and then click **Next**.



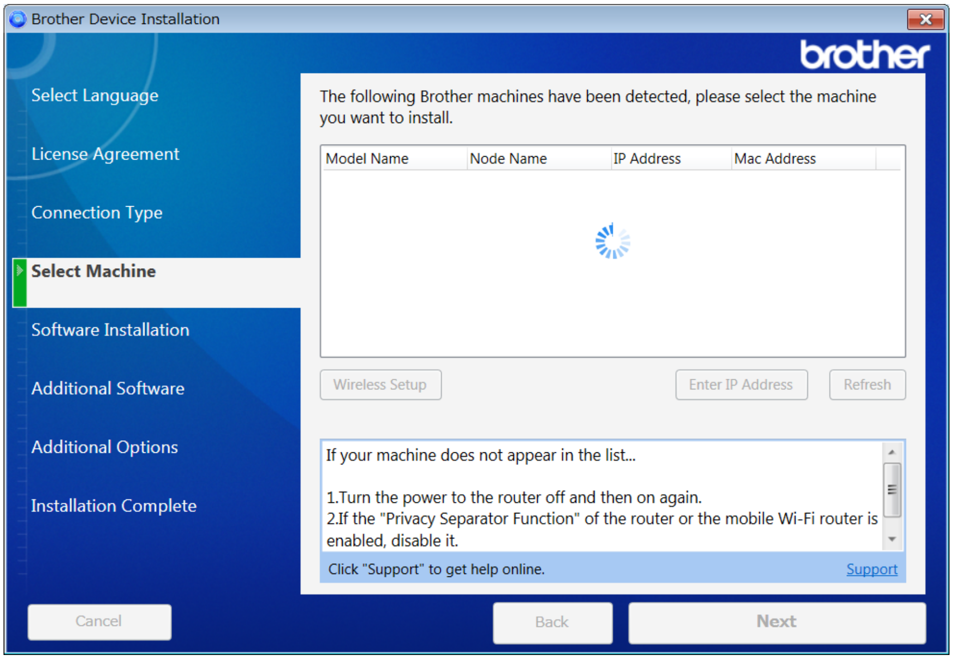
Select the connection type of the machine you want to install.

● Wireless Network Connection (Wi-Fi)

○ Wired Network Connection (Ethernet)

○ Local Connection (USB)

c Click **Wireless Setup**.



The following Brother machines have been detected, please select the machine you want to install.

Model Name	Node Name	IP Address	Mac Address

If your machine does not appear in the list...

1.Turn the power to the router off and then on again.
2.If the "Privacy Separator Function" of the router or the mobile Wi-Fi router is enabled, disable it.

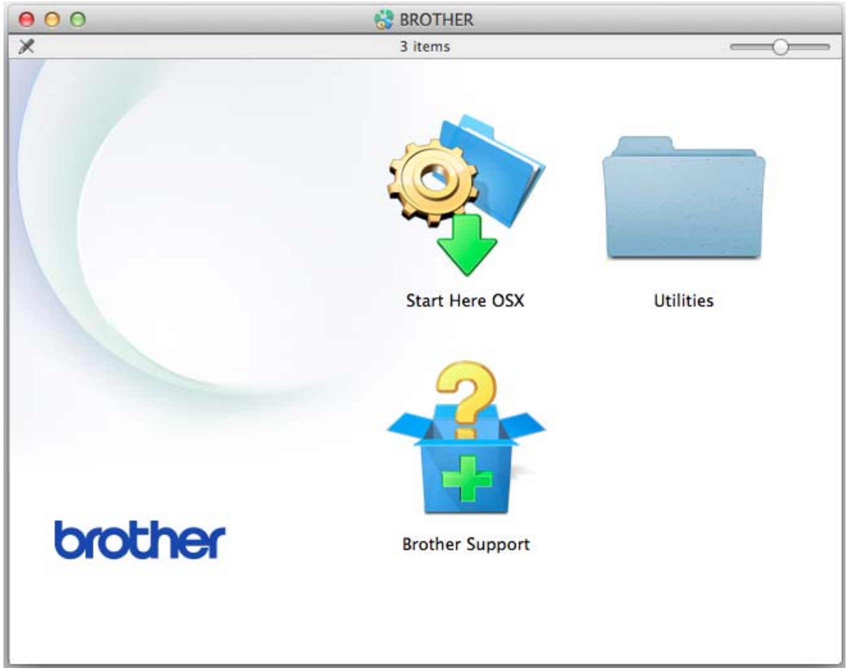
Click "Support" to get help online.

- Macintosh

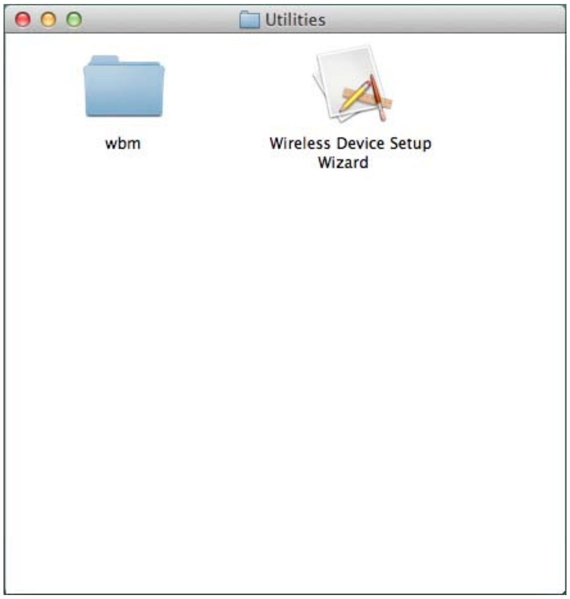
a Download the full driver and software package from the Brother Solutions Center (support.brother.com).

b Double-click the **BROTHER** icon on your desktop.

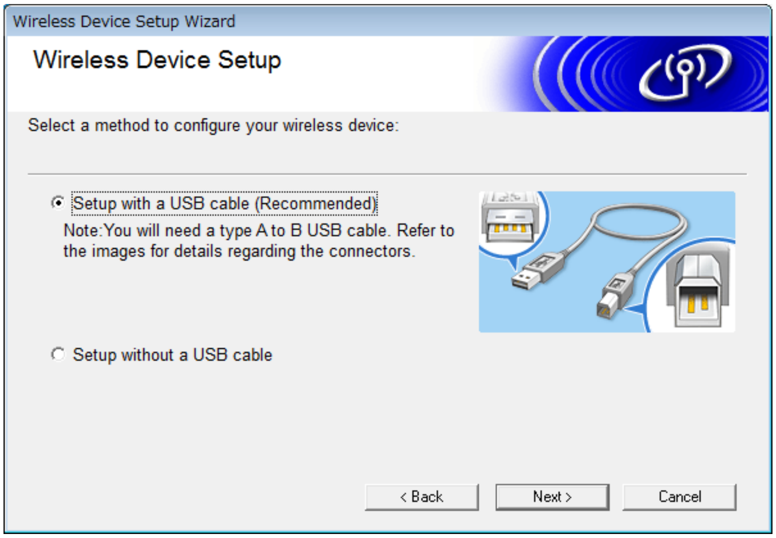
c Double-click **Utilities**.



d Double-click **Wireless Device Setup Wizard**.



3 Select **Setup with a USB cable (Recommended)**, and then click **Next**.
We recommend using a USB cable temporarily.


Wireless Device Setup Wizard

Wireless Device Setup

Select a method to configure your wireless device:

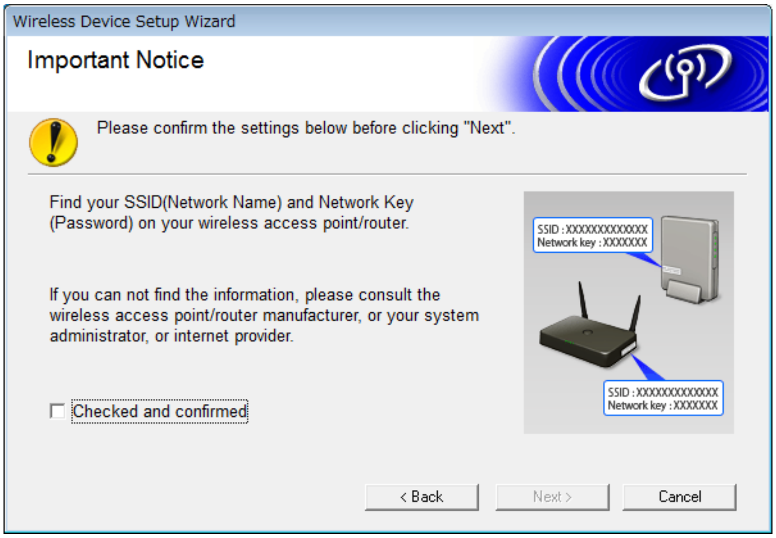
● Setup with a USB cable (Recommended)

Note:You will need a type A to B USB cable. Refer to the images for details regarding the connectors.

○ Setup without a USB cable

NOTE

If this screen appears, read the **Important Notice**. Confirm the SSID and Network Key, select the **Checked and confirmed** check box, and then click **Next**.


Wireless Device Setup Wizard

Important Notice

Please confirm the settings below before clicking "Next".

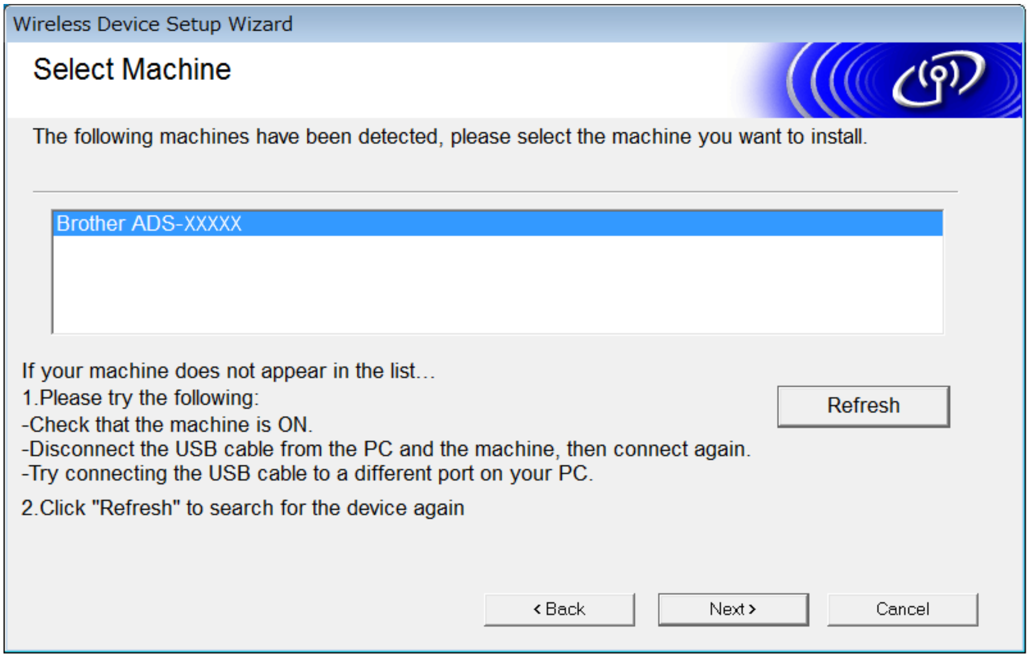
Find your SSID(Network Name) and Network Key (Password) on your wireless access point/router.

If you can not find the information, please consult the wireless access point/router manufacturer, or your system administrator, or internet provider.

□ Checked and confirmed

4 Temporarily connect the USB cable directly to the computer and the machine.
If the confirmation screen appears, click **Next**.

5 Click **Next**. (Windows® Only)



Wireless Device Setup Wizard

Select Machine

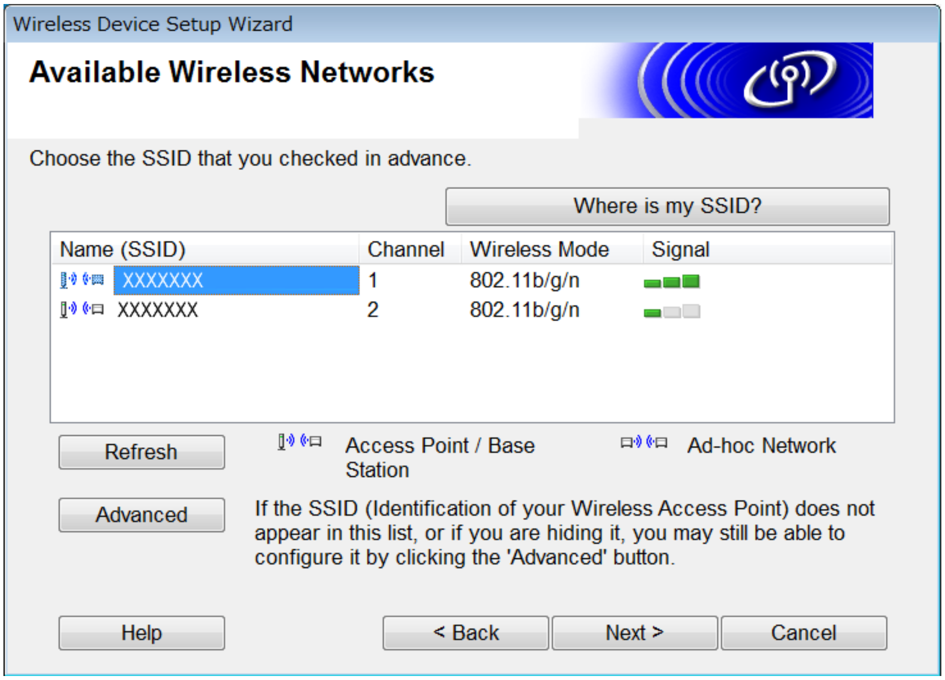
The following machines have been detected, please select the machine you want to install.

Brother ADS-XXXXX

If your machine does not appear in the list...
1.Please try the following:
-Check that the machine is ON.
-Disconnect the USB cable from the PC and the machine, then connect again.
-Try connecting the USB cable to a different port on your PC.
2.Click "Refresh" to search for the device again

6 Do one of the following:

- Select the SSID you want to use and click **Next**. Then configure **Network Key** and go to ❿.
- If the SSID you want to use is not broadcasting, click **Advanced** and go to ❼.



Wireless Device Setup Wizard

Available Wireless Networks

Choose the SSID that you checked in advance.

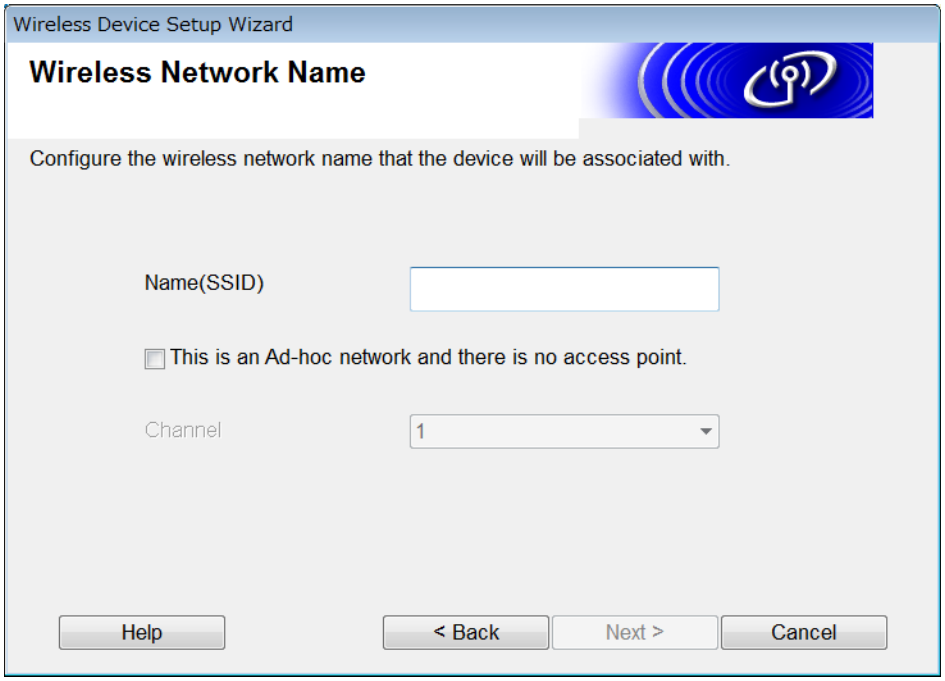
Name (SSID)	Channel	Wireless Mode	Signal
XXXXXXX	1	802.11b/g/n	🟩🟩🟩
XXXXXXX	2	802.11b/g/n	🟩⬜⬜

Access Point / Base Station

Ad-hoc Network

If the SSID (Identification of your Wireless Access Point) does not appear in this list, or if you are hiding it, you may still be able to configure it by clicking the 'Advanced' button.

7 Type a new SSID in the **Name(SSID)** field, and then click **Next**.



Wireless Device Setup Wizard

Wireless Network Name

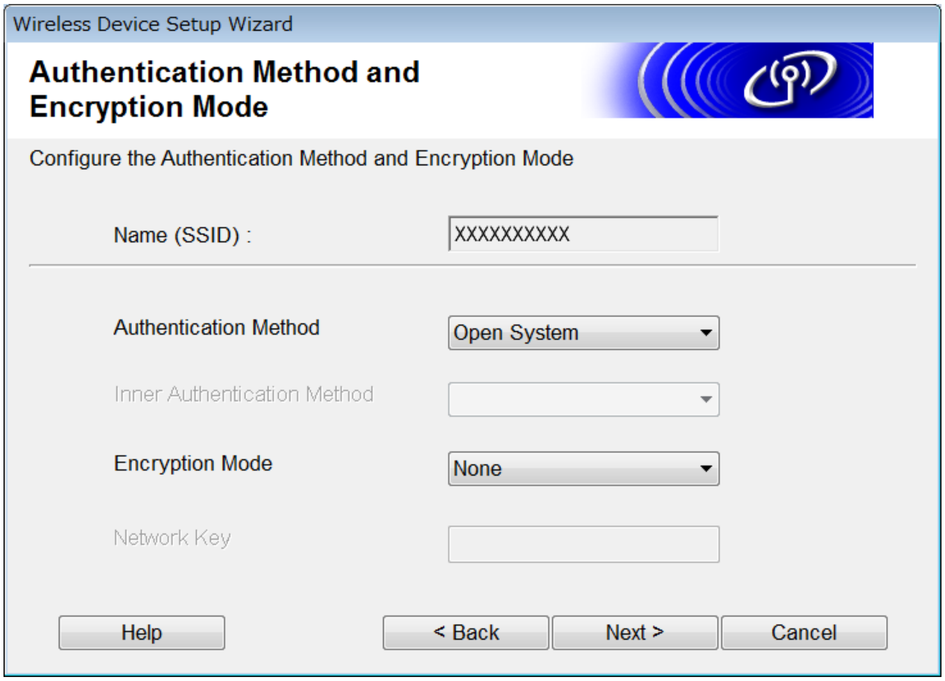
Configure the wireless network name that the device will be associated with.

Name(SSID)

□ This is an Ad-hoc network and there is no access point.

Channel: 1

8 Select the **Authentication Method** and **Encryption Mode** from the drop-down lists, type a network key in the **Network Key** field, and then click **Next** and go to ❿.



Wireless Device Setup Wizard

Authentication Method and Encryption Mode

Configure the Authentication Method and Encryption Mode

Name (SSID) : XXXXXXXXXX

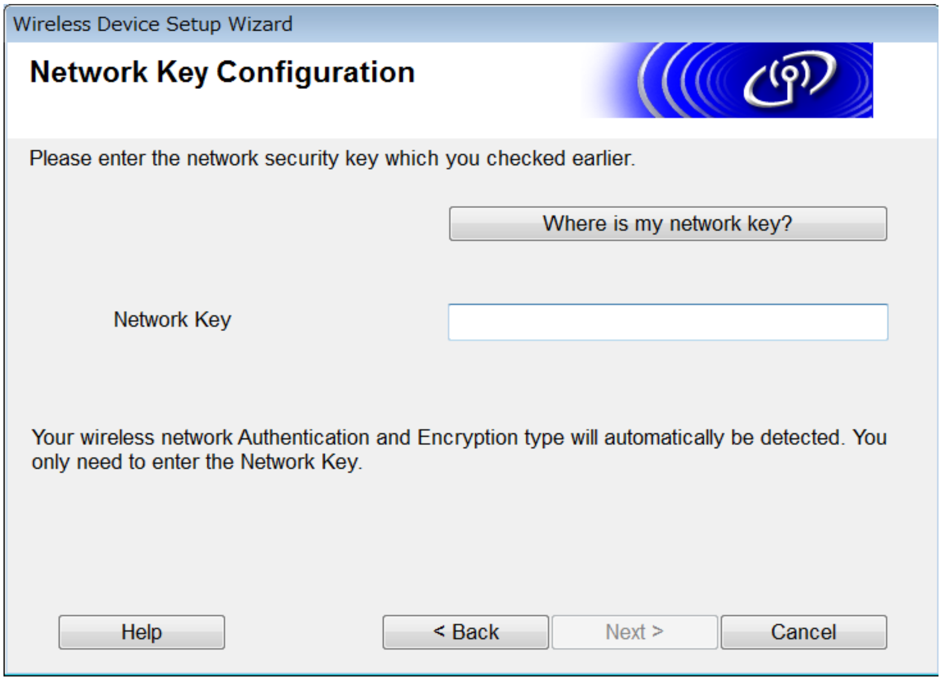
Authentication Method: Open System

Inner Authentication Method

Encryption Mode: None

Network Key

9 Type a new Network key in the **Network Key** field, and then click **Next**.



Wireless Device Setup Wizard

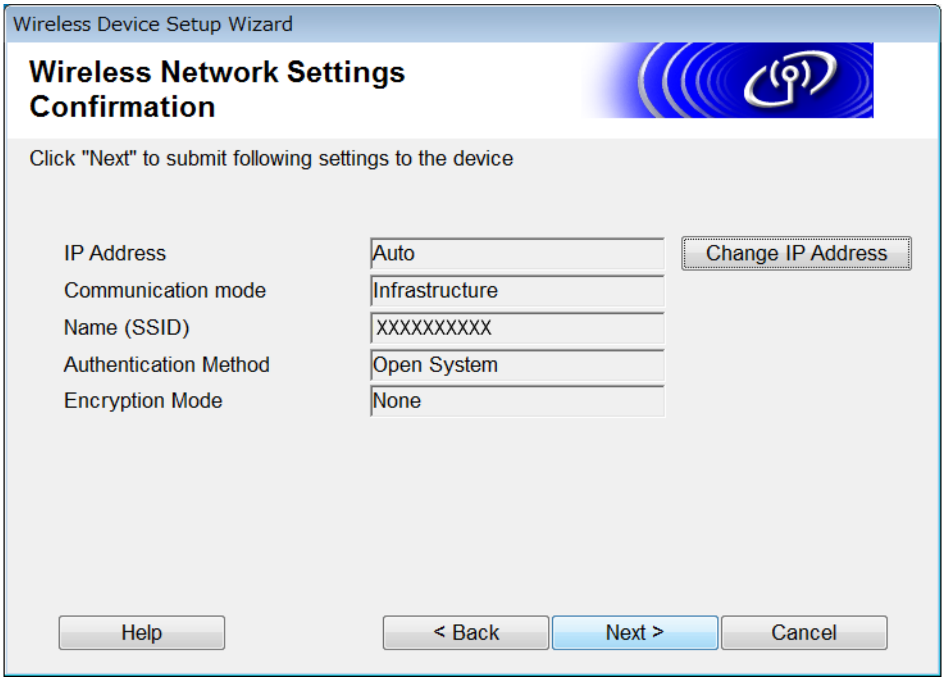
Network Key Configuration

Please enter the network security key which you checked earlier.

Network Key

Your wireless network Authentication and Encryption type will automatically be detected. You only need to enter the Network Key.

10 Click **Next**. The machine receives the settings.
(The following screen may differ depending on your settings.)



Wireless Device Setup Wizard

Wireless Network Settings Confirmation

Click "Next" to submit following settings to the device

IP Address	Auto
Communication mode	Infrastructure
Name (SSID)	XXXXXXXXXX
Authentication Method	Open System
Encryption Mode	None

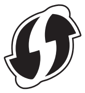
NOTE

DO NOT disconnect the USB cable until the on-screen instruction confirms that configuration is complete and that you can safely remove the cable.

11. Disconnect the USB cable between the computer and the machine.
12. Click **Finish**.

Using WPS (Wi-Fi Protected Setup™)

1. Confirm that your wireless access point/router has the WPS symbol as shown below.

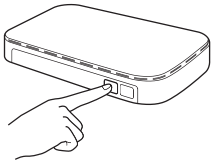


2. Place the Brother machine within range of your wireless access point/router. The range may differ depending on your environment. Refer to the instructions provided with your wireless access point/router.
3. On the machine's LCD, press 🛠 > `Network` > `WLAN` > `WPS`.
   When `Enable WLAN?` appears, press `Yes` to accept.

NOTE

- If you do not start `WPS` from the machine's LCD a few seconds after pressing the WPS button on your wireless access point/router, the connection may fail.
- If your wireless access point/router supports WPS and you want to configure your machine using the PIN (Personal Identification Number) Method, see *Using the PIN Method of Wi-Fi Protected Setup™ (WPS)* on page 19.

4. When the LCD instructs you to start WPS, press the WPS button on your wireless access point/router (for more information, see the instructions provided with your wireless access point/router).



   Press `OK` on your Brother machine's LCD.
5. Your machine automatically detects which mode (WPS) your wireless access point/router uses, and tries to connect to your wireless network.
6. If your wireless device is connected successfully, the LCD displays the message `Connected` until you press `OK`.
   The wireless setup is now complete. The Wi-Fi light 📶 on the Control Panel lights up, indicating that the machine's network interface is set to WLAN.

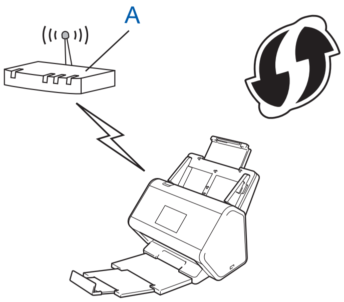
Using the PIN Method of Wi-Fi Protected Setup™ (WPS)

If your WLAN access point/router supports WPS (PIN Method), configure the machine using the instructions.

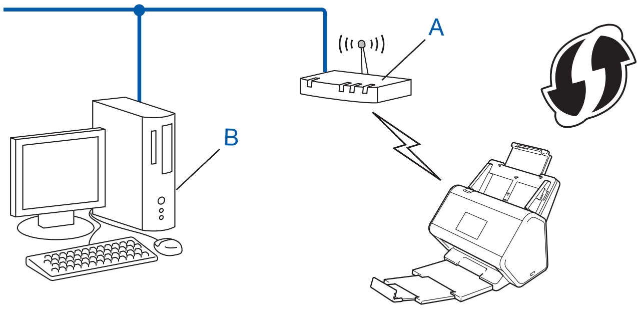
NOTE

The Personal Identification Number (PIN) Method is one of the connection methods developed by the Wi-Fi Alliance®. By entering a PIN created by an *Enrollee* (your machine) to the *Registrar* (a device that manages the wireless LAN), you can set up the WLAN network and security settings. See the *User's Guide* supplied with your WLAN access point/router for instructions on how to access WPS mode.

- Connection when the WLAN access point/router (A) doubles as a Registrar [1].



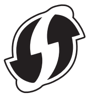
- Connection when another device (B), such as a computer, is used as a Registrar [1].



[1] The Registrar is normally the WLAN access point/router.

NOTE

Routers or access points that support WPS display this symbol:



1. On the machine's LCD, press .
2. Press `Network`.
3. Press `WLAN`.
4. Press ▲ or ▼ to display `WPS w/ PIN Code`.
   Press `WPS w/ PIN Code`.
5. When `Enable WLAN?` is displayed, press `Yes` to accept.
   The wireless setup wizard starts.
   To cancel, press `No`.
6. The LCD displays an eight-digit PIN and the machine starts searching for an access point.
7. In your browser's address bar, type the IP address of your access point (Registrar [1]).

   [1] The Registrar is normally the WLAN access point/router.
8. Go to the WPS setup page, type the PIN displayed on the LCD in step ❻ into the Registrar, and follow the on-screen instructions.

NOTE

- The setup page is different, depending on the brand of access point/router you are using. See the instruction manual supplied with your access point/router.
- To use a Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 computer as a Registrar, you need to register it to your network in advance. See the instruction manual that came with your WLAN access point/router.
- If you use Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 as a Registrar, you can install the scanner driver after the wireless configuration by following the on-screen instructions. To install the full driver and software package, follow the steps in the *Quick Setup Guide* for installation.

Windows Vista®/Windows® 7/Windows® 8/Windows® 8.1/Windows® 10

If you are using your computer as a Registrar, follow these steps:

a Windows Vista®

Click (**Start**) > **Network** > **Add a wireless device**.

Windows® 7
Click (**Start**) > **Devices and Printers** > **Add a device**.

Windows® 8 and Windows® 8.1
Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings** > **Control Panel** > **Devices and Printers** > **Add a device**.

Windows® 10
Click (**Start**) > **Settings** > **Devices** > **Connected Devices** > **Add a device**.

b Select the machine and click **Next**.

c Type the PIN displayed on the LCD in step ❻, and then click **Next**.

d Select the network you want to connect to, and then click **Next**.

e Click **Close**.

9 If your wireless device is connected successfully, the LCD displays `Connected`.
If the connection failed, the LCD shows an error code. Make a note of the error code, see *Wireless LAN Error Codes (ADS-2800W / ADS-3600W)* on page 89 and correct the error.

OK! **Windows®**

You have completed the wireless network setup. To continue installing the drivers and software necessary for operating your device, put the DVD-ROM into your DVD drive.

NOTE

If the Brother screen does not appear automatically, click **(Start)** > **Computer (My Computer)**.

(For Windows® 8, Windows® 8.1, Windows® 10: click the **(File Explorer)** icon on the taskbar, and then go to **This Computer/This PC**.) Double-click the DVD icon, and then double-click **start.exe**.

Macintosh

You have completed the wireless network setup. To continue installing the drivers and software necessary for operating your device, select **Start Here OSX** from the driver's menu.

Configuration in Ad-hoc Mode

Using a Configured SSID

If you are trying to pair the machine to a computer that is already in Ad-hoc mode with a configured SSID, complete the following steps:

1. Before configuring your machine, we recommend writing down your wireless network settings. You will need this information to proceed with the configuration.
   Check and record the current wireless network settings of the computer you are connecting with.

NOTE

The wireless network settings of the computer you are connecting with must be set to Ad-hoc mode with an SSID already configured. For instructions on how to set your computer to Ad-hoc mode, see the information included with your computer or contact your network administrator.

Network name (SSID)

Communication Mode	Encryption mode	Network key
Ad-hoc	NONE	—
	WEP	

For example:

Network name (SSID)
HELLO

Communication Mode	Encryption mode	Network key
Ad-hoc	WEP	12345

NOTE

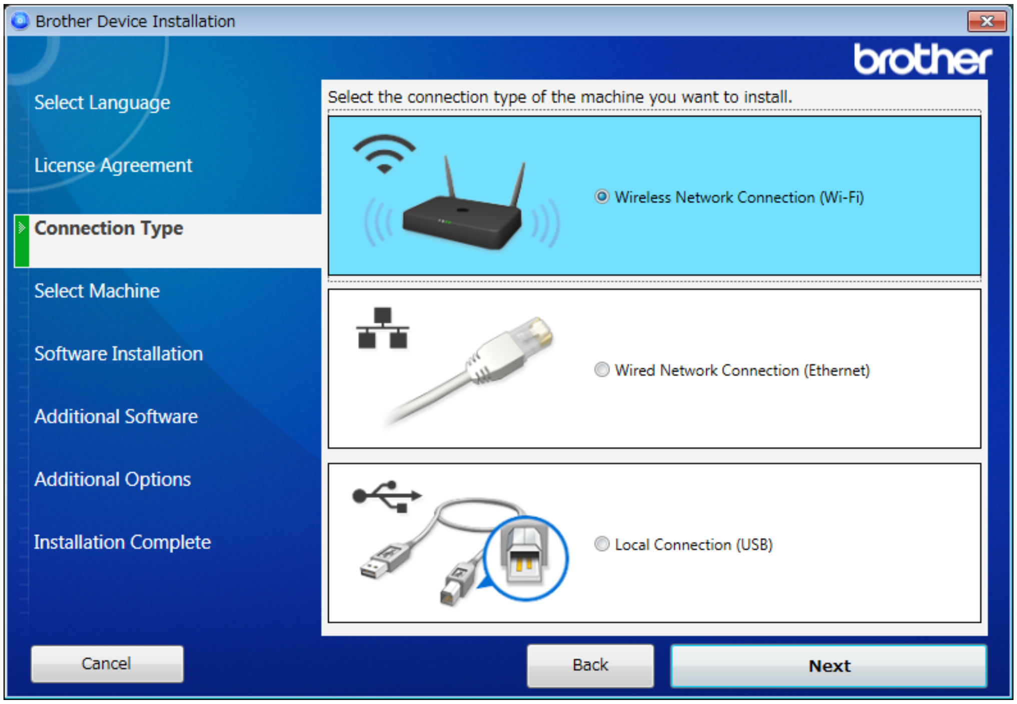
Your Brother machine supports the use of the first WEP key only.

2 Do one of the following:

- Windows®

a Insert the supplied DVD-ROM into your DVD-ROM drive.

b Select **Wireless Network Connection (Wi-Fi)**, and then click **Next**.



Brother Device Installation

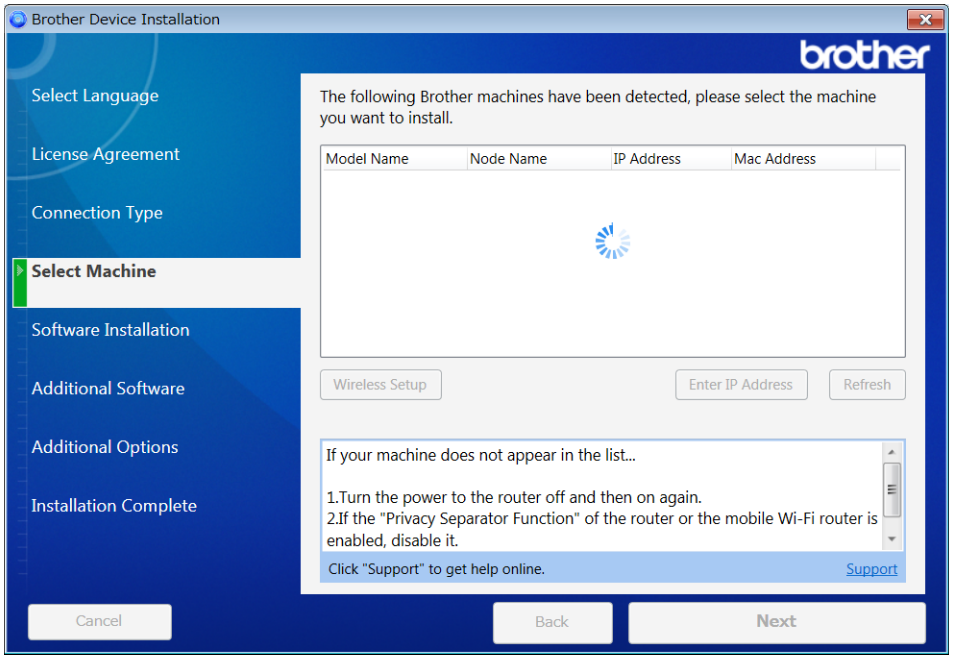
Select the connection type of the machine you want to install.

● Wireless Network Connection (Wi-Fi)

○ Wired Network Connection (Ethernet)

○ Local Connection (USB)

c Click **Wireless Setup**.



Brother Device Installation

The following Brother machines have been detected, please select the machine you want to install.

Model Name	Node Name	IP Address	Mac Address

If your machine does not appear in the list...

1.Turn the power to the router off and then on again.
2.If the "Privacy Separator Function" of the router or the mobile Wi-Fi router is enabled, disable it.

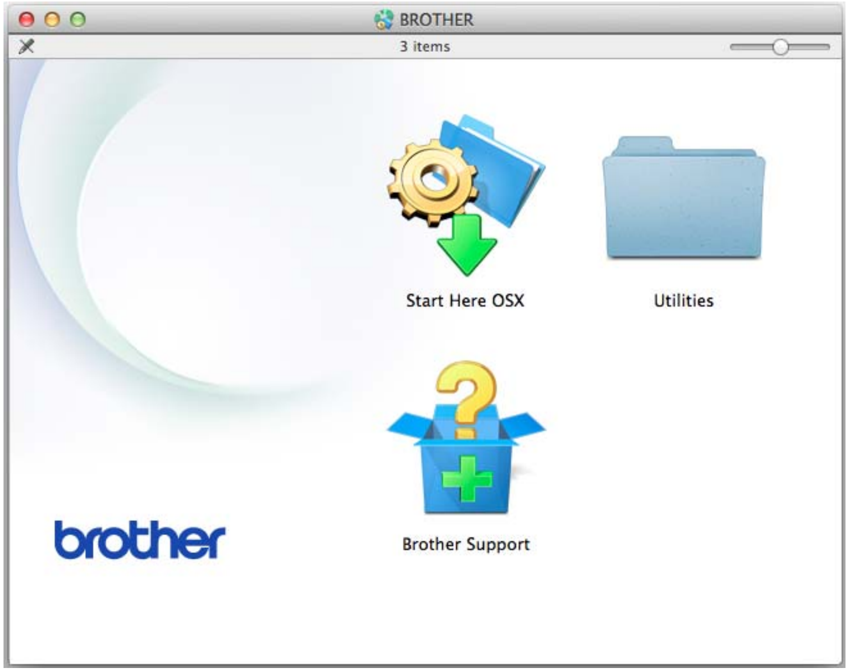
Click "Support" to get help online. Support

- Macintosh

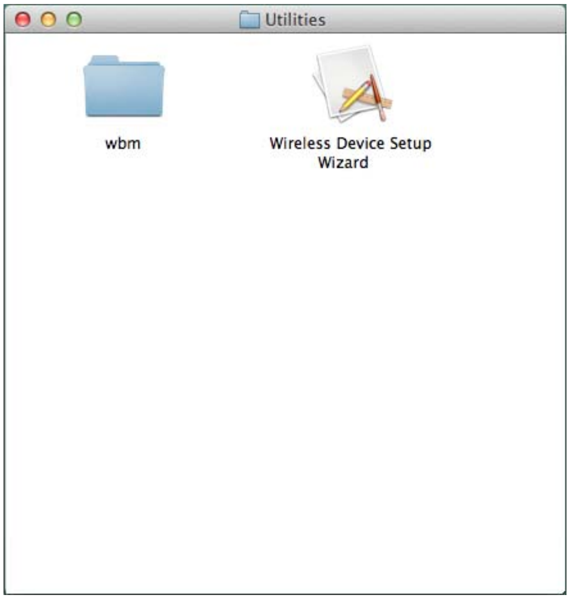
a Download the full driver and software package from the Brother Solutions Center (support.brother.com).

b Double-click the **BROTHER** icon on your desktop.

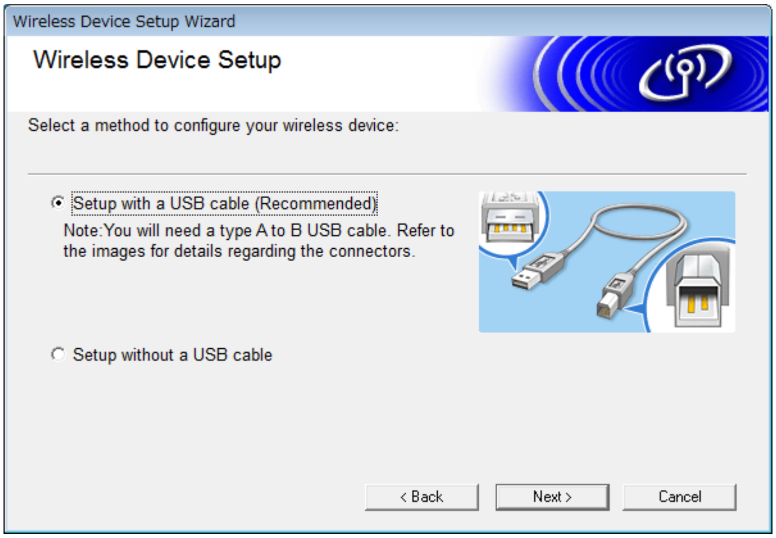
c Double-click **Utilities**.



d Double-click **Wireless Device Setup Wizard**.



3 Select **Setup with a USB cable (Recommended)**, and then click **Next**.
We recommend using a USB cable temporarily.



Wireless Device Setup Wizard

Wireless Device Setup

Select a method to configure your wireless device:

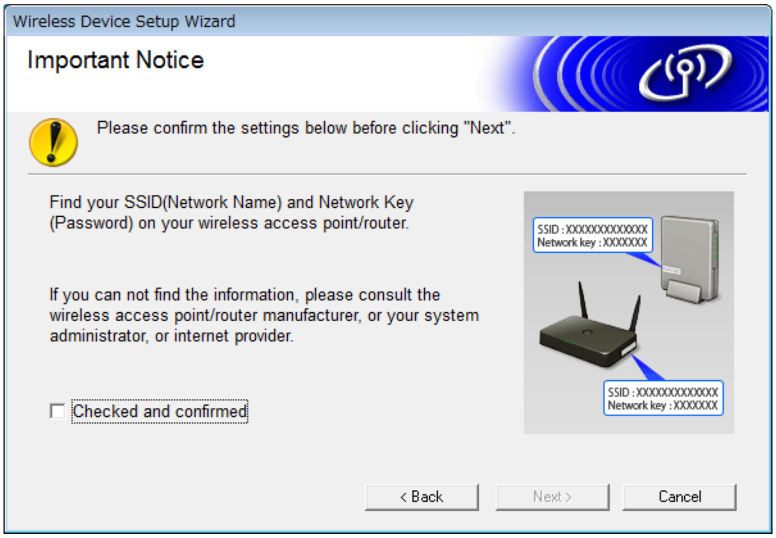
● Setup with a USB cable (Recommended)

Note:You will need a type A to B USB cable. Refer to the images for details regarding the connectors.

○ Setup without a USB cable

NOTE

If this screen appears, read the **Important Notice**. Confirm the SSID and Network Key, select the **Checked and confirmed** check box, and then click **Next**.



Wireless Device Setup Wizard

Important Notice

Please confirm the settings below before clicking "Next".

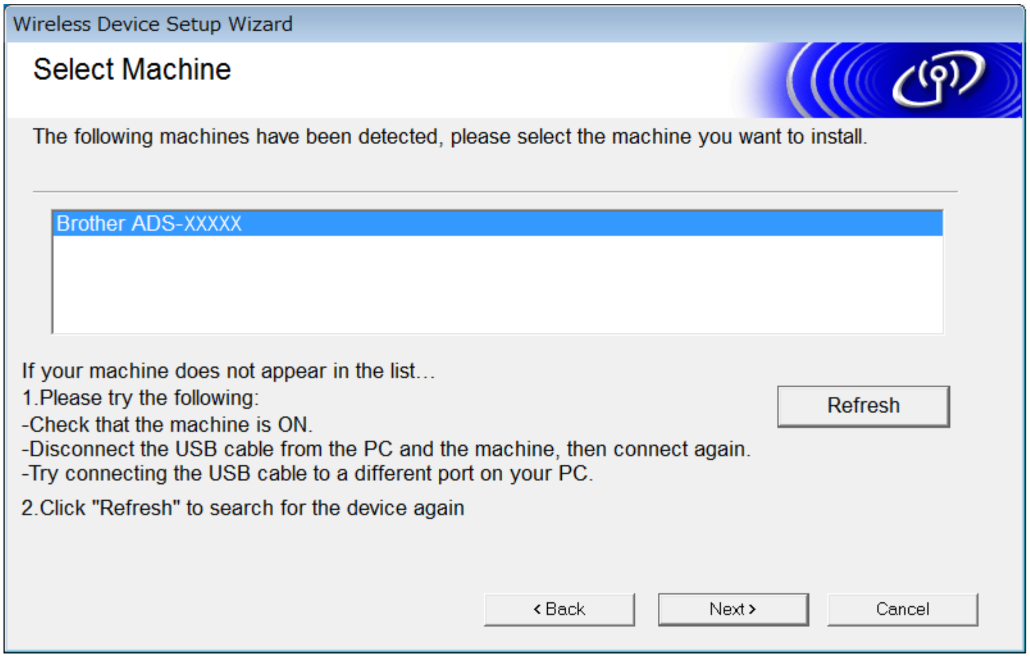
Find your SSID(Network Name) and Network Key (Password) on your wireless access point/router.

If you can not find the information, please consult the wireless access point/router manufacturer, or your system administrator, or internet provider.

□ Checked and confirmed

4 Temporarily connect the USB cable directly to the computer and the machine.
If the confirmation screen appears, click **Next**.

5 Click **Next**. (Windows® Only)



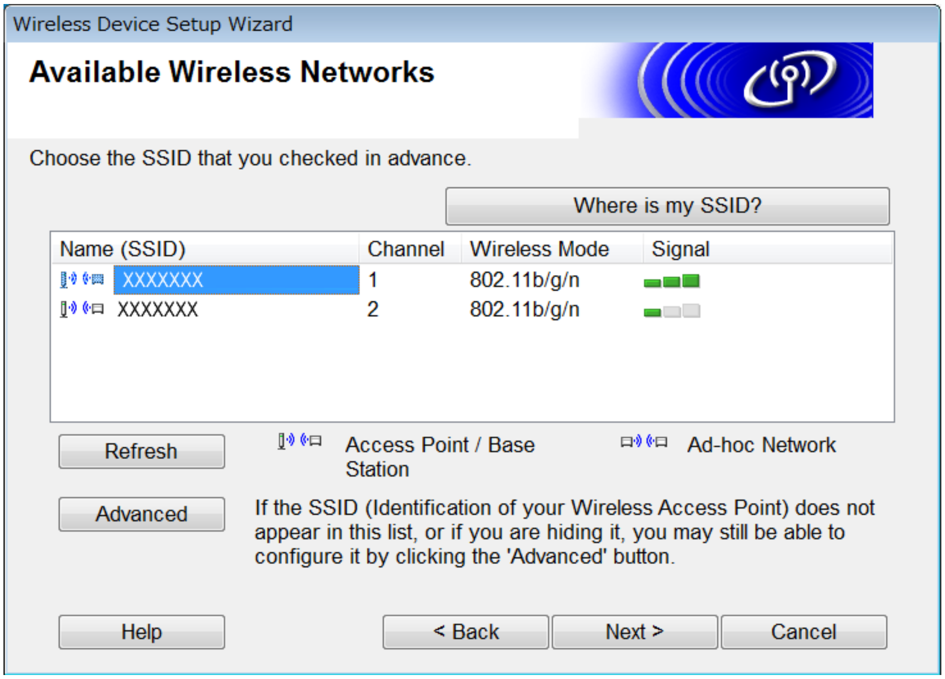
Select Machine

The following machines have been detected, please select the machine you want to install.

Brother ADS-XXXXX

If your machine does not appear in the list...
1.Please try the following:
-Check that the machine is ON.
-Disconnect the USB cable from the PC and the machine, then connect again.
-Try connecting the USB cable to a different port on your PC.
2.Click "Refresh" to search for the device again

6 Click **Advanced**.



Available Wireless Networks

Choose the SSID that you checked in advance.

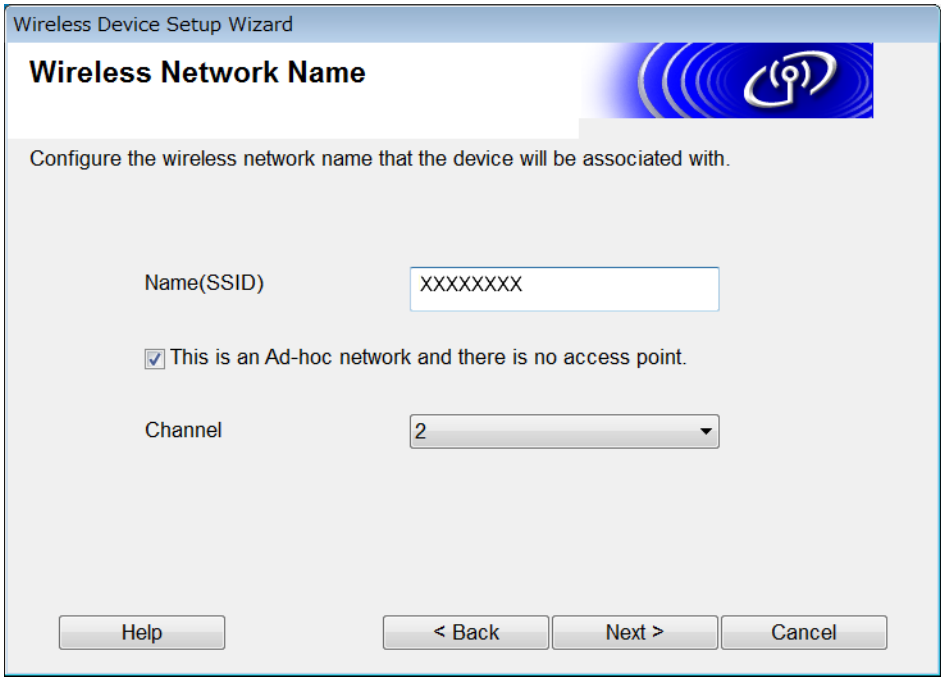
Name (SSID)	Channel	Wireless Mode	Signal
XXXXXXX	1	802.11b/g/n	🟩🟩🟩
XXXXXXX	2	802.11b/g/n	🟩⬜⬜

If the SSID (Identification of your Wireless Access Point) does not appear in this list, or if you are hiding it, you may still be able to configure it by clicking the 'Advanced' button.

NOTE

If the list is blank, confirm that the access point has power and is broadcasting the SSID, and then see if the machine and your computer are within range for wireless communication. Then click **Refresh**.

7 Check the **This is an Ad-hoc network and there is no access point.** and then click **Next**.


Wireless Device Setup Wizard

Wireless Network Name

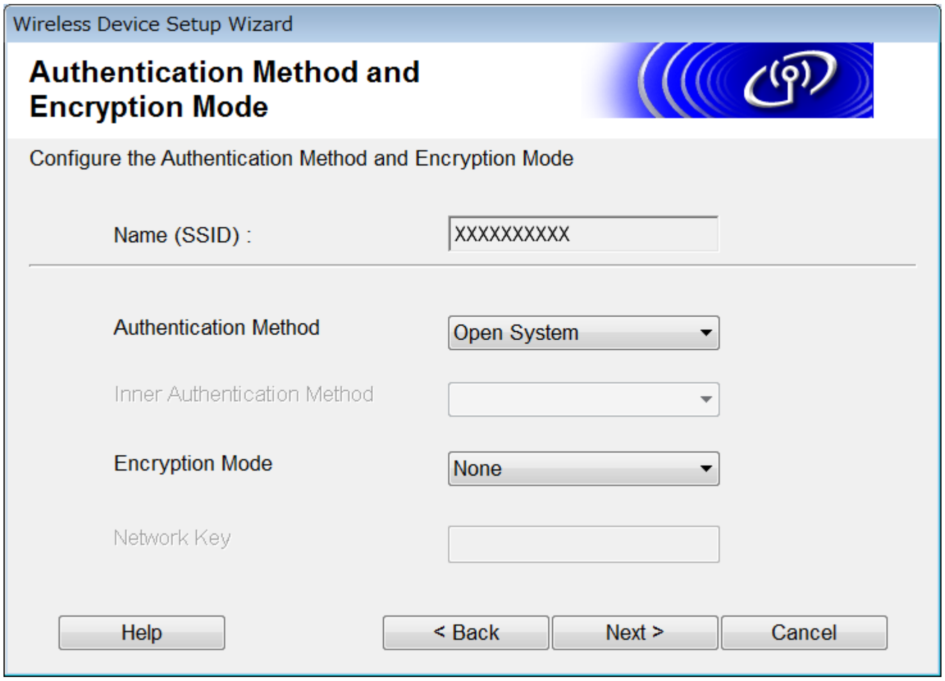
Configure the wireless network name that the device will be associated with.

Name(SSID) XXXXXXXX

☑ This is an Ad-hoc network and there is no access point.

Channel 2

8 Select the **Authentication Method** and **Encryption Mode** from the drop-down lists, type a network key in the **Network Key** field, and then click **Next**.


Wireless Device Setup Wizard

Authentication Method and Encryption Mode

Configure the Authentication Method and Encryption Mode

Name (SSID) : XXXXXXXXXX

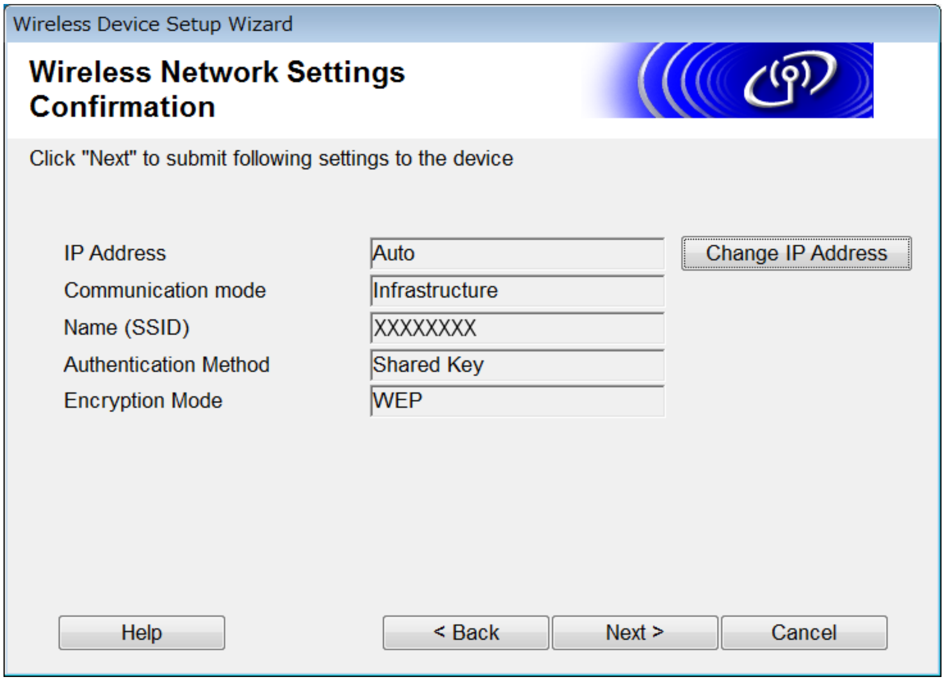
Authentication Method Open System

Inner Authentication Method

Encryption Mode None

Network Key

9 Click **Next**. The machine receives the settings. (Encryption Mode is WEP in the following example.)



Wireless Device Setup Wizard

Wireless Network Settings Confirmation

Click "Next" to submit following settings to the device

IP Address: Auto

Communication mode: Infrastructure

Name (SSID): XXXXXXXX

Authentication Method: Shared Key

Encryption Mode: WEP

10 Disconnect the USB cable between the computer and the machine.

11 Click **Finish**.

Configure Your Machine for a Wireless Network Using the Machine’s Control Panel Setup Wizard

Before configuring your machine, we recommend writing down your wireless network settings. You will need this information to proceed with the configuration.

1. Check and write down the current wireless network settings of the computer to which you are connecting.

Network Name (SSID)

Network Key

For example:

Network Name (SSID)
HELLO

Network Key
12345

NOTE

- Your access point/router may support the use of multiple WEP keys, however your Brother machine supports the use of the first WEP key only.
- If you need assistance during setup and want to contact Brother Customer Service, make sure you have your SSID (Network Name) and Network Key ready. We cannot help you find this information.
- You must know this information (SSID and Network Key) to continue the wireless setup.

  How can I find this information?

  a Check the documentation provided with your wireless access point/router.

  b The initial SSID could be the manufacturer’s name or the model name.

  c If you do not know the security information, please consult the router manufacture, your system administrator, or your Interner provider.

2. On your Brother machine’s LCD, press 🛠 > `Network` > `WLAN` > `Setup Wizard`.
3. The machine searches for your network, and then displays a list of available SSIDs.
   When a list of SSIDs is displayed, press ▲ or ▼ to display the SSID you want to connect to, and then press the SSID.
4. Press `OK`.

5 Do one of the following:

- If you are using an authentication and encryption method that requires a Network Key, enter the Network Key you wrote down in the first step.
  When you have entered all the characters, press `OK`, and then press `Yes` to apply your settings.
- If your authentication method is Open System and your encryption mode is `None`, go to the next step.
- If your WLAN access point/router supports WPS, `The selected access point/router supports WPS. Use WPS?` appears. To connect your machine using the automatic wireless mode, press `Yes`. (If you selected `No (Manual)`, enter the Network Key you wrote down in the first step.)
  When `Start WPS on your wireless access point/router, then press [Next].` appears, press the WPS button on your WLAN access point/router, and then press `Next`.

6 The machine attempts to connect to the wireless device you selected.

If your wireless device is connected successfully, the machine's LCD displays `Connected`.

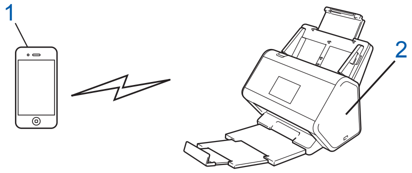
You have completed the wireless network setup. To install the drivers and software necessary for operating your machine, insert the installation DVD-ROM into your computer's drive or go to your model's **Downloads** page on the Brother Solutions Center at support.brother.com

Use Wi-Fi Direct®

- Scan from Your Mobile Device Using Wi-Fi Direct®
- Configure Your Wi-Fi Direct® Network
- Configure Your Wi-Fi Direct® Network Settings from Your Machine's Control Panel

Scan from Your Mobile Device Using Wi-Fi Direct®

Wi-Fi Direct® is one of the wireless configuration methods developed by the Wi-Fi Alliance®. It allows you to configure a secured wireless network between your Brother machine and a mobile device, such as an Android™ device, Windows® Phone device, iPhone, iPod touch, or iPad, without using an access point. Wi-Fi Direct® supports wireless network configuration using the one-push method or PIN Method of Wi-Fi Protected Setup™ (WPS). You can also configure a wireless network by manually setting an SSID and password. Your Brother machine's Wi-Fi Direct® feature supports WPA2™ security with AES encryption.



1 Mobile device

2 Your Brother machine

NOTE

- Although the Brother machine can be used in both a wired and wireless network, only one connection method can be used at a time. However, a wireless network connection and Wi-Fi Direct® connection, or a wired network connection and Wi-Fi Direct® connection can be used at the same time.
- The Wi-Fi Direct®-supported device can become a Group Owner (G/O). When configuring the Wi-Fi Direct® network, the G/O serves as an access point.
- Ad-hoc mode and Wi-Fi Direct® cannot be used at the same time. Disable one function to enable the other. To use Wi-Fi Direct® while you are using Ad-hoc mode, set Network I/F to "Wired LAN" or disable Ad-hoc mode and connect your Brother machine to the access point.

Configure Your Wi-Fi Direct® Network

Configure your Wi-Fi Direct® network settings from your machine’s control panel.

- Wi-Fi Direct® Network Configuration Overview

  The following instructions offer five methods for configuring your Brother machine in a wireless network environment. Select the method you prefer for your environment.

- Configure Your Wi-Fi Direct® Network Using the One-Push Method
- Configure Your Wi-Fi Direct® Network Using the One-Push Method of Wi-Fi Protected Setup™ (WPS)
- Configure Your Wi-Fi Direct® Network Using the PIN Method
- Configure Your Wi-Fi Direct® Network Using the PIN Method of Wi-Fi Protected Setup™ (WPS)
- Configure Your Wi-Fi Direct® Network Manually

Wi-Fi Direct® Network Configuration Overview

The following instructions offer five methods for configuring your Brother machine in a wireless network environment. Select the method you prefer for your environment.

Check your mobile device for configuration.

1 Does your mobile device support Wi-Fi Direct®?

Option	Description
Yes	Go to Step ❷.
No	Go to Step ❸.

2 Does your mobile device support the one-push method for Wi-Fi Direct®?

Option	Description
Yes	See *Configure Your Wi-Fi Direct® Network Using the One-Push Method* on page 33.
No	See *Configure Your Wi-Fi Direct® Network Using the PIN Method* on page 34.

3 Does your mobile device support Wi-Fi Protected Setup™ (WPS)?

Option	Description
Yes	Go to Step ❹.
No	See *Configure Your Wi-Fi Direct® Network Manually* on page 37.

4. Does your mobile device support the one-push method for Wi-Fi Protected Setup™ (WPS)?

Option	Description
Yes	See *Configure Your Wi-Fi Direct® Network Using the One-Push Method of Wi-Fi Protected Setup™ (WPS)* on page 34.
No	See *Configure Your Wi-Fi Direct® Network Using the PIN Method of Wi-Fi Protected Setup™ (WPS)* on page 35.

To use the Brother iPrint&Scan functionality in a Wi-Fi Direct® network configured by one-push method or by PIN Method configuration, the device you use to configure Wi-Fi Direct® must be running Android™ 4.0 or greater.

Configure Your Wi-Fi Direct® Network Using the One-Push Method

If your mobile device supports Wi-Fi Direct®, follow these steps to configure a Wi-Fi Direct® network.

NOTE

When the machine receives the Wi-Fi Direct® request from your mobile device, the message `Wi-Fi Direct connection request received. Press [OK] to connect.` appears on the LCD. Press `OK` to connect.

1. Press 🛠 > `Network` > `Wi-Fi Direct` > `Push Button`.
2. Activate Wi-Fi Direct® on your mobile device (see your mobile device's user's guide for instructions) when `Activate Wi-Fi Direct on other device. Then Press [OK].` appears on the machine's LCD. Press `OK` on your machine to start the Wi-Fi Direct® setup. To cancel, press ✖.
3. Do one of the following:
   - When your Brother machine is the Group Owner (G/O), connect your mobile device to the machine directly.
   - When your Brother machine is not the G/O, it displays the names of the devices that allow you to configure a Wi-Fi Direct® network. Select the mobile device you want to connect to and press `OK`. Search for the available devices again by pressing `Rescan`.
4. If your mobile device connects successfully, the machine's LCD displays `Connected`. You have now completed the Wi-Fi Direct® network setup.

Configure Your Wi-Fi Direct® Network Using the One-Push Method of Wi-Fi Protected Setup™ (WPS)

If your mobile device supports WPS (PBC: Push Button Configuration), follow these steps to configure a Wi-Fi Direct® network.

NOTE

When the machine receives the Wi-Fi Direct® request from your mobile device, the message Wi-Fi Direct connection request received. Press [OK] to connect. appears on the LCD. Press OK to connect.

1. Press 🛠 > Network > Wi-Fi Direct > Group Owner.
2. Press On.
3. Swipe up or down or press ▲ or ▼ to select the Push Button option. Press Push Button.
4. When Wi-Fi Direct On? appears, press On to accept. To cancel, press Off.
5. Activate your mobile device's WPS one-push configuration method (see your mobile device's user's guide for instructions) when Activate Wi-Fi Direct on other device. Then Press [OK]. appears on the machine's LCD. Press OK on your Brother machine.

   This will start the Wi-Fi Direct® setup. To cancel, press ✕.
6. If your mobile device connects successfully, the machine's LCD displays Connected.
   You have completed the Wi-Fi Direct® network setup.

Configure Your Wi-Fi Direct® Network Using the PIN Method

If your mobile device supports the PIN Method of Wi-Fi Direct®, follow these steps to configure a Wi-Fi Direct® network:

NOTE

When the machine receives the Wi-Fi Direct® request from your mobile device, the message Wi-Fi Direct connection request received. Press [OK] to connect. appears on the LCD. Press OK to connect.

1. Press 🛠 > Network > Wi-Fi Direct > PIN Code.
2. When Wi-Fi Direct On? appears, press On to accept. To cancel, press Off.
3. Activate Wi-Fi Direct® on your mobile device (see your mobile device's user's guide for instructions) when Activate Wi-Fi Direct on other device. Then Press [OK]. appears on the machine's LCD. Press OK on your machine to start the Wi-Fi Direct® setup. To cancel, press ✕.

4. Do one of the following:

   - If your Brother machine is the Group Owner (G/O), it waits for a connection request from your mobile device. When `PIN Code` appears, enter the PIN displayed on your mobile device in the machine. Press `OK` to complete the setup.

     If the PIN is displayed on your Brother machine, enter the PIN on your mobile device.

   - If your Brother machine is not the G/O, it displays the names of the devices that allow you to configure a Wi-Fi Direct® network. Select the mobile device you want to connect to and press `OK`.

     Search for the available devices again by pressing `Rescan`.

5. Do one of the following:

   - Press `Display PIN Code` to display the PIN on your machine and enter the PIN on your mobile device. Go to the next step.

   - Press `Input PIN Code` to enter a PIN displayed by your mobile device on the machine, and then press `OK`. Go to the next step.

     If your mobile device does not display a PIN, press ⌂ on your Brother machine.

     Go back to the first step and try again.

6. If your mobile device connects successfully, the machine's LCD displays `Connected`.
   You have completed the Wi-Fi Direct® network setup.

Configure Your Wi-Fi Direct® Network Using the PIN Method of Wi-Fi Protected Setup™ (WPS)

If your mobile device supports the PIN Method of Wi-Fi Protected Setup™ (WPS), follow these steps to configure a Wi-Fi Direct® network.

NOTE

When the machine receives the Wi-Fi Direct® request from your mobile device, the message `Wi-Fi Direct connection request received. Press [OK] to connect.` appears on the LCD. Press `OK` to connect.

1. Press 🔧 > `Network` > `Wi-Fi Direct` > `Group Owner`.
2. Press `On`.
3. Swipe up or down or press ▲ or ▼ to select the `PIN Code` option. Press `PIN Code`.
4. When `Wi-Fi Direct On?` appears, press `On` to accept. To cancel, press `Off`.
5. When `Activate Wi-Fi Direct on other device. Then Press [OK].` appears, activate your mobile device's WPS PIN configuration method (see your mobile device's user's guide for instructions), and then press `OK` on your Brother machine.
   The Wi-Fi Direct® setup starts. To cancel, press ✕.

6. The machine waits for a connection request from your mobile device. When `PIN Code` appears, enter the PIN displayed on your mobile device on the machine. Press `OK`.

7. If your mobile device connects successfully, the machine's LCD displays `Connected`.
   You have now completed the Wi-Fi Direct® network setup.

Configure Your Wi-Fi Direct® Network Manually

If your mobile device does not support Wi-Fi Direct® or WPS, you must configure a Wi-Fi Direct® network manually.

NOTE

When the machine receives the Wi-Fi Direct® request from your mobile device, the message `Wi-Fi Direct connection request received. Press [OK] to connect.` appears on the LCD. Press `OK` to connect.

1. Press 🛠 > `Network` > `Wi-Fi Direct` > `Manual`.
2. When `Wi-Fi Direct On?` appears, press `On` to accept. To cancel, press `Off`.
3. The machine displays the SSID name and Password for two minutes. Go to your mobile device's wireless network settings screen and enter the SSID name and password.
4. If your mobile device connects successfully, the machine's LCD displays `Connected`.
   You have completed the Wi-Fi Direct® network setup.

4 Web Based Management

Overview

A standard web browser can be used to manage your machine from a computer on your network using the Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

- Obtain status information, maintenance information, and software version information for your Brother machine and scan server.
- Change network and machine configuration details (see *Configure Your Machine Settings* on page 39).
- Configure settings to restrict unauthorized access from others.
  - See *Set a Login Password* on page 40.
  - See *Configure Active Directory LDAP Authentication (ADS-2800W / ADS-3600W)* on page 43.
- Configure/Change network settings.
  - See *Change the Scan to FTP Configuration* on page 49.
  - See *Change the Scan to SFTP Configuration* on page 50.
  - See *Change the Scan to Network Configuration (Windows®)* on page 52.
  - See *Synchronize with the SNTP Server* on page 47.
  - See *LDAP Operation (ADS-2800W / ADS-3600W)* on page 44.
  - See *Configure TCP/IP Advanced Settings* on page 56.
- Address Book Import/Export. (See *Address Book Import/Export (ADS-2800W / ADS-3600W)* on page 58.)

NOTE

We recommend Microsoft® Internet Explorer® 8.0/10.0/11.0 for Windows® and Safari 8.0 for Macintosh. Make sure your web browser has both Javascript and cookies enabled. If you are using a different web browser, make sure it is compatible with HTTP 1.0 and HTTP 1.1.

You must use the TCP/IP protocol on your network, and have a valid IP address registered to the scan server and your computer.

Configure Your Machine Settings

1. Start Web Based Management.

   a Start your web browser.

   b In your browser’s address bar, type the IP address of your machine.
   For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as “SharedScanner” instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    http://brwxxxxxxxxxxxx/

  You can find the NetBIOS name on your machine’s control panel under `Node Name`.
- To use the secure HTTPS protocol for configuring settings using Web Based Management, you must configure a CA certificate before starting Web Based Management. See *Manage Multiple Certificates* on page 69.

2. No password is required by default. Type the password if you have set one, and then click →.

3. You can now configure your machine settings.

NOTE

If you have changed the protocol settings, restart your Brother machine after clicking **Submit** to activate the configuration.

Set a Login Password

We recommend setting a login password to prevent unauthorized access to Web Based Management.

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click the **Administrator** tab, and then click **Login Password** in the left navigation bar.
3. Type the password you want to use (up to 32 characters).
4. Retype the password in the **Confirm New Password** field.
5. Click **Submit**.
   The next time you access Web Based Management, type the password in the **Login** box, and then click →.
   When finished, log off by clicking →.

NOTE

You can also set a Login Password by clicking **Please configure the password** in Web Based Management.

Use LDAP Authentication

Introduction to LDAP Authentication

LDAP Authentication restricts the use of your Brother machine. If LDAP Authentication is enabled, the machine’s control panel will be locked. You cannot change the machine’s settings until you enter a user ID and password.

- Obtains email address depending on the user ID from LDAP server when sending scanned data to an email server.
  To use this feature, select the **Get Mail Address** option. Your email address will be set as the sender when the machine sends scanned data to an email server, or as the recipient if you want to send the scanned data to your email address.

You can change the LDAP Authentication settings using Web Based Management or BRAdmin Professional 3 (Windows®).

Configure LDAP Authentication using Web Based Managament

1. Start your web browser.
2. Type “http://machines’s IP address” in your browser’s address bar (where “machines’s IP address” is the machines’s IP address).
   For example:
   http://192.168.1.2
3. Click the **Administrator** tab.
4. Click the **User Restriction Function** menu in the left navigation bar.
5. Select **LDAP Authentication**.
6. Click **Submit**.
7. Select **LDAP Authentication** in the left navigation bar.

8 Configure the following settings:

Option	Description
Remember User ID	Select this option to save your user ID.
LDAP Server Address	Type the IP address or the server name (for example: ad.example.com) of the LDAP Server.
Get Mail Address	Select this option to obtain your machine's email address from LDAP server.
LDAP Server Port	Type the LDAP server port number.
LDAP Search Root	Type the LDAP search root.
Attribute of Name (Search Key)	Type the attribute you want to use as a search key.

9 Click **Submit**.

Log on to change the Machine Settings using the Machine's Control Panel

NOTE

When LDAP Authentication is enabled, the machine's control panel will be locked until you enter your User ID and password on the machine's control panel.

1 On the machine's control panel, use the Touchscreen to enter your User ID and Password.

2 Press `OK`.

3 When authentication is successful, the machine's control panel will be unlocked.

Restrict Users

Configure Active Directory LDAP Authentication (ADS-2800W / ADS-3600W)

Active Directory Authentication restricts the use of your Brother machine. When Active Directory Authentication is enabled, the machine's control panel is locked. To use scan functions, enter a user ID, domain name and password.

NOTE

- Active Directory Authentication supports Kerberos authentication.
- You must configure Simple Network Time Protocol (SNTP) (Network time server) first.

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. Click the **Administrator** tab.
3. Click the **User Restriction Function** menu in the left navigation bar.
4. Select **Active Directory Authentication**.
5. Click **Submit**.
6. Select **Active Directory Authentication** in the left navigation bar.
7. Configure the following settings:

   - **Remember User ID**

     Select this option to save your user ID.

   - **Active Directory Server Address**

     Type the IP address or the server name (for example: "ad.example.com") of the Active Directory Server.

   - **Active Directory Domain Name**

     Type the Active Directory domain name.

   - **Protocol & Authentication Method**

     Select the protocol and authentication method.

   - **Get Mail Address**

     Select this option to obtain your machine's email address from the LDAP server (available only for the **LDAP + kerberos** authentication method).

   - **Get User's Home Directory**

     Select this option to obtain your home directory and set it as the Scan to Network destination.

   - **LDAP Server Port**

     Type the LDAP server port number (available only for the **LDAP + kerberos** authentication method).

- **LDAP Search Root**

  Type the LDAP search root (available only for the **LDAP + kerberos** authentication method).
- **Fetch DNS**

  Follow the on-screen instructions.
- **SNTP**

  See page 47 for more information about the SNTP protocol.

8. Click **Submit**.

Unlock the Machine when Active Directory Authentication is Enabled

1. On the machine's LCD, use the Touchscreen to enter your `User ID`, and `Password`.
2. Press `OK`.
3. When your data is authenticated, the control panel unlocks, allowing you to use Scan functions.

NOTE

You cannot change any settings if **Active Directory Authentication** is enabled.

LDAP Operation (ADS-2800W / ADS-3600W)

The LDAP protocol allows you to search for email addresses from your server using the Scan to E-mail server function.

Changing LDAP Configuration

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. Click **Network** on the machine's web page.
3. Click **Protocol** in the left navigation bar.
4. Select the **LDAP** check box, and then click **Submit**.
5. Restart your Brother machine to activate the configuration.
6. On your computer, in Web Based Management's **Address Book** tab, select **LDAP** in the left navigation bar.
7. Configure the following LDAP settings:
   - **LDAP Server Address**
   - **Port** (The default port number is 389.)
   - **Search Root**
   - **Authentication**

- **Username**

  The availability of this selection depends on the authentication method used.
- **Password**

  The availability of this selection depends on the authentication method used.
- **Kerberos Server Address**

  The availability of this selection depends on the authentication method used.
- **SNTP**
- **Timeout for LDAP**
- **Attribute of Name (Search Key)**
- **Attribute of Email**

8. When finished, click **Submit**. Make sure the **Status** is **OK** on the Test Result page.

NOTE

- The LDAP Protocol does not support simplified Chinese, traditional Chinese and Korean.
- If the LDAP server supports Kerberos Authentication, we recommend selecting Kerberos for the **Authentication** setting. It provides strong authentication between the LDAP server and your machine. You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly on your machine's control panel for Kerberos Authentication. (For information about setting SNTP, see *Synchronize with the SNTP Server* on page 47.)

Changing LDAP Configuration Using Your Machine's Control Panel (ADS-2800W / ADS-3600W)

After you configure LDAP settings, use the LDAP search from your machine to find email addresses.

1. Load the document you want to scan and email into your machine.
2. On the machine's LCD, press `to E-mail Server`.
3. Press `Address Book`.
4. Press 🔍 to search.
5. Enter the initial characters for your search using the buttons on the LCD.

NOTE

- You can enter up to 15 characters.
- For more information on how to enter text, see *Entering Text (ADS-2800W / ADS-3600W)* in the *User's Guide*.

6. Press OK.
   The LDAP search results appear on the LCD with 💻 before results from the local address book. If there is no match on the server and the local address book, the LCD displays Results cannot be found.
7. Press ▲ or ▼ to scroll until you find the name you want, and then press the name.
8. If the result includes more than one email address, press the email address you want.
9. Press Apply.
10. Press OK.

NOTE

Press Options to adjust your scan settings before scanning the document.

11. Press Start.

NOTE

- The LDAP function of this machine supports LDAPv3.
- For more information, click ? on the right side of the LDAP setting screen.

Synchronize with the SNTP Server

Simple Network Time Protocol (SNTP) is used to synchronize the time used by the machine for authentication with the SNTP time server (this is not the time displayed on the machine's LCD). You can regularly synchronize the machine's time with the Coordinated Universal Time (UTC) provided by the SNTP time server.

NOTE

- This function is not available in some countries.
- Except for Date&Time, the SNTP functionality will work without changing any initial settings.

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click **Network**, and then click the **Protocol** menu in the left navigation bar.
3. Select the **SNTP** check box.
4. Click **Advanced Setting**.

   - **Status**

     Displays whether the SNTP server settings are enabled or disabled.

   - **Synchronization Status**

     Confirm the latest synchronization status.

   - **SNTP Server Method**

     Select **AUTO** or **STATIC**.

     - **AUTO**

       If you have a DHCP server on your network, the SNTP server automatically obtains the address from that server.

     - **STATIC**

       Type the address you want to use.

   - **Primary SNTP Server Address**, **Secondary SNTP Server Address**

     Type the server address (up to 64 characters).

     The Secondary SNTP server address is used as a backup to the Primary SNTP server address. If the Primary server is unavailable, the machine will contact the Secondary SNTP server.

   - **Primary SNTP Server Port**, **Secondary SNTP Server Port**

     Type the Port number (between 1 and 65535).

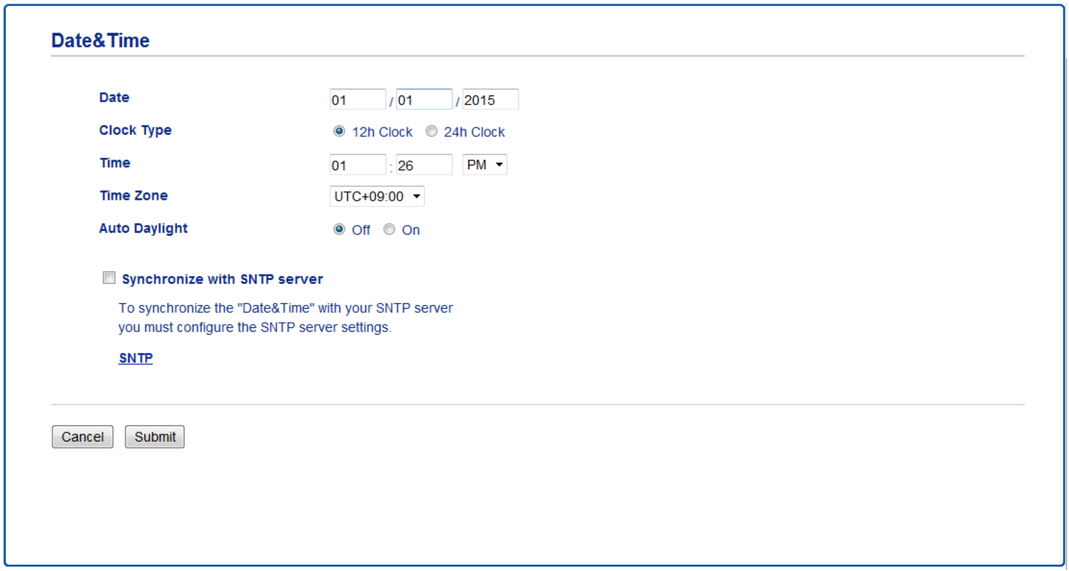
     The Secondary SNTP server port is used as a backup to the Primary SNTP server port. If the Primary port is unavailable, the machine will contact the Secondary SNTP port.

- **Synchronization Interval**

  Type the number of hours between server synchronization attempts (between 1 and 168 hours).

NOTE

- You must configure **Date&Time** to synchronize the time used by the machine with the SNTP time server. Click **Date&Time**, and then configure **Date&Time** on the **General** screen.



Date&Time

Date: 01 / 01 / 2015

Clock Type: ● 12h Clock ○ 24h Clock

Time: 01 : 26 PM

Time Zone: UTC+09:00

Auto Daylight: ● Off ○ On

□ Synchronize with SNTP server

To synchronize the "Date&Time" with your SNTP server you must configure the SNTP server settings.

SNTP

- Select the **Synchronize with SNTP server** check box. Verify your time zone settings, and select the time difference between your location and UTC from the **Time Zone** drop-down list. For example, the time zone for Eastern Time in the USA and Canada is UTC-5, the UK is UTC and Central European Time is UTC+1.

5 Click **Submit**.

Change the Scan to FTP Configuration

Scan to FTP allows you to scan a document directly to an FTP server on your local network or on the Internet. For more information about Scan to FTP, see *Scan Documents to an FTP Server* in the *User's Guide*.

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click the **Scan** tab, and then click **Scan to FTP/SFTP/Network/SharePoint** in the left navigation bar.
3. Select the **FTP** checkbox in the profile numbers (from 1 to 25).
4. Click **Submit**.
5. Click **Scan to FTP/SFTP/Network/SharePoint Profile** in the left navigation bar.
6. Click the **FTP** of the Profile No. you selected in step ❸
   You can configure the following Scan to FTP settings:
   - **Profile Name** (up to 15 characters)
   - **Host Address**
   - **Username**
   - **Password**
   - **Store Directory**
   - **File Name**
   - **Quality**
   - **Auto Color detect adjust**
   - **File Type**
   - **Password for Secure PDF** (ADS-2400N / ADS-3000N)
   - **Document Size**
   - **Margin Settings**
   - **File Size**
   - **Auto Deskew**
   - **Skip Blank Page**
   - **Skip blank page sensitivity**
   - **2-sided Scan**
   - **Brightness**
   - **Contrast**
   - **Continuous Scan** (ADS-2800W / ADS-3600W)
   - **Passive Mode**
   - **Port Number**

   Set **Passive Mode** to **Off** or **On** depending on your FTP server and network firewall configuration. By default, this setting is **On**. You can also change the port number used to access the FTP server. The default for this setting is port 21. In most cases, these two settings can remain set as default.
7. Click **Submit**.

Change the Scan to SFTP Configuration

Scan to SFTP allows you to scan a document directly to an SFTP server on your local network or on the Internet. For more information about Scan to SFTP, see *Scan Documents to an SFTP Server* in the *User's Guide*.

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click the **Scan** tab, and then click **Scan to FTP/SFTP/Network/SharePoint** in the left navigation bar.
3. Select the **SFTP** checkbox in the profile numbers (from 1 to 25).
4. Click **Submit**.
5. Click **Scan to FTP/SFTP/Network/SharePoint Profile** in the left navigation bar.
6. Click the **SFTP** of Profile No. you selected in step ❸
   You can configure the following Scan to SFTP settings:
   - **Profile Name** (up to 15 characters)
   - **Host Address**
   - **Username**
   - **Auth. Method**
   - **Password**
   - **Client Key Pair**
   - **Server Public Key**
   - **Store Directory**
   - **File Name**
   - **Quality**
   - **Auto Color detect adjust**
   - **File Type**
   - **Password for Secure PDF** (ADS-2400N / ADS-3000N)
   - **Document Size**
   - **Margin Settings**
   - **File Size**
   - **Auto Deskew**
   - **Skip Blank Page**
   - **Skip blank page sensitivity**
   - **2-sided Scan**
   - **Brightness**
   - **Contrast**

- **Continuous Scan** (ADS-2800W / ADS-3600W)
- **Port Number**

You can change the port number used to access the SFTP server.
The default for this setting is port 21. In most cases, this setting can remain set as default.

7 Click **Submit**.

Change the Scan to Network Configuration (Windows®)

Scan to Network allows you to scan documents directly to a shared folder located on your local network or the Internet. For more information about Scan to Network, see *Scan Documents to a Shared Folder / Network Location (Windows®)* in the *User's Guide*.

NOTE

Scan to Network supports NTLMv2 Authentication.

You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly on the machine's control panel for authentication. (For information about setting SNTP, see *Synchronize with the SNTP Server* on page 47. For information about setting the date, time and time zone, see the *User's Guide*.)

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click the **Scan** tab, and then click **Scan to FTP/SFTP/Network/SharePoint** in the left navigation bar.
3. Select the **Network** checkbox in the profile numbers (from 1 to 25).
4. Click **Submit**.
5. Click **Scan to FTP/SFTP/Network/SharePoint Profile** in the left navigation bar.
6. Click the **Network** of Profile No. you selected in step ❸
   You can configure the following Scan to Network settings:
   - **Profile Name** (up to 15 characters)
   - **Network Folder Path**
   - **File Name**
   - **Quality**
   - **Auto Color detect adjust**
   - **File Type**
   - **Password for Secure PDF** (ADS-2400N / ADS-3000N)
   - **Document Size**
   - **Margin Settings**
   - **File Size**
   - **Auto Deskew**
   - **Skip Blank Page**
   - **Skip blank page sensitivity**
   - **2-sided Scan**
   - **Brightness**
   - **Contrast**
   - **Continuous Scan** (ADS-2800W / ADS-3600W)

- **Use PIN for Authentication**
- **PIN Code**
- **Auth. Method**
- **Username**
- **Password**
- **Date&Time**

7 Click **Submit**.

Change the Scan to SharePoint Configuration (Windows$^{®}$)

SharePoint

Scan documents directly to a SharePoint server when you need to share the scanned document. For added convenience, configure different profiles to save your favorite Scan to SharePoint destinations. For more information about Scan to SharePoint, see *Scan Documents to SharePoint* in the *User's Guide*.

NOTE

Scan to Sharepoint supports NTLMv2 Authentication.

You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly on the machine's control panel for authentication. (For information about setting SNTP, see *Synchronize with the SNTP Server* on page 47. For information about setting the date, time and time zone, see the *User's Guide*.)

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. When the Web Based Management screen appears, click the **Scan** tab, and then click **Scan to FTP/SFTP/Network/SharePoint** in the left navigation bar.
3. Select the **SharePoint** checkbox in the profile numbers (from 1 to 25).
4. Click **Submit**.
5. Click **Scan to FTP/SFTP/Network/SharePoint Profile** in the left navigation bar.
6. Click the **SharePoint** of Profile No. you selected in step ❸.
   You can configure the following Scan to Sharepoint settings:
   - **Profile Name** (up to 15 characters)
   - **SharePoint Site Address**
   - **SSL/TLS**

NOTE

SSL/TLS appears only when you select **HTTPS** in the **Sharepoint Site Address**.

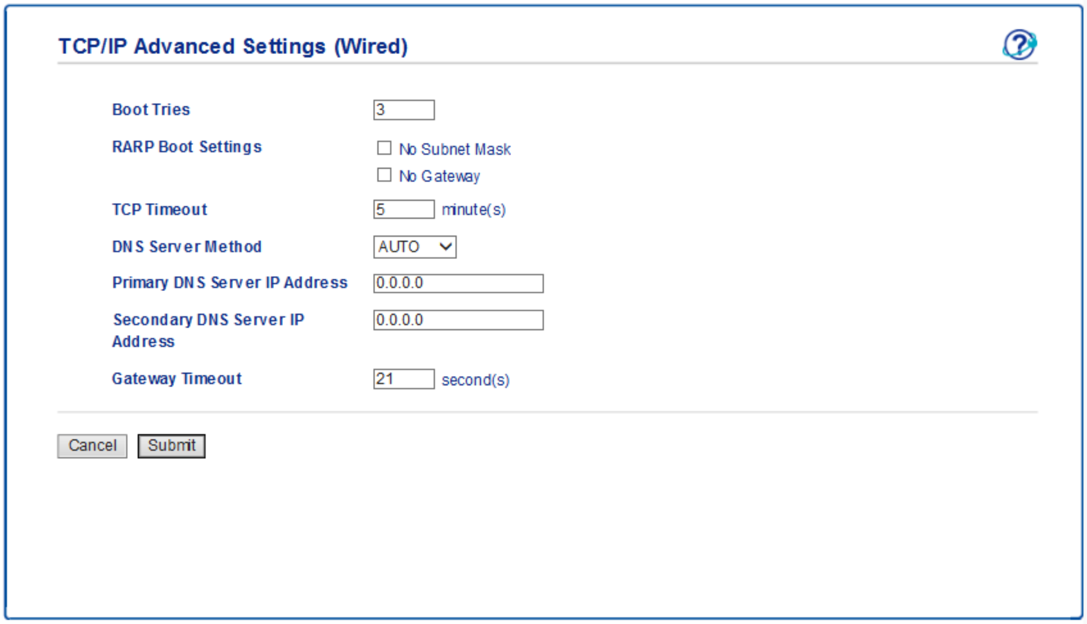
- **File Name**
- **Quality**
- **Auto Color detect adjust**
- **File Type**
- **Password for Secure PDF** (ADS-2400N / ADS-3000N)
- **Document Size**
- **Margin Settings**
- **File Size**
- **Auto Deskew**
- **Skip Blank Page**

- **Skip blank page sensitivity**
- **2-sided Scan**
- **Brightness**
- **Contrast**
- **Continuous Scan** (ADS-2800W / ADS-3600W)
- **Use PIN for Authentication**
- **PIN Code**
- **Auth. Method**
- **Username**
- **Password**
- **Date&Time**

7 Click **Submit**.

Configure TCP/IP Advanced Settings

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. Click the **Network** tab, and then select your connection type (**Wired** or **Wireless**).
3. Select **TCP/IP** in the left navigation menu.
4. Click **Advanced Settings**. Configure the following settings: (the example below uses **TCP/IP Advanced Settings (Wired)**).



TCP/IP Advanced Settings (Wired)

Boot Tries: 3

RARP Boot Settings: □ No Subnet Mask □ No Gateway

TCP Timeout: 5 minute(s)

DNS Server Method: AUTO

Primary DNS Server IP Address: 0.0.0.0

Secondary DNS Server IP Address: 0.0.0.0

Gateway Timeout: 21 second(s)

- **Boot Tries**

  Type the number of times to attempt start up using the Boot method (between 0 and 32767).

- **RARP Boot Settings**

  Select **No Subnet Mask** or **No Gateway**.

  - **No Subnet Mask**

    Subnet Mask is not changed automatically.

  - **No Gateway**

    Gateway Address is not changed automatically.

- **TCP Timeout**

  Type the number of minutes before TCP Timeout (between 0 and 32767).

- **DNS Server Method**

  Select **AUTO** or **STATIC**.

- **Primany DNS Server IP Address**, **Secondary DNS Server IP Address**

  Type the server’s IP address.

  The Secondary DNS server IP Address is used as a backup to the Primary DNS server IP address. If the Primary DNS server is unavailable, the machine will contact the Secondary DNS server.

- **Gateway Timeout**

  Type the number of seconds before the router times out (between 1 and 32767).

5 Click **Submit**.

Address Book Import/Export (ADS-2800W / ADS-3600W)

Address Book Import

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. Click the **Address Book** tab.
3. Select **Import** in the left navigation menu.
4. Input **“Address Book” data file** or **“Group” data file**.
5. Click **Submit**.

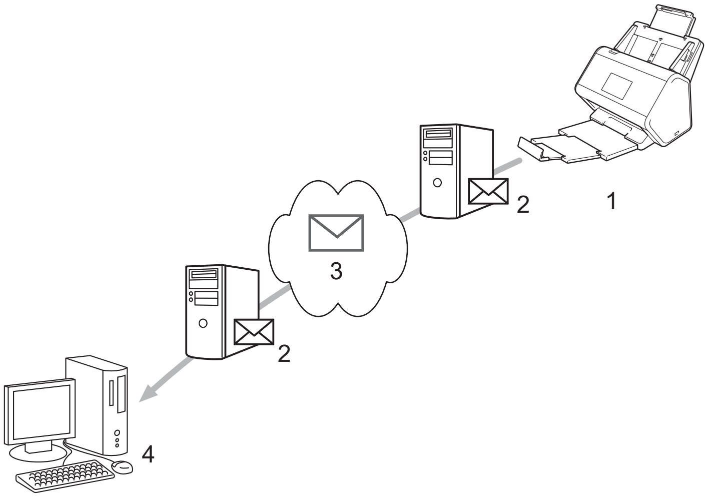
Address Book Export

1. Start Web Based Management and access your Brother machine (see step ❶ on page 39).
2. Click the **Address Book** tab.
3. Select **Export** in the left navigation menu.
4. Click the **Export to file** button.

5 Scan to E-mail Server (ADS-2800W / ADS-3600W)

Overview

The Scan to E-mail Server function allows you to send scanned documents as attachments via email.



1 Sender

2 Email server

3 Internet

4 Receiver

Size Restrictions When Using Scan to E-mail Server

If a document’s image data is too large, transmission may be unsuccessful.

Configure the Scan to E-mail Server Settings

Before using the Scan to E-mail Server function, you must configure your Brother machine to communicate with your network and your email server. You can configure these items using Web Based Management, Remote Setup, or BRAdmin Professional 3. You must ensure that the following items are configured on your machine:

- IP address (If you are already using your machine on your network, the machine's IP address has been configured correctly.)
- Email address
- SMTP server address/port/Authentication method/Encryption method/Server Certificate Verification
- SMTP-AUTH Account Name and password

If you are unsure of any of these items, contact your network administrator.

NOTE

Although you must configure an email address on your machine, the machine does not have an email receiving function. Therefore, if the recipient replies to an email sent from your machine, the machine cannot receive it.

Before Scanning to E-mail Server

You may have to configure the following items (using Web Based Management or Remote Setup):

- Sender Subject
- Size Limit
- Notification (for more information, see *Transmission (TX) Verification Mail* on page 62.)

How to Scan to E-mail Server

1. Load your document.
2. Swipe left or right, or press ◀ or ▶ to display `to E-mail Server`.
3. Select the email address you want to use, and then press `OK`.
4. Press `Start`.

For more information about email settings, see *Send Scanned Documents Directly to an Email Address (ADS-2800W / ADS-3600W)* in the *User's Guide*.

After the document is scanned, it is sent to the specified email address automatically via your SMTP server. When finished, the machine's LCD displays the Home screen.

NOTE

Some email servers do not allow you to send large email documents (the system administrator may often limit the maximum email size). With the Scan to E-mail Server function enabled, the machine will display `Out of Memory` when trying to send email documents over 1 Mbyte in size, and the document will not be sent. Divide your document into smaller documents that will be accepted by the mail server.

Additional Scan to E-mail Server Features

Transmission (TX) Verification Mail

Use TX Verification Mail to request notification from the destination computer that your email was received and processed.

Setup Mail TX

Use your machine's control panel to turn the verification feature on. When `Setup Mail TX` is `On`, your email contains an additional field that is automatically populated with the email's arrival date and time.

1. On your machine's LCD, press 🛠.
2. Press `Network`.
3. Press `E-mail`.
4. Press `Setup Mail TX`.
5. Press `Notification`.
6. Press `On` (or `Off`).

NOTE

- Message Disposition Notification (MDN)
  This field requests the status of the email message after delivery through the Simple Mail Transfer Protocol (SMTP) transport system. Once the recipient has received the message, this data is used when the machine or user reads the received email. For example, if the message is opened and read, the receiver sends back a notification to the original sending machine or user.
  The recipient must activate the MDN field to be able to send a notification report; otherwise the request will be ignored.
- This Brother machine cannot receive email messages. To use the TX Verification feature, you must redirect the return notification to a different email address. Configure the email address using the machine's LCD. Press `Network` > `E-mail` > `Mail Address`, and then enter the email address that you want to receive the notification.

6 Security Features

Overview

Your Brother machine employs some of the latest network security and encryption protocols available. These network features can be integrated into your overall network security plan to help protect your data and prevent unauthorized access to the machine.

You can configure the following security features:

- Send an email securely (see *Send an Email Securely (ADS-2800W / ADS-3600W)* on page 64)
- Manage multiple certificates (see *Manage Multiple Certificates* on page 69)
- Create a Client Key Pair (see *Create a Client Key Pair* on page 66)
- Export a Client Key Pair (see *Export a Client Key Pair* on page 67)
- Import a Server Public Key (see *Import a Server Public Key* on page 68)
- Manage Your Network Machine Securely Using IPsec (see *Manage Your Network Machine Securely Using IPsec* on page 71)
- Restrict scan function from external devices (see *Restricting Scan Functions from External Devices* on page 83)
- Secure Function Lock 3.0 (see *Secure Function Lock 3.0 (ADS-2800W / ADS-3600W)* on page 84)

NOTE

We recommend disabling the FTP and TFTP protocols. Accessing the machine using these protocols is not secure. However, if you disable FTP, the Scan to FTP function will be disabled. (For more information about how to configure the protocol settings, see *Configure Your Machine Settings* on page 39.)

Send an Email Securely (ADS-2800W / ADS-3600W)

Configuration Using Web Based Management

Configure secured email sending with user authentication or email sending and receiving using SSL/TLS.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then click →.
4. Click **Network**.
5. Click **Protocol**.
6. Click **Advanced Setting** of **SMTP** and make sure the status of **SMTP** is **Enabled**.
7. Configure the **SMTP** settings on this page.

NOTE

- You can confirm that email settings are correct, by sending a test email after the configuration is complete.
- If you do not know the SMTP server settings, contact your system administrator or Internet Service Provider (ISP) for more information.

8. When finished, click **Submit**. The **Test Send E-mail Configuration** dialog box appears.
9. Follow the on-screen instructions to test scan with the current settings.

Sending an Email with User Authentication

This machine prioritizes SMTP-AUTH method to send an email using an email server that requires user authentication. This method prevents any unauthorized users from accessing the email server. You can use Web Based Management or BRAdmin Professional 3 to configure these settings. You can use SMTP-AUTH method for Email Notification, email reports and Scan to E-mail Server.

Email Client Settings

- You must match the SMTP authentication method settings with the method used by your email application.
- Contact your network administrator or your ISP about the email client configuration.
- You must select the **SMTP-AUTH** check box of **Server Authentication Method** to enable SMTP server authentication.

SMTP settings

- You can change the SMTP port number using Web Based Management. This is useful if your ISP (Internet Service Provider) implements the "Outbound Port 25 Blocking (OP25B)" service.
- By changing the SMTP port number to a specific number that your ISP is using for the SMTP server (for example, port 587), you can send an email via the SMTP server.

Sending an Email Securely Using SSL/TLS

This machine supports SSL/TLS to send an email via an email server that requires secure SSL/TLS communication. To send email via an email server that is using SSL/TLS communication, you must configure SSL/TLS correctly.

Verifying Server Certificate

- If you selected **SSL** or **TLS** for **SSL/TLS**, the **Verify Server Certificate** check box is automatically selected to verify the Server Certificate.
  - The server certificate is verified during the connection attempt with the server when sending email.
  - If you do not need to verify the Server Certificate, clear the **Verify Server Certificate** check box.

Port Number

- If you selected **SSL** or **TLS**, the **Port** value is changed to match the protocol. To change the port number manually, select **SSL/TLS**, and then type the port number.
- You must configure the SMTP communication method to match the email server. For details about the email server settings, contact your network administrator or ISP (Internet Service Provider).

  In most cases, the secured webmail services require the following settings:

SMTP

Port: 587

Server Authentication Method: SMTP-AUTH

SSL/TLS: TLS

Security Settings for SFTP

You can configure security key settings for SFTP connection.

Create a Client Key Pair

Client Key Pair is created to establish an SFTP connection.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as "SharedScanner" instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    http://brnxxxxxxxxxxxx/

  The NetBIOS name can be found in the Network Configuration Report.

3. No password is required by default. Type a password if you have set one, and then press ➔.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click **Client Key Pair** in the left navigation bar.
7. Click **Create New Client Key Pair**.
8. In the **Client Key Pair Name** field, type the name (up to 20 characters) you want.
9. Click the **Public Key Algorithm** drop-down list, and then select the algorithm you want.
10. Click **Submit**.
    The client key pair is created and saved in your machine's memory. The client key pair name and public key algorithm appears in the **Client Key Pair List**.

Export a Client Key Pair

Client Key Pair is used to establish an SFTP connection when Public Key is selected as the authentication protocol.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as "SharedScanner" instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    http://brnxxxxxxxxxxxx/

  The NetBIOS name can be found in the Network Configuration Report.

3. No password is required by default. Type a password if you have set one, and then press ➡.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click **Client Key Pair** in the left navigation bar.
7. Click **Export Public Key** shown with **Client Key Pair List**.
8. Click **Submit**.
9. Specify the location where you want to save the file.

The client key pair is exported to your computer.

Import a Server Public Key

Server Public Key is used to establish an SFTP connection when using Scan to SFTP.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as "SharedScanner" instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    http://brnxxxxxxxxxxxx/

  The NetBIOS name can be found in the Network Configuration Report.

3. No password is required by default. Type a password if you have set one, and then press →.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click **Server Public Key** in the left navigation bar.
7. Click **Import Server Public Key** shown with **Server Public Key List**.
8. Specify the file you want to import.
9. Click **Submit**.

The server public key is imported to your machine.

Manage Multiple Certificates

The Multiple Certificate feature feature allows you to use Web Based Management to manage each certificate installed on your machine. In Web Based Management, navigate to the **CA Certificate** screen to view certificate content, delete, or export your certificates.

You can store up to three CA certificates to use SSL.

We recommend storing one certificate fewer than allowed, reserving an empty spot in case of certificate expiration. When a certificate expires, import a new certificate into the reserved spot, and then delete the expired certificate. This ensures that you avoid configuration failure.

NOTE

When you use SSL for SMTP communications, you do not have to select a certificate. The necessary certificate is selected automatically.

Importing a CA Certificate

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as "SharedScanner" instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.
  - For example:

    http://brwxxxxxxxxxxxx/

  You can find the NetBIOS name on your machine's control panel under `Node Name`.

3. No password is required by default. Type a password if you have set one, and then click ➡.
4. Click the **Network** tab, and then click **Security**.
5. Click **CA Certificate**.
6. Click **Import CA Certificate** and select the certificate.
7. Click **Submit**.

Exporting a CA Certificate

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.

NOTE

- If you are using a Domain Name System or enable a NetBIOS name, you can type another name, such as "SharedScanner" instead of the IP address.
  - For example:

    http://SharedScanner/

  If you enable a NetBIOS name, you can also use the node name.

  - For example:

    http://brwxxxxxxxxxxxx/

  You can find the NetBIOS name on your machine's control panel under `Node Name`.

3. No password is required by default. Type a password if you have set one, and then click →.
4. Click the **Network** tab, and then click **Security**.
5. Click **CA Certificate**.
6. Select the certificate you want to export and click **Export**.
7. Click **Submit**.

Manage Your Network Machine Securely Using IPsec

- Introduction to IPsec

  IPsec (Internet Protocol Security) is a security protocol that uses an optional Internet Protocol function to prevent data manipulation and ensure the confidentiality of data transmitted as IP packets. IPsec encrypts data carried over the network. 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.

- Configure IPsec Using Web Based Management

  The IPsec connection conditions consist of two **Template** types: **Address** and **IPsec**.

  You can configure up to 10 connection conditions.

- Configure an IPsec Address Template Using Web Based Management
- Configure an IPsec Template Using Web Based Management

Introduction to IPsec

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 Internet Key Exchange (IKE) 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 Virtual Private Network (VPN).

NOTE

For IPsec transmissions, the following conditions are necessary:

- A computer that can communicate using IPsec is connected to the network.
- Your Brother machine is configured for IPsec communication.
- The computer connected to your Brother machine is configured for IPsec connections.

- IPsec settings

  The settings that are necessary for connections using IPsec. These settings can be configured using Web Based Management.

NOTE

To configure the IPsec settings, you must use the browser on a computer that is connected to the network.

Configure IPsec Using Web Based Management

The IPsec connection conditions consist of two **Template** types: **Address** and **IPsec**. You can configure up to 10 connection conditions.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then click →.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click the **IPsec** menu in the left navigation bar.
7. In the **Status** field, enable or disable IPsec.
8. Select **Negotiation Mode** for IKE Phase 1.
   IKE is a protocol used to exchange encryption keys to carry out encrypted communication using IPsec. In **Main** mode, the processing speed is slow, but the security is high. In **Aggressive** mode, the processing speed is faster than in **Main** mode, but the security is lower.
9. In the **All Non-IPsec Traffic** field, select the action to be taken for non-IPsec packets.
   When using Web Services, you must select **Allow** for **All Non- IPsec Traffic**. If you selected **Drop**, Web Services cannot be used.
10. In the **Broadcast/Multicast Bypass** field, select **Enabled** or **Disabled**.
11. In the **Protocol Bypass** field, select the check box for the option or options you want.
12. In the **Rules** table, select the **Enabled** check box to activate the template.
    When you select multiple check boxes, the lower-numbered check boxes have priority if the settings for the selected check boxes conflict.
13. Click the corresponding drop-down list to select the **Address Template** that is used for the IPsec connection conditions.
    To add an **Address Template**, click **Add Template**.
14. Click the corresponding drop-down list to select the **IPsec Template** that is used for the IPsec connection conditions.
    To add an **IPsec Template**, click **Add Template**.
15. Click **Submit**.
    If the computer must be restarted to register the new settings, the restart confirmation screen appears.
    If there is a blank item in the template you enabled in the **Rules** table, an error message appears. Confirm your choices and submit again.

Configure an IPsec Address Template Using Web Based Management

1. Start your web browser.
2. In your browser’s address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then click →.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click the **IPsec Address Template** menu in the left navigation bar.
   The Template List appears, displaying 10 Address Templates.
   Click the **Delete** button to delete an **Address Template**. When an **Address Template** is in use, it cannot be deleted.
7. Click the **Address Template** you want to create. The **IPsec Address Template** appears.
8. In the **Template Name** field, type a name for the template (up to 16 characters).
9. Select a **Local IP Address** option to 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** from the drop-down list.

     If you selected **Custom** from the drop-down list, type the IP address (IPv4 or IPv6) in the text box.
   - **IP Address Range**

     Type the starting and ending IP addresses for the IP address range in the text boxes. If the starting and ending IP addresses are not standardized to the IPv4 or IPv6 format, or the ending IP address is shorter than the starting address, an error will occur.
   - **IP Address / Prefix**

     Specify the IP address using CIDR notation.

     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.xxx are valid.
10. Select a **Remote IP Address** option to specify the IP address conditions for the recipient:
    - **Any**

      Enables all IP addresses.
    - **IP Address**

      Allows you to type the specified IP address (IPv4 or IPv6) in the text box.
    - **IP Address Range**

      Allows you to type 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 shorter than the starting address, an error will occur.

- **IP Address / Prefix**

  Specify the IP address using CIDR notation.

  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.xxx are valid.

11. Click **Submit**.

NOTE

When you change the settings for the template currently in use, the IPsec screen in Web Based Management closes and opens again.

Configure an IPsec Template Using Web Based Management

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then click ➡.
4. Click the **Network** tab.
5. Click the **Security** tab.
6. Click **IPsec Template** in the left navigation bar.
   The Template List appears, displaying 10 IPsec Templates.
   Click the **Delete** button to delete an **IPsec Template**. When an **IPsec Template** is in use, it cannot be deleted.
7. Click **IPsec Template** you want to create. The **IPsec Template** screen appears.
   The configuration fields differ based on the **Use Prefixed Template** and **Internet Key Exchange (IKE)** you select.
8. In the **Template Name** field, type a name for the template (up to 16 characters).
9. Select the **Internet Key Exchange (IKE)** options.
10. Click **Submit**.

IKEv1 Settings for an IPsec Template

Template Name

Type a name for the template (up to 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 may differ depending on whether you selected **Main** or **Aggressive** for **Negotiation Mode** on the **IPsec** configuration screen.

Internet Key Exchange (IKE)

IKE is a communication protocol used to exchange encryption keys to carry out encrypted communication using IPsec. To carry out encrypted communication this time only, the encryption algorithm 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 the encrypted communication limited to IKE is carried out.

If you selected **Custom** in **Use Prefixed Template**, select **IKEv1**, **IKEv2**, or **Manual**. If you selected a setting other than **Custom**, the IKE, authentication type and Encapsulating Security selected in **Use Prefixed Template** are displayed.

Authentication Type

Configure 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.

  Select **Group1**, **Group2**, **Group5**, or **Group14**.

- **Encryption**

  Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.

- **Hash**

  Select **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.

- **SA Lifetime**

  Specify the IKE SA lifetime.

  Type the time (seconds) and number of kilobytes (KByte).

Encapsulating Security

- **Protocol**

  Select **ESP**, **AH+ESP** or **AH**.

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 consists 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 (Authentication Header) 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, 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**

  Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**. The encryption can be selected only when **ESP** is selected in **Protocol**.

- **Hash**

  Select **None**, **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.

  None can be selected only when **ESP** is selected in **Protocol**.

  When **AH+ESP** is selected in **Protocol**, select each protocol for **Hash(AH)** and **Hash(ESP)**.

- **SA Lifetime**

  Specify the IPsec SA lifetime.

  Type the time (seconds) and number of kilobytes (KByte).

- **Encapsulation Mode**

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

- **Remote Router IP-Address**

  Specify the IP address (IPv4 or IPv6) of the remote router. Enter this information 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, to establish a secure communication channel before communication begins. SA may also refer to an already established virtual encrypted communication channel. 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 the previous keys that 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 is limited only to the messages that were encrypted using that key.

Select **Enabled** or **Disabled**.

Authentication Method

Select the authentication method. Select **Pre-Shared Key** or **Certificates**.

Pre-Shared Key

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

If you selected **Pre-Shared Key** for the **Authentication Method**, type the **Pre-Shared Key** (up to 32 characters).

- **Local ID Type/ID**

  Select the sender's ID type, and then type the ID.

  Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type. If you selected **Certificate**, type the common name of the certificate in the **ID** field.

- **Remote ID Type/ID**

  Select the recipient's ID type, and then type the ID.

  Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type. If you selected **Certificate**, type the common name of the certificate in the **ID** field.

Certificate

If you selected **Certificates** for **Authentication Method**, select the certificate.

NOTE

You can select only the certificates that were created using the **Certificate** page of the Web Based Management's Security configuration screen.

IKEv2 Settings for an IPsec Template

Template Name

Type a name for the template (up to 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 may differ depending on whether you selected **Main** or **Aggressive** for **Negotiation Mode** on the **IPsec** configuration screen.

Internet Key Exchange (IKE)

IKE is a communication protocol used to exchange encryption keys to carry out encrypted communication using IPsec. To carry out encrypted communication this time only, the encryption algorithm 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 the encrypted communication that is limited to IKE is carried out.

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

If you selected a setting other than **Custom**, the IKE, authentication type and Encapsulating Security selected in **Use Prefixed Template** are displayed.

Authentication Type

Configure 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 the open information generated using a random number and the secret key.

  Select **Group1**, **Group2**, **Group5**, or **Group14**.

- **Encryption**

  Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.

- **Hash**

  Select **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.

- **SA Lifetime**

  Specify the IKE SA lifetime.

  Type the time (seconds) and number of kilobytes (KByte).

Encapsulating Security

- **Protocol**

  Select **ESP**.

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 consists 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.

- **Encryption**

  Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.

- **Hash**

  Select **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.

- **SA Lifetime**

  Specify the IPsec SA lifetime.

  Type the time (seconds) and number of kilobytes (KByte).

- **Encapsulation Mode**

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

- **Remote Router IP-Address**

  Specify the IP address (IPv4 or IPv6) of the remote router. Enter this information 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, 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 the previous keys that 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 is limited only to the messages that were encrypted using that key.

Select **Enabled** or **Disabled**.

Authentication Method

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

Pre-Shared Key

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

If you selected **Pre-Shared Key** for the **Authentication Method**, type the **Pre-Shared Key** (up to 32 characters).

- **Local ID Type/ID**

  Select the sender's ID type, and then type the ID.

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

  If you selected **Certificate**, type the common name of the certificate in the **ID** field.

- **Remote ID Type/ID**

  Select the recipient's ID type, and then type the ID.

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

  If you selected **Certificate**, type the common name of the certificate in the **ID** field.

Certificate

If you selected **Certificates** for **Authentication Method**, select the certificate.

NOTE

You can select only the certificates that were created using the **Certificate** page of the Web Based Management's Security configuration screen.

EAP

EAP is an authentication protocol that is an extension of PPP. When using EAP with IEEE 802.1x, a different key is used for user authentication during 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**

  Type the user name (up to 32 characters).

- **Password**

  Type the password (up to 32 characters). The password must be entered two times for confirmation.

- **Certificate**

  Click this button to move to the **Certificate** configuration screen.

Manual Settings for an IPsec Template

Template Name

Type a name for the template (up to 16 characters).

Use Prefixed Template

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

NOTE

The default template may differ depending on whether you selected **Main** or **Aggressive** for **Negotiation Mode** on the **IPsec** configuration screen.

Internet Key Exchange (IKE)

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

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

If you selected a setting other than **Custom**, the IKE, authentication type and Encapsulating Security selected in **Use Prefixed Template** are displayed.

Authentication Key (ESP, AH)

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

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

NOTE

The number of characters you can set may differ depending on the setting you selected for **Hash** in the **Encapsulating Security** section.

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

- **MD5**: 128 bits (16 bytes)
- **SHA1**: 160 bits (20 bytes)
- **SHA256**: 256 bits (32 bytes)
- **SHA384**: 384 bits (48 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. Type 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 may differ depending on the setting you selected for **Encryption** in the **Encapsulating Security** section.

If the length of the specified code key is different than 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 security information. Generally, a host has multiple Security Associations (SAs) 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 Authentication Header (AH) and Encapsulating Security Payload (ESP) header.

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

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

Encapsulating Security

- **Protocol**

  Select **ESP** or **AH**.

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 consists 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, 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**

  Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**. The encryption can be selected only when **ESP** is selected in **Protocol**.

- **Hash**

  Select **None**, **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.

  None can be selected only when **ESP** is selected in **Protocol**.

- **SA Lifetime**

  Specify the IKE SA lifetime.

  Type the time (seconds) and number of kilobytes (KByte).

- **Encapsulation Mode**

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

- **Remote Router IP-Address**

  Specify the IP address (IPv4 or IPv6) of the connection destination. Enter this information 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, 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.

Submit

Click this button to register the settings.

NOTE

When you change the settings for the template currently in use, the IPsec screen in Web Based Management closes and opens again.

Restricting Scan Functions from External Devices

This feature allows you to restrict scan functions from external devices.

When you restrict scan functions from external devices, an error message appears on the device and users cannot use those scan functions.

Restricting Scan Functions from External Devices Using a Web Browser Settings

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then press →.
4. Click the **Scan** tab.
5. Click the **Scan from PC** menu in the navigation bar.
6. Select **Pull Scan** for Disabled.
7. Click **Submit**.

Secure Function Lock 3.0 (ADS-2800W / ADS-3600W)

Secure Function Lock lets you restrict Public access to the following machine operations:

- Scan to PC
- Scan to FTP/SFTP
- Scan to Network
- Scan to USB
- Scan to Web
- Scan to Email Server
- Scan to SharePoint
- Scan to WSS (Web Service Scan)
- Apps

Secure Function Lock also prevents users from changing the default settings of the machine by limiting access to the machine's settings.

Before using the security features you must first enter an administrator password.

The administrator can set up restrictions for individual users along with a user password.

Carefully write down your password. If you forget it, you will have to reset the password stored in the machine. For information about how to reset the password contact Brother Customer Service.

NOTE

- Secure Function Lock can be set using Web Based Management or BRAdmin Professional 3 (Windows® only).
- Only administrators can set limitations and make changes for each user.
- (For ADS-3600W)
  Use card authentication to switch to a different user and access scan functions, such as Scan to PC, Scan to FTP, or Scan to Network.

Before You Begin to Use Secure Function Lock 3.0

You can configure the Secure Function Lock settings using a web browser. First, do the following:

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. Type an Administrator password in the **Login** box. (This is a password to log on to the machine's web page.) Click ➔.

Turning Secure Function Lock on/off

1. Click **Administrator**.
2. Click **User Restriction Function**.
3. Select **Secure Function Lock** or **Off**.
4. Click **Submit**.

Configure Secure Function Lock 3.0 Using Web Based Management

Set up groups with restrictions and users with a password and card ID (NFC ID)[1]. You can set up to 100 restricted groups and 100 users. Configure these settings using a web browser. To set up the web page, see *Before You Begin to Use Secure Function Lock 3.0* on page 84, and then follow these steps:

[1] For ADS-3600W

1. Click **Administrator**.
2. Click **User Restriction Function**.
3. Select **Secure Function Lock**.
4. Click **Submit**.
5. Click **User List xx-xx**.
6. In the **User List** field, type the user name up to 20 characters.
7. In the **PIN Number** box, type a four-digit password.
8. (For ADS-3600W)
   In the **Card ID** box, type the card number (up to 16 characters).[1]

   [1] You can use numbers from 0 - 9 and letters from A - F (not case-sensitive).
9. Select **User List / Restricted Functions** from the drop-down list for each user.
10. Click **Submit**.

Firmware Update

You can update to the latest firmware by visiting Brother's site.

NOTE

If you use a proxy server for internet communication, you will need to enter the details in the Proxy setting.

1. Start your web browser.
2. In your browser's address bar, type the IP address of your machine. For example: http://192.168.1.2.
3. No password is required by default. Type a password if you have set one, and then press ➡.
4. Click the **Administrator** tab.
5. Click the **Firmware Update** menu in the navigation bar.
6. Click **Check for new firmware**.

7 Troubleshooting

Overview

This chapter explains how to resolve typical network problems you may encounter when using your Brother machine.

To download other manuals for your machine, go to your model's page on the Brother Solutions Center at solutions.brother.com/manuals

Identifying Your Problem

Make sure that the following items are configured before reading this chapter.

Make sure you have checked the following:

The AC Adapter is connected properly and the Brother machine is turned on.
The access point, router, or hub is turned on and its link button is blinking.
All protective packaging has been removed from the machine.
The Front Cover, Separation Pad Cover and Pick-up Roller Cover are completely closed.

Go to the page for your solution:

- *I cannot complete the wireless network setup configuration.* on page 88.
- *Wireless LAN Error Codes (ADS-2800W / ADS-3600W)* on page 89.
- *The Brother machine is not found on the network during the Brother Device installation.* on page 91.
- *The Brother machine cannot scan over the network. The Brother machine is not found on the network even after successful installation.* on page 92.
- *I am using security software.* on page 94.
- *I want to check that my network devices are working properly.* on page 95.

I cannot complete the wireless network setup configuration.

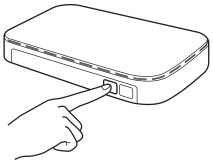
Problem	Interface	Solution
Did your machine fail to connect to the network during wireless setup?	wireless	Turn your wireless router off and back on, and then try and configure the wireless settings again.
Are your security settings (SSID/Network Key) correct?	wireless	Confirm your security settings. ■ The manufacturer's name or model number of the WLAN access point/router may be used as the default security settings. ■ See the instructions supplied with your WLAN access point/router for information on how to find the security settings. ■ Ask the manufacturer of your WLAN access point/router, your Internet provider, or your network administrator.
Are you using MAC address filtering?	wireless	Confirm that the Brother machine's MAC address is allowed by the filter. You can find the MAC address using the the Brother machine's control panel.
Is your WLAN access point/router in stealth mode (not broadcasting the SSID)?	wireless	■ Type the correct SSID name manually. ■ Check the SSID name or the Network Key in the instructions supplied with your WLAN access point/router and reconfigure the wireless network setup. (For more information, see *When the SSID Is Not Broadcasting* on page 11.)
I have checked and tried all of the above, but still cannot complete the wireless configuration. Is there anything else I can do?	wireless	Use the Network Connection Repair Tool. See *The Brother machine cannot scan over the network. The Brother machine is not found on the network even after successful installation.* on page 92.
Your security settings (SSID/password) are not correct.	Wi-Fi Direct®	Confirm the SSID and password. When you are configuring the network manually, the SSID and password are displayed on your Brother machine. If your mobile device supports the manual configuration, the SSID and password will be displayed on your mobile device's screen.
You are using Android™ 4.0.	Wi-Fi Direct®	If your mobile device disconnects (approximately six minutes after using Wi-Fi Direct®), try the one-push method using WPS (recommended) and set the Brother machine as a G/O.
Your Brother machine is placed too far from your mobile device.	Wi-Fi Direct®	Move your Brother machine within about 1 metre of the mobile device when you configure the Wi-Fi Direct® network settings.
There are some obstructions (walls or furniture, for example) between your machine and the mobile device.	Wi-Fi Direct®	Move your Brother machine to an obstruction-free area.

Problem	Interface	Solution
There is a wireless computer, Bluetooth-supported device, microwave oven, or digital cordless phone near the Brother machine or the mobile device.	Wi-Fi Direct®	Move other devices away from the Brother machine or the mobile device.
If you have checked and tried all of the above, but still cannot complete the Wi-Fi Direct® configuration, do the following:	Wi-Fi Direct®	■ Turn your Brother machine off and back on. Then try to configure the Wi-Fi Direct® settings again. ■ If you are using your Brother machine as a client, confirm how many devices are allowed in the current Wi-Fi Direct® network, and then check how many devices are connected.

Wireless LAN Error Codes (ADS-2800W / ADS-3600W)

If the LCD displays an error code, locate the code in the table and use the recommended solution to correct the error.

Error Code	Recommended Solutions
TS-01	The wireless setting is not activated. Turn the wireless setting on: 1 On your machine, press 🛠 > `Network` > `WLAN` > `Setup Wizard`. 2 When `Enable WLAN?` is displayed, press `Yes`, to start the wireless setup wizard.
TS-02	The wireless access point/router cannot be detected. 1 Check the following: ■ Make sure the wireless access point/router is powered on. ■ Move your machine to an obstruction-free area, or closer to the wireless access point/router. ■ Temporarily place your machine within about 1 metre from the wireless access point/router when you are configuring the wireless settings. ■ If your wireless access point/router is using MAC address filtering, confirm that the Brother machine's MAC address is allowed in the filter. 2 If you manually entered the SSID and security information (SSID/authentication method/encryption method/Network Key), the information may be incorrect. Confirm the SSID and security information and re-enter the correct information as necessary. This device does not support a 5 GHz SSID/ESSID and you must select a 2.4 GHz SSID/ESSID. Make sure the access point/router is set to 2.4 GHz or 2.4 GHz/5 GHz mixed mode.
TS-03	The wireless network and security setting you entered may be incorrect. Confirm the wireless network settings. Confirm that the entered or selected SSID/authentication method/encryption method/UserID/Userpass are correct.

<table>
<tr><th>Error Code</th><th>Recommended Solutions</th></tr>
<tr><td>TS-04</td><td>The Authentication/Encryption methods used by the selected wireless access point/router are not supported by your machine.
For the infrastructure mode, change the authentication and encryption methods of the wireless access point/router. Your machine supports the following authentication methods:
<table>
<tr><th>Authentication Method</th><th>Encryption Method</th></tr>
<tr><td rowspan="2">WPA-Personal</td><td>TKIP</td></tr>
<tr><td>AES</td></tr>
<tr><td>WPA2-Personal</td><td>AES</td></tr>
<tr><td rowspan="2">Open</td><td>WEP</td></tr>
<tr><td>None (without encryption)</td></tr>
<tr><td>Shared key</td><td>WEP</td></tr>
</table>
If your problem is not solved, the SSID or network settings you entered may be incorrect. Confirm the wireless network settings.
For Ad-hoc mode, change the authentication and encryption methods of your computer for the wireless setting. Your machine supports the Open authentication method only, with optional WEP encryption.</td></tr>
<tr><td>TS-05</td><td>The security information (SSID/Network Key) is incorrect.
Confirm the SSID and security information (Network Key).
If your router uses WEP encryption, enter the key used as the first WEP key. Your Brother machine supports the use of the first WEP key only.</td></tr>
<tr><td>TS-06</td><td>The wireless security information (Authentication method/Encryption method/Network Key) is incorrect.
Confirm the wireless security information (Authentication method/Encryption method/Network Key) using the Authentication Method table in error TS-04.
If your router uses WEP encryption, enter the key used as the first WEP key. Your Brother machine supports the use of the first WEP key only.</td></tr>
<tr><td>TS-07</td><td>The machine cannot detect a wireless access point/router that has WPS enabled.
To configure your wireless settings using WPS, you must operate both your machine and the wireless access point/router.
If you do not know how to operate your wireless access point/router using WPS, see the documentation provided with your wireless access point/router, ask the manufacturer of your wireless access point/router, or ask your network administrator.
</td></tr>
<tr><td>TS-08</td><td>Two or more wireless access points that have WPS enabled are detected.
Confirm that only one wireless access point/router within range has the WPS method active and try again.</td></tr>
<tr><td>TS-20</td><td>The machine is still trying to connect to your wireless network. Please wait a few minutes, and then check the WLAN status.</td></tr>
</table>

The Brother machine is not found on the network during the Brother Device installation.

Question	Interface	Solution
Is your computer connected to the network?	wired/ wireless	Make sure your computer is connected to a network (for example, a LAN environment or Internet services. For further support, contact your network administrator.
Is your machine connected to the network and does it have a valid IP address?	wired/ wireless	(Wired network) Check that `Status` in `Wired Status` is `Active XXXX-XX`. (Where `XXXX-XX` is your selected Ethernet interface.) See *How to Check the Network Status (ADS-2800W / ADS-3600W)* on page 3. If the LCD message shows `Inactive` or `Wired OFF`, ask your network administrator whether your IP address is valid or not. (Wireless network) Check that `Status` in `WLAN Status` is not `Connection Failed`. See *How to Check the WLAN Status (ADS-2800W / ADS-3600W)* on page 9. If the LCD message shows `Connection Failed`, ask your network administrator whether your IP address is valid or not.
Are you using security software?	wired/ wireless	■ In the installer dialog box, search for the Brother machine again. ■ Allow access when the alert message of the security software appears during the Brother Device installation. ■ For more information about security software, see *I am using security software.* on page 94.
Are you using a Wi-Fi router?	wireless	The privacy separator on your Wi-Fi router may be enabled. Disable the privacy separator.
Is your Brother machine placed too far from the WLAN access point/router?	wireless	Place your Brother machine within about 1 metre of the WLAN access point/router when you configure the wireless network settings.
Are there any obstructions (walls or furniture, for example) between your machine and the WLAN access point/router?	wireless	Move your Brother machine to an obstruction-free area, or closer to the WLAN access point/router.
Is there a wireless computer, Bluetooth supported device, microwave oven or digital cordless phone near the Brother machine or the WLAN access point/router?	wireless	Move all the devices away from the Brother machine or WLAN access point/router.

The Brother machine cannot scan over the network.
The Brother machine is not found on the network even after successful installation.

Question	Interface	Solution
Are you using security software?	wired/ wireless	See *I am using security software.* on page 94.
Is your Brother machine assigned to an available IP address?	wired/ wireless	■ Confirm the IP address and the Subnet Mask Verify that both the IP addresses and Subnet Masks of your computer and the Brother machine are correct and located on the same network. For more information on how to verify the IP address and the Subnet Mask, ask your network administrator. ■ (Windows®) Confirm the IP address and the Subnet Mask using the Network Connection Repair Tool. Use the Network Connection Repair Tool to fix the Brother machine's network settings (it will assign the correct IP address and the Subnet Mask). To use the Network Connection Repair Tool, ask the network administrator for the required information, and then follow the steps below: **NOTE** • (Windows® XP) You must log on with Administrator rights. • Make sure that the Brother machine is turned on and is connected to the same network as your computer.

Question	Interface	Solution
Is your Brother machine assigned to an available IP address? (continued)	wired/ wireless	1 Insert the supplied DVD-ROM into your DVD-ROM drive. When the DVD-ROM Top Menu appears, close it. 2 Open computer directory for your operating system: ■ Windows® XP Click **Start** > **All Programs** > **Accessories** > **Windows Explorer** > **My Computer**. ■ Windows Vista®/Windows® 7 Click (**Start**) > **Computer**. ■ Windows® 8/Windows® 8.1 Click the (**File Explorer**) icon on the taskbar, and then go to **This Computer**. ■ Windows® 10 Click the (**File Explorer**) icon on the taskbar, and then go to **This PC**. 3 Double-click **DVD Drive**, double-click **Tools**, double-click **NetTool**, and then double-click **BrotherNetTool.exe** to run the program. **NOTE** If the **User Account Control** screen appears: (Windows Vista®) Click **Continue (Allow)**. (Windows® 7/Windows® 8/Windows® 8.1/Windows® 10) Click **Yes**. 4 Follow the on-screen instructions. If the correct IP address and the Subnet mask are still not assigned even after using the Network Connection Repair Tool, ask your network administrator for this information.
Are you connecting the Brother machine to the network using wireless capabilities?	wireless	■ Check `Status` in `WLAN Status`. See *How to Check the WLAN Status (ADS-2800W / ADS-3600W)* on page 9. If the LCD message shows `Connection Failed`, ask your network administrator whether your IP address is valid or not. ■ See *The Brother machine is not found on the network during the Brother Device installation.* on page 91.
I have checked and tried all of the above, but the Brother machine does not scan. Is there anything else I can do?	wired/ wireless	Uninstall Brother Device and reinstall it.

I am using security software.

Question	Interface	Solution
Did you select **Accept** in the security alert dialog box during the Brother Device installation, applications' start-up process, or when using the scanning features?	wired/ wireless	If you did not select **Accept** in the security alert dialog box, the firewall function of your security software may be denying access. Some security software might block access without showing a security alert dialog box. To allow access, see your security software instructions or ask the manufacturer.
I want to know the necessary port number for the security software settings.	wired/ wireless	The following port numbers are used for Brother network features: ■ Network scanning → Port number 54925/Protocol UDP ■ Network scanning, Remote Setup [1] → Port number 161 and 137/Protocol UDP ■ BRAdmin Light [1] → Port number 161/Protocol UDP [1] Windows® only. For information about how to open the port, see the security software instructions or ask the manufacturer.

I want to check that my network devices are working properly.

Question	Interface	Solution
Is your Brother machine, access point/router or network hub turned on?	wired/ wireless	Make sure you have confirmed all instructions in *Make sure you have checked the following:* on page 87.
Where can I find my Brother machine's network settings, such as IP address?	wired/ wireless	■ For Web Based Management 1 Start Web Based Management and access your Brother machine (see step ❶ on page 39). 2 When the Web Based Management screen appears, click the **Network** tab, and then click **Network Status** in the left navigation bar. ■ For Control panel (ADS-2800W / ADS-3600W) Check the settings in `Network` from the control panel on your machine.
How can I check the link status of my Brother machine?	wired/ wireless	■ For Web Based Management 1 Start Web Based Management and access your Brother machine (see step ❶ on page 39). 2 When the Web Based Management screen appears, click the **Network** tab, and then click **Network Status** in the left navigation bar. ■ For Control panel (ADS-2800W / ADS-3600W) (Wired network) Check that `Status` in `Wired Status` is `Active XXXX-XX` (where `XXXX-XX` is your selected Ethernet interface). To check the network status: press 🛠 > `Network` > `Wired LAN` > `Wired Status` > `Status`. If the LCD message shows `Inactive` or `Wired OFF`, ask your network administrator whether your IP address is valid or not. (Wireless network) Check the `Status` in `WLAN Status` is not `Connection Failed`. See *How to Check the WLAN Status (ADS-2800W / ADS-3600W)* on page 9. If the LCD message displays `Connection Failed`, ask your network administrator whether your IP address is valid or not.

Question	Interface	Solution
Can you "ping" the Brother machine from your computer?	wired/ wireless	Ping the Brother machine from your computer by entering the IP address or the node name at the Windows® command prompt: `ping` <`ipaddress`> or <`nodename`>. ■ Successful > Your Brother machine is working correctly and connected to the same network as your computer. ■ Unsuccessful > Your Brother machine is not connected to the same network as your computer. (Windows®) Ask your network administrator and use the Network Connection Repair Tool to fix the IP address and the subnet mask automatically. For more information about the Network Connection Repair Tool, see *Is your Brother machine assigned with an available IP address?* in *The Brother machine cannot scan over the network. The Brother machine is not found on the network even after successful installation.* on page 92. (Macintosh) Confirm the IP address and the Subnet Mask are set correctly. See *Confirm the IP address and the Subnet Mask* in *The Brother machine cannot scan over the network. The Brother machine is not found on the network even after successful installation.* on page 92.
Is the Brother machine connecting to the wireless network?	wireless	Check `Status` in `WLAN Status`. See *How to Check the WLAN Status (ADS-2800W / ADS-3600W)* on page 9. If the LCD message shows `Connection Failed`, ask your network administrator whether your IP address is valid or not.
I have checked and tried all of the above, however, I am still having problems. Is there anything else I can do?	wireless	See the instructions supplied with your WLAN access point/router to find the SSID and the Network Key information and set them correctly. For more information about the SSID and the Network Key, see *Are your security settings (SSID/Network Key) correct?* in *I cannot complete the wireless network setup configuration.* on page 88.

8 Additional Network Settings (Windows®)

Setting Types

The following optional network features are also available:

- Web Services for scanning (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, and Windows® 10)
- Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, and Windows® 10)

NOTE

Verify that either the host computer and the machine are on the same subnet or that the router is properly configured to pass data between the two devices.

Install Drivers Used for Scanning via Web Services (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

The Web Services feature allows you to monitor machines on the network, which simplifies the driver installation process. Drivers used for scanning via Web Services can be installed by right-clicking the scanner icon on the computer, and the computer's Web Services port (WSD port) is created automatically. (For more information about scanning using Web Services, see *Scan Using Web Services (Windows Vista®, Windows® 7, Windows® 8, Windows® 8.1 and Windows® 10)* in the *User's Guide*.)

NOTE

Before you configure this setting, you must configure your machine's IP address.

1. Open network settings for your operating system:
   - Windows Vista®

     Click (**Start**) > **Network**.
   - Windows® 7

     Click (**Start**) > **Control Panel** > **Network and Internet** > **View network computers and devices**.
   - Windows® 8/Windows® 8.1

     Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings** > **Change PC settings** > **Devices** > **Add a device**.
   - Windows® 10

     Click ⊞ (**Start**) > **Settings** > **Devices** > **Printers & Scanners**.
2. The machine's Web Services Name is displayed with the scanner icon.
   - Windows Vista®/Windows® 7/Windows® 8/Windows® 8.1

     Right -click the machine you want to install.
   - Windows® 10

     Click the machine you want to install.

NOTE

The Web Services Name for the Brother machine is your model name and MAC Address (Ethernet Address) (for example, Brother ADS-XXXXX (model name) [XXXXXXXXXXXX] (MAC Address/Ethernet Address)).

3 Start an installation for the machine:

- Windows Vista®/Windows® 7

  Click **Install** in the machine's drop-down menu.
- Windows® 8/Windows® 8.1

  Select the machine you want to install.
- Windows® 10

  Click **Add devices**.

Network Scanning Installation for Infrastructure Mode When Using Vertical Pairing (Windows® 7, Windows® 8, Windows® 8.1, Windows® 10)

Windows® Vertical Pairing is a technology that allows your Vertical Pairing-supported wireless machine to connect to your Infrastructure network using the PIN Method of WPS and the Web Services feature. This also enables the scanner driver installation from the scanner icon in the **Add a device** screen.

If you are in the Infrastructure mode, you can connect your machine to the wireless network, and then install the scanner driver using this feature. Follow the steps below:

NOTE

- If you have set your machine's Web Services feature to Off, you must set it back to On. The default setting of the Web Services for the Brother machine is On. You can change the Web Services setting using Web Based Management (web browser) or BRAdmin Professional 3.
- Make sure your WLAN access point/router includes the Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 compatibility logo. If you are not sure about the compatibility logo, contact your access point/router manufacturer.
- Make sure your computer includes the Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 compatibility logo. If you are not sure about the compatibility logo, contact your computer's manufacturer.
- If you are configuring your wireless network using an external wireless NIC (Network Interface Card), make sure the wireless NIC includes the Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 compatibility logo. For more information, contact your wireless NIC manufacturer.
- To use a Windows® 7, Windows® 8, Windows® 8.1, or Windows® 10 computer as a Registrar, you need to register it to your network in advance. See the instructions supplied with your WLAN access point/router.

1. Turn on your machine.
2. Set your machine to WPS mode (see *Using the PIN Method of Wi-Fi Protected Setup™ (WPS)* on page 19).
3. Open Add a device menu for your operating system:
   - Windows® 7

     Click (**Start**) > **Devices and Printers** > **Add a device**.
   - Windows® 8/Windows® 8.1

     Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings** > **Control Panel** > **Hardware and Sound** > **Devices and Printers** > **Add a device**.
   - Windows® 10

     Click (**Start**) > **Settings** > **Devices** > **Printers & Scanners** > **Add a printer or scanner**.
4. Select your machine and type the PIN that your machine displayed.
5. Select the Infrastructure network you want to connect to, and then click **Next**.
6. When your machine appears in the **Devices and Printers** dialog box, the wireless configuration and the scanner driver installation is successful.

A Appendix

Supported Protocols and Security Features

Interface	Ethernet	10BASE-T, 100BASE-TX
	Wireless (ADS-2800W / ADS-3600W)	IEEE 802.11b/g/n (Infrastructure Mode/Ad-hoc Mode) IEEE 802.11g/n (Wi-Fi Direct®)
Network (common)	Protocol (IPv4)	ARP, RARP, BOOTP, DHCP, APIPA (Auto IP), WINS/NetBIOS name resolution, DNS Resolver, mDNS, LLMNR responder, Custom Raw Port/Port9100, SMTP Client, FTP Client and Server, LDAP Client (ADS-2800W / ADS-3600W only), CIFS Client, WebDAV Client, SNMPv1/v2c/v3 (MD5/SHA1), HTTP/HTTPS server, TFTP client and server, ICMP, Web Services (Scan), SNTP Client
	Protocol (IPv6)	NDP, RA, DNS resolver, mDNS, LLMNR responder, Custom Raw, Port/Port9100, SMTP Client, FTP Client and Server, LDAP Client, CIFS Client, TELNET Server, SNMPv1/v2c/v3, HTTP/HTTPS server, TFTP client and server, ICMPv6, Web Services (Scan), SNTP Client, WebDav Client
Network (Security)	Wired	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, IPsec
	Wireless (ADS-2800W / ADS-3600W)	SMTP-AUTH, SSL/TLS (HTTPS, SMTP), SSH, SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos, Ipsec
Email (Security) (ADS-2800W / ADS-3600W)	Wired and Wireless	SMTP-AUTH, SSL/TLS (SMTP)
Network (Wireless) (ADS-2800W / ADS-3600W)	Wireless Certification	Wi-Fi Certification Mark License (WPA™/WPA2™ - Enterprise, Personal), Wi-Fi Protected Setup™ (WPS) Identifier Mark License, Wi-Fi CERTIFIED Wi-Fi Direct®

Web Based Management Function Table

NOTE

For more information, click ? on the right side on each page of the Web Based Management interface.

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
General	-	**Status**	**Device Status / Automatic Refresh / Web Language / Device Location**	Display Device Status, Contact and Location. You can change the Language of the Web Based Management interface.
	-	**Auto Refresh Interval**	**Refresh Interval**	Configure Refresh Interval (between 15 seconds and 60 minutes).
	-	**Maintenance Information**	**Node Information / Remaining Life / Total Pages Scanned / Replace Count / Reset Count / Error Count / Error History (last 10 errors)**	Display your Brother machine's maintenance information including as Model, Consumable accessory, page counter, and Error. Click **Submit** to convert this maintenance Information page to a CSV file.
	-	**Find Device**	**Node Name / Model Name / Device Status / IP Address**	Display all network connected devices.
	-	**Contact & Location**	**Contact / Location**	After configuring Contact and Location here, it can be displayed with **General** > **Status** > **Device Location**.
	-	**Sleep Time**	**Sleep Time**	Configure Sleep Time (up to 90 minutes).
	-	**Auto Power Off**	**Auto Power Off**	
	-	**Volume**	**Beep**	Configure sound volume (**Off** / **Low** / **Medium** / **High**).
	-	**Panel** (ADS-2800W / ADS-3600W)	**Backlight / Dim Timer**	
	-	**Scheduled Maintenance Alert**	**Scheduled Maintenance Alert**	

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Address book (ADS-2800W / ADS-3600W)	-	**Address**	**Address / E-mail Address / Name**	Register Email Address and Name (up to 300).
	-	**Setup Groups**	**Group / Address / Name / Members**	Register the contact group (up to 20). Select **Address#** and click **Select** to configure the group members.
	-	**LDAP**	**LDAP Search / Quick Settings / Advanced Settings**	Configure the LDAP settings.
	-	**Import**	**“Address Book” data file / “Group” data file**	
	-	**Export**		
E-mail (ADS-2800W / ADS-3600W)	-	**E-mail Send**	**E-mail Subject / E-mail Message / Size Limit / Request Delivery Notification (Send) / SMTP**	Configure the E-mail Send settings, such as subject, message, or limit Email Size and Delivery Notification. Click **SMTP** to Jump to **Network** > **Network** > **Protocol** > **SMTP** > **Advanced Setting**.

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Scan	-	**Scan**	**Multifeed Detection / Scan offset correction / Front Page Offset X / Front Page Offset Y / Back Page Offset X / Back Page Offset Y / Display Scan Result**	
	-	**Scan Job e-mail report** (ADS-2800W / ADS-3600W)	**SMTP Server Address / Administrator Address / SMTP / Scan to E-mail Server / Scan to FTP / Scan to SFTP / Scan to Network / Scan to SharePoint**	
	-	**Scan File Name**	**File Name Style / Add Date & Time / Counter / Scan to USB 1~5 / Scan to E-mail Server 1~10 / Scan to FTP/SFTP 1~15 / Scan to Network/SharePoint 1~15**	
	-	**Scan to USB**	**File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF** (ADS-2400N / ADS-3000N) **/ Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W)	Configure the Scan to USB settings.
	-	**Scan to E-mail Server** (ADS-2800W / ADS-3600W)	**File Name / Quality / Auto Color detect adjust / Color / Black and White/Gray / File Type / Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W) **/ Send to My E-mail**	Configure the Scan to E-mail Server settings.
	-	**Scan to PC** (ADS-2400N / ADS-3000N)	**Scan to**	
	-	**Scan to FTP/SFTP/ Network/ SharePoint**	**Profile 1~25 / Send to My Folder** (ADS-2800W / ADS-3600W)	Configure the Scan to FTP/SFTP/Network/SharePoint settings.
	-	**Scan to FTP/SFTP/ Network/ SharePoint Profile**	**Profile 1~25**	Configure the Profile settings.

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Scan (continue)	-	**Profile (FTP)**	**Profile Name / Host Address / Username / Password / Store Directory / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF** (ADS-2400N / ADS-3000N) **/ Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W) **/ Passive Mode / Port Number**	Configure the Profile settings. For more information, see *Change the Scan to FTP Configuration* on page 49.
	-	**Profile (SFTP)**	**Profile Name / Host Address / Username / Auth. Method / Client Key Pair / Server Public Key / Store Directory / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF** (ADS-2400N / ADS-3000N) **/ Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W) **/ Port Number**	Configure the Profile settings. For more information, see *Change the Scan to SFTP Configuration* on page 50.
	-	**Profile (Network)**	**Profile Name / Network Folder Path / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF** (ADS-2400N / ADS-3000N) **/ Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W) **/ Use PIN for Authentication / PIN Code / Auth. Method / Username / Password / Date&Time**	Configure the Profile settings. For more information, see *Change the Scan to Network Configuration (Windows$^{®}$)* on page 52.

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Scan (continue)	-	**Profile (SharePoint)**	**Profile Name / SharePoint Site Address / SSL/TLS / File Name / Quality / Auto Color detect adjust / File Type / Password for Secure PDF** (ADS-2400N / ADS-3000N) **/ Document Size / Margin Settings / File Size / Auto Deskew / Skip Blank Page / Skip blank page sensitivity / 2-Sided Scan / Brightness / Contrast / Continuous Scan** (ADS-2800W / ADS-3600W) **/ Use PIN for Authentication / Pin Code / Auth. Method / Username / Password / Date&Time**	Configure the Profile settings. For more information, see *Change the Scan to SharePoint Configuration (Windows®)* on page 54.
	-	**Scan to Network Device** (ADS-2400N / ADS-3000N)	**Network Device1 / Type / Destionation / Network Device2 / Type / Destionation / Network Device3 / Type / Destionation**	
	-	**Scan from PC**	**Pull Scan**	

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Administrator	-	**Login Password**	**Password**	Configure the password used to log in to the Web Based Management. You can change the settings only on the **General** tab without logging in.
	-	**User Restriction Function** (ADS-2800W / ADS-3600W)		
	-	**Secure Function Lock** (ADS-2800W / ADS-3600W)	**Web / PC / Network / FTP/SFTP / E-mail Server / Share Point / WS Scan / USB**	**Secure Function Lock** restricts scan functions and Web Connect functions based on user permissions. For more information, see *Secure Function Lock 3.0 (ADS-2800W / ADS-3600W)* on page 84.
	-	**Active Directory Authentication** (ADS-2800W / ADS-3600W)	**Remember User ID / Active Directory Server Address / Active Directory Domain Name / Get User's Home Directory / Protocol & Authentication Method / Get Mail Address / LDAP Server Port / LDAP Search Root / SNTP**	**Active Directory Authentication** restricts the use of your Brother machine. For more information, see *Configure Active Directory LDAP Authentication (ADS-2800W / ADS-3600W)* on page 43.
	-	**LDAP Authentication** (ADS-2800W / ADS-3600W)	**Remember User ID / LDAP Server Address / Get Mail Address / LDAP Server Port / LDAP Search Root / Attribute of Name(Serch Key) / SNTP**	**LDAP Authentication** restricts the use of your Brother machine. For more information, see *Changing LDAP Configuration* on page 44.
	-	**Setting Lock** (ADS-2800W / ADS-3600W)	**Setting Lock / Password**	Configure the password to change machine settings using your Brother machine's LCD.
	-	**Signed PDF**	**Select the Ceríficate / Cerificate**	Configure the certificate settings for Signed PDF.
	-	**Date & Time**	**Date / Clock Type / Time / Time Zone / Auto Daylight / Synchronize with SNTP server / SNTP**	
	-	**Reset Menu**	**Machine Reset / Network / Address Book / All Settings / Factory Reset**	
	-	**Firmware Update**	**Model Name / Serial Number / Firmware Version / MAIN / Firmware Update / Proxy**	See *Firmware Update* on page 86

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Network	**Network**	**Network Status**	**Wired / Wireless**	Display Network Status.
		Interface (ADS-2800W / ADS-3600W)	**Interface / Wi-Fi Direct**	Change the interface.
		Protocol	**Web Based Management (Web Server) / Telnet / SNTP / Remote Setup / Raw Port / Web Services / Proxy / Network Scan / SMTP / FTP Server / FTP Client / SFTP / TFTP / WebDAV / CIFS / LDAP / mDNS / LLMNR / SNTP**	Configure your Brother machine's protocol settings. Select the check box for each protocol you want to use.
		Notification	**SMTP Server Address / Device E-mail Address / SMTP / Administrator Address**	Configure the Error Notification settings.
		E-mail Reports (ADS-2800W / ADS-3600W)	**SMTP Server Address / E-mail Address / SMTP / Date&Time / Administrator Address**	
	Wired	**TCP/IP (Wired)**	**Ethernet 10/100/1000 BASE-T / IP Address / Subnet Mask / Gateway / Boot Method / Advanced Settings / Interface**	Configure the TCP/IP (Wired) settings.
		Node Name (Wired)	**Node Name**	
		NetBIOS (Wired)	**NETBIOS/IP / Computer Name / WINS Server Method / Primary WINS Server IP Address / Secondary WINS Server IP Address**	
		IPv6 (Wired)	**IPv6 / Static IPv6 Address / Primary DNS Server IP Address / Secondary DNS Server IP Address / IPv6 Address List**	
		Ethernet	**Ethernet Mode**	
		Wired 802.1x Authentication	**Wired 802.1x status / Authentication Method / Inner Authentication Method / User ID / Password / Client Certificate / Server Certificate Verification / Server ID / Certificate**	

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Network (continue)	**Wireless** (ADS-2800W / ADS-3600W)	**TCP/IP (Wireless)**	**IEEE 802.11b/g/n / IP Address / Subnet Mask / Gateway / Boot Method / Advanced Settings / Interface**	Configure the TCP/IP (Wireless) settings.
		Node Name (Wireless)	**Node Name**	
		NetBIOS (Wireless)	**NETBIOS/IP / Computer Name / WINS Server Method / Primary WINS Server IP Address / Secondary WINS Server IP Address**	
		IPv6 (Wireless)	**IPv6 / Static IPv6 Address / Primary DNS Server IP Address / Secondary DNS Server IP Address / IPv6 Address List**	
		Wireless (Setup Wizard)		Click **Start Wizard** to start the setup wizard for your wireless network.
		Wireless (Personal)	**Current Status / Communication Mode / Wireless Network Name (SSID) / Channel / Authentication Method / Encryption Mode / Network key**	
		Wireless (Enterprise)	**Current Status / Communication Mode / Wireless Network Name (SSID) / Channel / Authentication Method / Inner Authentication Method / Encryption Mode / User ID / Password / Client Certificate / Server Certificate Verification / Server ID / Certificate**	

Main Category	Sub Category	Function Menu	Function Options	Description / Optional Settings
Network (continue)	**Security**	**IPv4 Filter**	**Use IP Filtering Feature / Administrator IP Address / Access Setting**	Configure Access Settings by filtering IP address.
		Certificate	**Certificate List / Create Self-Signed Certificate / Create CSR / Install Certificate / Import Certificate and Private Key**	Configure the Certificate settings.
		CA Certificate	**CA Certificate List / Import CA Certificate**	Configure the CA Certificate settings.
		Client Key Pair	**Client Key Pair List / Create New Client Key Pair**	Configure the Client Key Pair settings.
		Server Public Key	**Server Public Key List / Import Server Public Key**	Configure the Server Public Key settings.
		IPsec	**Status / Negotiation Mode / All Non-IPsec Traffic / Broadcast/Multicast Bypass / Protocol Bypass / Rules**	Configure the IPsec settings.
		IPsec Address Template	**Template List**	
		IPsec Template	**Template List**	

B Index