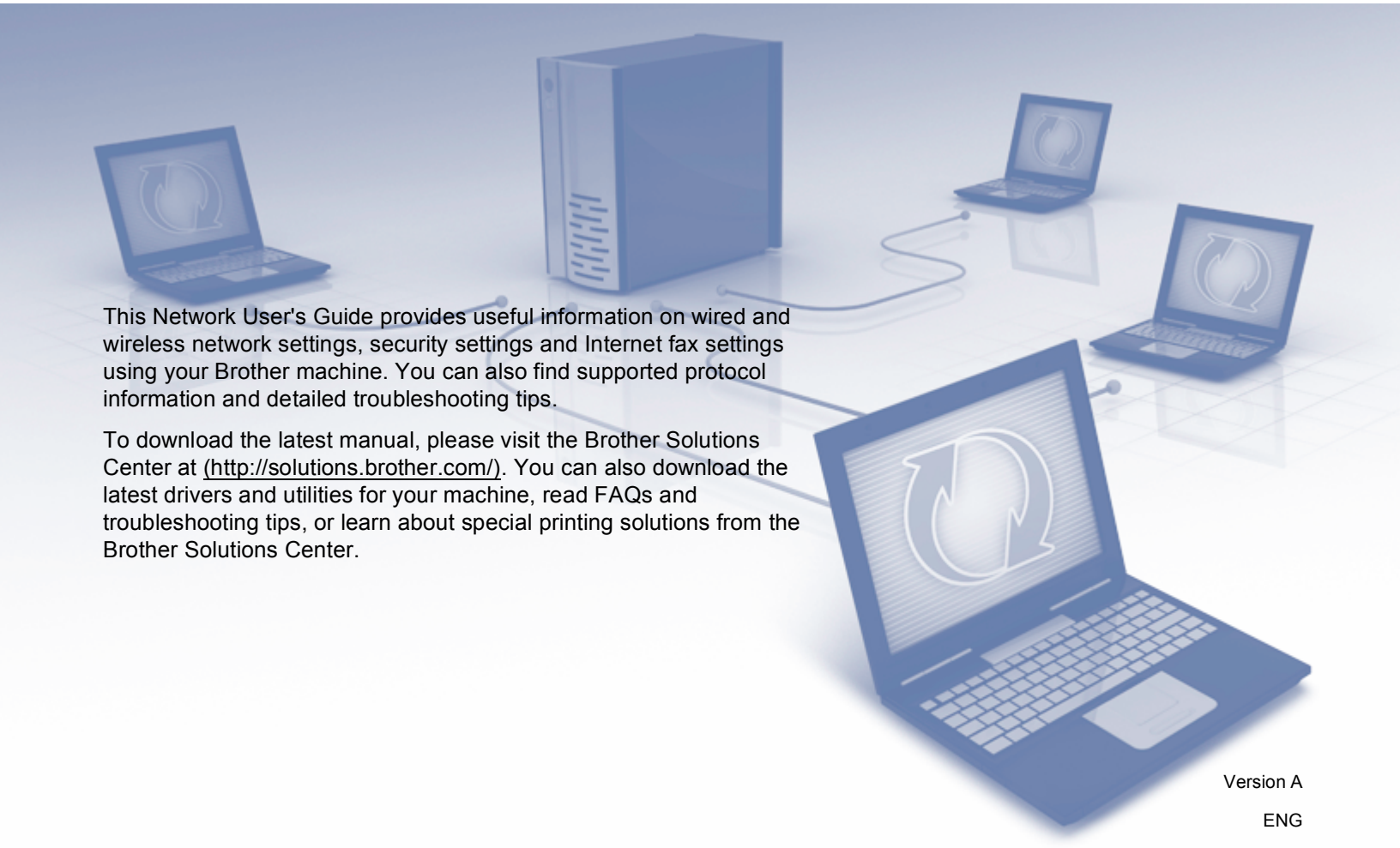
Network User’s Guide

Multi-Protocol On-board Ethernet Multi-function Print Server and Wireless Multi-function Print Server



This Network User's Guide provides useful information on wired and wireless network settings, security settings and Internet fax settings using your Brother machine. You can also find supported protocol information and detailed troubleshooting tips.

To download the latest manual, please visit the Brother Solutions Center at (http://solutions.brother.com/). You can also download the latest drivers and utilities for your machine, read FAQs and troubleshooting tips, or learn about special printing solutions from the Brother Solutions Center.

Version A

ENG

Applicable models

This User's Guide applies to the following models.

HL-3180CDW/DCP-9015CDW/9020CDN/9020CDW/MFC-9130CW/9140CDN/9330CDW/9340CDW

Definitions of notes

The following icons are used throughout this User's Guide.

IMPORTANT	IMPORTANT indicates a potentially hazardous situation which, if not avoided, may result in damage to property or loss of product functionality.
NOTE	Notes tell you how you should respond to a situation that may arise or give tips about how the operation works with other features.

IMPORTANT NOTE

- Do not use this product outside the country of purchase as it may violate the wireless telecommunication and power regulations of that country.
- Windows® XP in this document represents Windows® XP Professional, Windows® XP Professional x64 Edition and Windows® XP Home Edition.
- Windows Server® 2003 in this document represents Windows Server® 2003 and Windows Server® 2003 x64 Edition.
- Windows Server® 2008 in this document represents Windows Server® 2008 and Windows Server® 2008 R2.
- Windows Server® 2012 in this document represents all editions of Windows Server® 2012.
- Windows Vista® in this document represents all editions of Windows Vista®.
- Windows® 7 in this document represents all editions of Windows® 7.
- Windows® 8 in this document represents all editions of Windows® 8.
- Please go to the Brother Solutions Center at http://solutions.brother.com/ and click Manuals on your model page to download the other manuals.
- Not all models are available in all countries.

Table of Contents

Section I Network Operation

1 Introduction 2

Network features....2
Other Network features....4

2 Changing your machine's network settings 5

How to change your machine's network settings
(IP address, Subnet mask and Gateway)....5
Using the control panel....5
Using the BRAdmin Light utility....5
Other Management Utilities....8
Web Based Management (web browser)....8
BRAdmin Professional 3 utility (Windows®)....8
BRPrint Auditor (Windows®)....9

3 Configuring your machine for a wireless network (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) 10

Overview....10
Confirm your network environment....11
Connected to a computer with a WLAN access point/router in the network (Infrastructure mode)....11
Connected to a wireless capable computer without a WLAN access point/router in the network (Ad-hoc mode)....12
Wireless configuration temporarily using a USB cable (Recommended)....13
Configuration using the machine's control panel Setup Wizard....18
Manual configuration from the control panel....19
Configuring your machine when the SSID is not broadcast....21
Configuring your machine for an enterprise wireless network....23
One push configuration using WPS (Wi-Fi Protected Setup) or AOSS™....27
Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)....29
Configuration in Ad-hoc mode....32
Using configured SSID....32
Using a New SSID....34

4 Control panel setup 36

Network menu....36
TCP/IP....36
Ethernet (wired network only)....39
Wired Status (For HL-3180CDW, DCP-9015CDW, DCP-9020CDN, DCP-9020CDW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)....39
Setup Wizard (wireless network only)....39
WPS (Wi-Fi Protected Setup)/AOSS™ (wireless network only)....39
WPS (Wi-Fi Protected Setup) w/PIN Code (wireless network only)....39

WLAN Status (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) 39
MAC Address 40
Set to Default 40
Wired Enable (For DCP-9020CDW, MFC-9330CDW and MFC-9340CDW) 40
WLAN Enable 40
E-mail / IFAX (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download) 40
Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download) 44
How to set a new default for Scan to FTP 46
How to set a new default for Scan to Network (Windows®) 46
Reset the network settings to the factory default 47
Printing the Network Configuration Report 48
Printing the WLAN report (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) 48
Function table and default factory settings 49

5 Web Based Management 56

Overview 56
How to configure the machine settings using Web Based Management (web browser) 57
Setting a password 58
Secure Function Lock 2.0 59
How to configure the Secure Function Lock 2.0 settings using Web Based Management (web browser) 60
Synchronize with SNTP server 62
Store Print Log to Network 64
How to configure the Store Print Log to Network settings using Web Based Management (web browser) 64
Error Detection Setting 66
Understanding Error Messages 67
Using Store Print Log to Network with Secure Function Lock 2.0 68
Changing the Scan to FTP configuration using a web browser 68
Changing the Scan to Network configuration using a web browser (Windows®) 70

6 Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download) 72

Internet fax overview 72
Important information on Internet fax 73
How to Internet fax 74
Sending an Internet fax 74
Receiving E-mail or Internet fax 75
Additional Internet Fax options 77
Forwarding received E-mail and fax messages 77
Relay broadcasting 77
TX Verification Mail 81
Error mail 82

7 Security features 83

Overview 83
Using Certificates for device security 84
Configure certificate using Web Based Management 85
Creating and installing a certificate 86
Choosing the certificate 88
How to install the self-signed certificate on your computer 89
Import and export the certificate and private key 93
Import and export a CA certificate 94
Managing multiple certificates 94
Managing your network machine securely using SSL/TLS 95
Secure Management using Web Based Management (web browser) 95
Secure Management using BRAdmin Professional 3 (Windows®) 97
To use the BRAdmin Professional 3 utility securely, you need to follow the points below 97
Printing documents securely using SSL/TLS 98
Sending or Receiving an E-mail securely 99
Configuration using Web Based Management (web browser) 99
Sending an E-mail with user authentication 100
Sending or Receiving an E-mail securely using SSL/TLS 101
Using IEEE 802.1x authentication 102
IEEE 802.1x authentication configuration using Web Based Management (web browser) 102

8 Troubleshooting 105

Overview 105
Identifying your problem 105

Section II Network Glossary

9 Types of network connections and protocols 114

Types of network connections 114
Wired network connection example 114
Protocols 116
TCP/IP protocols and functions 116

10 Configuring your machine for a network 120

IP addresses, subnet masks and gateways 120
IP address 120
Subnet mask 121
Gateway (and router) 121
IEEE 802.1x Authentication 122

11 Wireless network terms and concepts (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) 124

Specifying your network....124
SSID (Service Set Identifier) and channels....124
Security terms....124
Authentication and encryption....124
Authentication and Encryption methods for a personal wireless network....125
Authentication and Encryption methods for an enterprise wireless network....126

12 Additional network settings from Windows® 128

Types of additional network settings....128
Installing drivers used for printing and scanning via Web Services (Windows Vista®, Windows® 7 and Windows® 8)....128
Uninstalling drivers used for printing and scanning via Web Services (Windows Vista®, Windows® 7 and Windows® 8)....130
Network printing and scanning installation for Infrastructure mode when using Vertical Pairing (Windows® 7 and Windows® 8)....131

13 Security terms and concepts 133

Security features....133
Security terms....133
Security protocols....134
Security methods for E-mail Sending and Receiving....135

Section III Appendixes

A Appendix A 137

Supported protocols and security features....137

B Appendix B 138

Using services....138
Other ways to set the IP address (for advanced users and administrators)....138
Using DHCP to configure the IP address....138
Using RARP to configure the IP address....139
Using BOOTP to configure the IP address....140
Using APIPA to configure the IP address....140
Using ARP to configure the IP address....141
Using the TELNET console to configure the IP address....142

C Index 143

Section I

Network Operation

Introduction	2
Changing your machine's network settings	5
Configuring your machine for a wireless network (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)	10
Control panel setup	36
Web Based Management	56
Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)	72
Security features	83
Troubleshooting	105

1 Introduction

Network features

Your Brother machine can be shared on a 10/100 MB wired [1] or IEEE 802.11b/g/n wireless (for wireless models) Ethernet network using the internal network print server. The print server supports various functions and methods of connection depending on the operating system you are running on a network supporting TCP/IP. The following chart shows what network features and connections are supported by each operating system.

NOTE

- Although the Brother machine can be used in both a wired [1] 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.
- For details, please refer to the Wi-Fi Direct™ Guide located on the Manuals download page for your model on the Brother Solutions Center (http://solutions.brother.com/).

[1] A wired network interface is available on the DCP-9020CDW, MFC-9330CDW and MFC-9340CDW.

Operating Systems	Windows® XP Windows Vista® Windows® 7 Windows® 8	Windows Server® 2003/2008/2012	Mac OS X v10.6.8, 10.7.x, 10.8.x
Printing	✔	✔	✔
Scanning See Software User's Guide	✔		✔
PC Fax Send [1] See Software User's Guide	✔		✔
PC Fax Receive [1] See Software User's Guide	✔		
BRAdmin Light [2] See page 5.	✔	✔	✔
BRAdmin Professional 3 [3] See page 8.	✔	✔	
Web Based Management (web browser) See page 56.	✔	✔	✔
Remote Setup [1] See Software User's Guide	✔		✔
Status Monitor See Software User's Guide	✔		✔
Driver Deployment Wizard	✔	✔	
Vertical Pairing See page 131.	✔ [4]		

1 Not available for DCP models.

2 BRAdmin Light for Macintosh is available as a download from http://solutions.brother.com/.

3 BRAdmin Professional 3 is available as a download from http://solutions.brother.com/.

4 Windows® 7 and Windows® 8 only.

Other Network features

Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)

Internet fax (IFAX) allows you to send and receive fax documents using the Internet as the transport mechanism. (See *Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)* on page 72.)

In order to use this function, please download the necessary firmware from the “Downloads” page for your model on the Brother Solutions Center at http://solutions.brother.com/. 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. For details, please refer to the user’s guide for Internet fax on the website listed above.

Security

Your Brother machine employs some of the latest network security and encryption protocols available. (See *Security features* on page 83.)

Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)

The Fax to Server feature allows the machine to scan a document and send it over the network to a separate fax server. (See *Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)* on page 44.)

In order to use this function, please download the necessary firmware from the “Downloads” page for your model on the Brother Solutions Center at http://solutions.brother.com/. Before using this function, you have to configure the necessary machine settings by using the machine’s control panel, BRAdmin Professional 3, or Web Based Management. For details, please refer to the user’s guide for Internet fax on the website listed above.

Secure Function Lock 2.0

Secure Function Lock 2.0 increases security by restricting the use of functions. (See *Secure Function Lock 2.0* on page 59.)

Store Print Log to Network

The Store Print Log to Network feature allows you to save the print log file from your Brother machine to a network server using CIFS. (See *Store Print Log to Network* on page 64.)

Brother Web Connect

Brother Web Connect allows you to download and print images and to upload files by accessing services on the Internet directly from your machine. For details, please refer to the Web Connect Guide located on the Manuals download page for your model on the Brother Solutions Center (http://solutions.brother.com/).

2 Changing your machine’s network settings

How to change your machine’s network settings (IP address, Subnet mask and Gateway)

The machine’s network settings can be changed using the control panel, BRAdmin Light, Web Based Management, and BRAdmin Professional 3. Please read this chapter for details.

Using the control panel

You can configure your machine for a network using the Network control panel menu. (See *Control panel setup* on page 36.)

Using the BRAdmin Light utility

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 for Windows®

1. Please make sure that your machine is ON.
2. Turn on your computer. Close any applications running before configuration.
3. Put the installer CD-ROM into your CD-ROM drive. The opening screen will appear automatically. If the model name screen appears, choose your machine. If the language screen appears, choose your language.
4. The CD-ROM main menu will appear. Click **Custom Installation**, and then **Network Utilities**.
5. Click **BRAdmin Light** and follow the on-screen instructions.

Installing BRAdmin Light for Macintosh

You can download Brother's latest BRAdmin Light utility from http://solutions.brother.com/.

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

NOTE

- You can download Brother's latest BRAdmin Light utility from http://solutions.brother.com/.
- If you require more advanced machine management, use the latest version of BRAdmin Professional 3 utility that is available as a download from http://solutions.brother.com/. This utility is only available for Windows® users.
- If you are using a firewall function of anti-spyware or antivirus applications, temporarily disable them. Once you are sure that you can print, re-enable the application.
- Node name: The Node name appears in the current BRAdmin Light window. The default node name of the print server in the machine is "BRNxxxxxxxxxxxx" for a wired network or "BRWxxxxxxxxxxxx" for a wireless network. ("xxxxxxxxxxxx" is your machine's MAC Address / Ethernet Address.)
- No password is required by default. Enter a password if you have set one and press **OK**.

1. Start the BRAdmin Light utility.

   ■ Windows®

   (Windows® XP/Windows® Vista/Windows® 7/Windows Server® 2003/Windows Server® 2008)

   Click (**Start**) > **All Programs** > **Brother** > **BRAdmin Light** > **BRAdmin Light**.

   (Windows® 8/Windows Server® 2012)

   Click (**BRAdmin Light**).

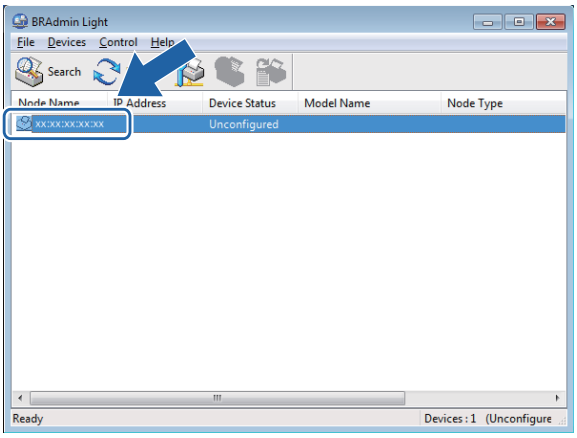
   ■ Macintosh

   When the download has completed, double click the **BRAdmin Light.jar** file to start the BRAdmin Light utility.

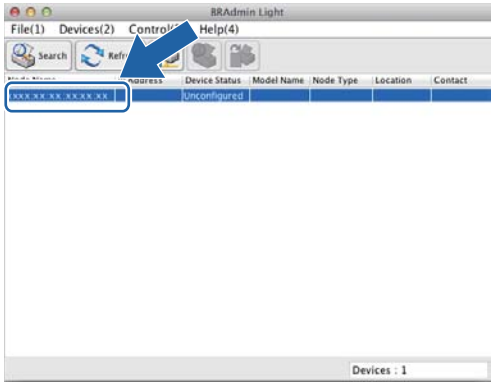
2. BRAdmin Light will search for new devices automatically.

3 Double-click the unconfigured device.

Windows®



Macintosh

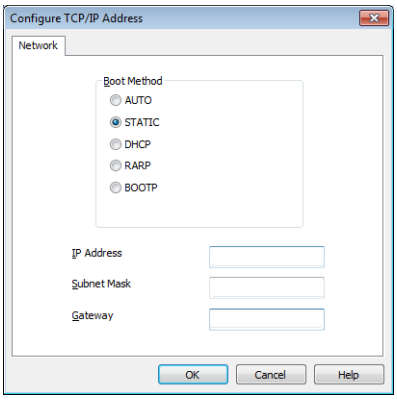


NOTE

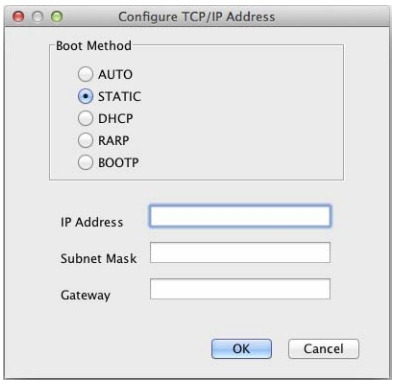
- If the print server is set to its factory default settings (if you do not use a DHCP/BOOTP/RARP server), the device will appear as **Unconfigured** in the BRAdmin Light utility screen.
- You can find the Node Name and MAC Address (Ethernet Address) by printing the Network Configuration Report (See *Printing the Network Configuration Report* on page 48). You can also find the Node Name and MAC Address from the control panel. (See *Chapter 4: Control panel setup*.)

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

Windows®



Macintosh



5 Click **OK**.

6 With the correctly programmed IP address, you will see the Brother machine in the device list.

Other Management Utilities

Your Brother machine has the following management utilities other than the BRAdmin Light utility. You can change your network settings using these utilities.

Web Based Management (web browser)

A standard web browser can be used to change your print server settings using the HTTP (Hyper Text Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer). (See *How to configure the machine settings using Web Based Management (web browser)* on page 57.)

BRAdmin Professional 3 utility (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 view the device status from an easy to read Explorer style window that changes color identifying the status of each device. You can configure network and device settings along with the ability to update device firmware from a Windows® computer on your LAN. BRAdmin Professional 3 can also log activity of Brother devices on your network and export the log data in an HTML, CSV, TXT, or SQL format.

For users who want to monitor locally connected machines, install the Print Auditor Client software on the client PC. This utility allows you to monitor machines that are connected to a client PC via the USB or parallel interface from BRAdmin Professional 3.

For more information and to download the software, visit us at http://solutions.brother.com/.

NOTE

- Please use the latest version of the BRAdmin Professional 3 utility that is available as a download from http://solutions.brother.com/. This utility is only available for Windows® users.
- If you are using a firewall function of anti-spyware or antivirus applications, temporarily disable them. Once you are sure that you can print, configure the software settings following the instructions.
- Node name: The Node name for each Brother device on the network appears in BRAdmin Professional 3. The default Node name is "BRNxxxxxxxxxxxx" for a wired network or "BRWxxxxxxxxxxx" for a wireless network. ("xxxxxxxxxxxx" is your machine's MAC Address / Ethernet Address.)

BRPrint Auditor (Windows®)

The BRPrint Auditor software brings the monitoring power of Brother network management tools to locally connected machines. This utility allows a client computer to collect usage and status information from a Brother machine connected via the parallel or USB interface. The BRPrint Auditor can then pass this information to another computer on the network running BRAdmin Professional 3. This allows the administrator to check items such as page counts, toner and drum status and the firmware version. In addition to reporting to Brother network management applications, this utility can E-mail the usage and status information directly to a predefined E-mail address in a CSV or XML file format (SMTP Mail support required). The BRPrint Auditor utility also supports E-mail notification for reporting warning and error conditions.

3 Configuring your machine for a wireless network (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)

Overview

To connect your machine to your wireless network, we recommend following one of the setup methods outlined in the Quick Setup Guide.

The wireless setup method using the installer CD-ROM and a USB cable is the easiest method for setup.

For additional wireless configuration methods, please read this chapter for more details on how to configure the wireless network settings. For information on TCP/IP settings, see *How to change your machine's network settings (IP address, Subnet mask and Gateway)* on page 5.

NOTE

- To achieve optimum results with normal everyday document printing, 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 as well as interference from other electronic devices can affect the data transfer speed of your documents.

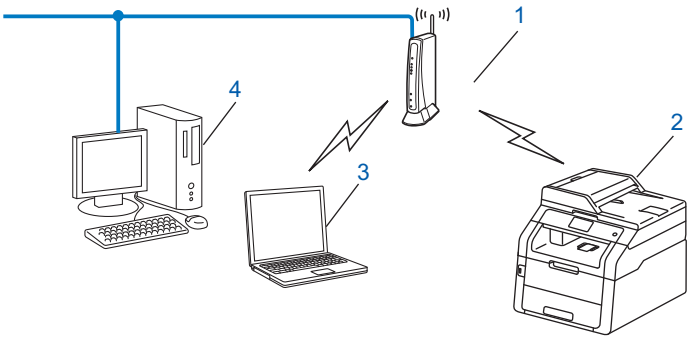
  Due to these factors, wireless may not be the best method of connection for all types of documents and applications. If you are printing large files, such as multi-page documents with mixed text and large graphics, you may want to consider choosing wired Ethernet for a faster data transfer [1], or USB for the fastest throughput speed.

- Although the Brother machine can be used in both a wired [1] 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.
- For details, please refer to the Wi-Fi Direct™ Guide located on the Manuals download page for your model on the Brother Solutions Center (http://solutions.brother.com/).
- Before configuring wireless settings, you will need to know your Network name: (SSID) and Network Key. If you are using an enterprise wireless network, you also need to know the User ID and Password.

[1] A wired network interface is available on the DCP-9020CDW, MFC-9330CDW and MFC-9340CDW.

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® MWT (My WiFi Technology), you can use your computer as a WPS (Wi-Fi Protected Setup) supported access point.

2 Wireless network machine (your machine)

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

4 Wired computer which is not wireless capable connected to the WLAN access point/router with a network cable

Configuration method

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

- Wireless configuration temporarily using a USB cable (Recommended)

  See *Wireless configuration temporarily using a USB cable (Recommended)* on page 13.

- Wireless configuration using the Setup Wizard from the control panel

  See *Configuration using the machine's control panel Setup Wizard* on page 18.

- One push wireless configuration using WPS (Wi-Fi Protected Setup™) or AOSS™

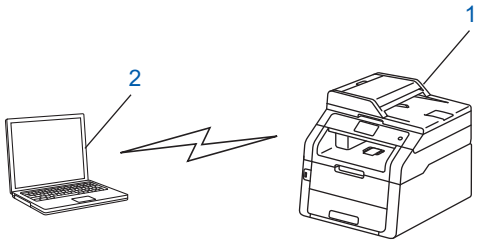
  See *One push configuration using WPS (Wi-Fi Protected Setup) or AOSS™* on page 27.

- PIN Method wireless configuration using WPS

  See *Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)* on page 29.

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 each other. When the Brother wireless machine (your machine) is part of this network, it receives all print jobs directly from the computer sending the print data.



1 Wireless network machine (your machine)

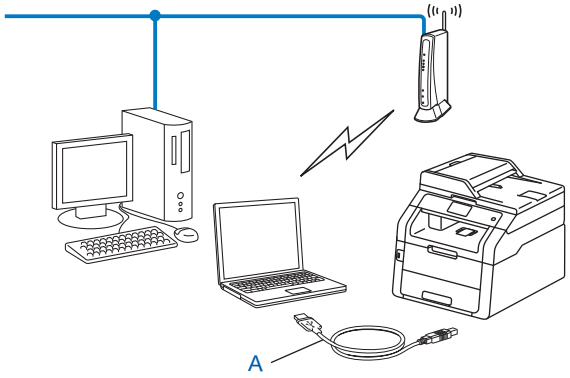
2 Wireless capable computer

We do not guarantee the wireless network connection with Windows Server® products in Ad-hoc mode. To set up your machine in Ad-hoc mode, see *Configuration in Ad-hoc mode* on page 32.

Wireless configuration temporarily using a USB cable (Recommended)

It is recommended that you use a computer wirelessly connected to your network for this method.

You can remotely configure the machine from the computer on the network using a USB cable (A) [1].



[1] You can configure the wireless settings of the machine using a USB cable temporarily connected to a wired or wireless computer.

IMPORTANT

- The following instructions will install your Brother machine in a network environment using the Brother installer application found on the CD-ROM we have provided with the machine.
- If you have previously configured the wireless settings of the machine, you must reset the LAN settings before you can configure the wireless settings again.

  To reset the LAN settings, see *Reset the network settings to the factory default* on page 47.
- If you are using the Windows® Firewall or a firewall function of anti-spyware or antivirus applications, temporarily disable them. Once you are sure that you can print, please re-enable your firewall.
- You need to temporarily use a USB cable during configuration.
- **You must know your wireless network settings before you proceed with this installation.**

  If you are going to connect your Brother machine to your network, we recommend that you contact your system administrator prior to installation.
- 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.

1 Before configuring your machine, we recommend you write down your wireless network settings. You will need this information before you continue with the configuration.

For a personal wireless network configuration

If you are configuring your machine for a smaller wireless network, such as your home environment, record your SSID and the Network key.

If you are using Windows® XP or using a network cable to connect your computer with your wireless access point/router, you need to know the SSID and Network Key of your WLAN access point/router before you proceed.

Network name: (SSID)	Network Key

For example:

Network name: (SSID)	Network Key
HELLO	12345678

For an enterprise wireless network configuration

If you are configuring your machine for an IEEE 802.1x supported wireless network, record your Authentication method, Encryption method, User ID and Password.

Network name: (SSID)

Communication Mode	Authentication method	Encryption mode	User ID	Password
Infrastructure	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

For example:

Network name: (SSID)
HELLO

Communication Mode	Authentication method	Encryption mode	User ID	Password
Infrastructure	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

NOTE

- If you configure your machine using EAP-TLS Authentication, you must install the Client Certificate issued by a CA (Certificate Authority) before you start configuration. Contact your network administrator about the Client Certificate. If you have installed more than one certificate, we recommend you write down the certificate name you want to use. For details on installing the certificate, see *Using Certificates for device security* on page 84.
- If you verify your machine using the Common Name of the Server Certificate, we recommend you write down the Common Name before you start configuration. Contact your network administrator about the Common Name of the Server Certificate.

2 Turn on your computer and put the installer CD-ROM into your CD-ROM drive.

(Windows®)

1 The opening screen will appear automatically.

If the model name screen appears, choose your machine. If the language screen appears, choose your language.

2 The CD-ROM main menu will appear. Click **Install MFL-Pro Suite** and click **Yes** if you accept the license agreements. Follow the on-screen instructions.

NOTE

- If the Brother screen does not appear automatically, go to **Computer** (**My Computer**). (For Windows® 8: Click the  (**File Explorer**) icon on the taskbar, and then go to **Computer**.) Double-click the CD-ROM icon, and then double-click **start.exe**.
- When the **User Account Control** screen appears,
  (Windows Vista®) click **Allow**.
  (Windows® 7/Windows® 8) click **Yes**.

3 Choose **Wireless Network Connection**, and then click **Next**.

4 Choose the option of the Firewall setting in the **Firewall/AntiVirus detected** screen, and then click **Next**.

(Macintosh)

1 The opening screen will appear automatically. Click **Start Here OSX**. Choose your machine and click **Next**.

2 Choose **Wireless Network Connection** and then click **Next**.

3 Choose **Yes, I have a USB cable to use for installation.** and then click **Next**.

4 Follow the on-screen instructions to configure the wireless settings.

NOTE

- When the **Available Wireless Networks** screen appears, if your access point is set to not broadcast the SSID, you can manually add it by clicking the **Advanced** button. Follow the on-screen instructions for entering the **Name (SSID)**.
- If the wireless setup failure screen appears, click **Retry** and try again.

OK! **After you have completed the wireless setup, you can proceed to the drivers and software necessary for operating your device. Click Next in the installation dialog box and follow the on-screen instructions.**

Configuration using the machine's control panel Setup Wizard

You can use the machine's control panel to configure your wireless network settings. By using the control panel `Setup Wizard` function, you can easily connect your Brother machine to your wireless network. **You must know your wireless network settings before you proceed with this installation.**

IMPORTANT

- If you have previously configured the wireless settings of the machine, you must reset the LAN settings before you can configure the wireless settings again.

  To reset the LAN settings, see *Reset the network settings to the factory default* on page 47.
- 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.

- If you are configuring your machine for a smaller wireless network, such as your home environment:
  - To configure your machine for an existing wireless network using the SSID and Network Key (if required), see *Manual configuration from the control panel* on page 19.
  - If your WLAN access point/router is set to not broadcast the SSID name, see *Configuring your machine when the SSID is not broadcast* on page 21.
  - If you are configuring your machine for Ad-hoc mode, see *Configuration in Ad-hoc mode* on page 32.
- If you are configuring your machine for an IEEE 802.1x supported wireless network, see *Configuring your machine for an enterprise wireless network* on page 23.
- If your WLAN access point/router supports WPS or AOSS™, see *One push configuration using WPS (Wi-Fi Protected Setup) or AOSS™* on page 27.
- If you are configuring your machine using WPS (PIN Method), see *Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)* on page 29.

Manual configuration from the control panel

1. Before configuring your machine, we recommend you write down your wireless network settings. You will need this information before you continue with the configuration.
   Check and record the current wireless network settings.

Network name: (SSID)	Network Key

For example:

Network name: (SSID)	Network Key
HELLO	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.
- If you see the WiFi button at the top right on the Touchscreen, you can configure the wireless settings by pressing the button. Go to step ❺.

2. Press .
3. Press `Network`.
4. Press `WLAN`.
5. Swipe up or down, or press ▲ or ▼ to display `Setup Wizard`.
   Press `Setup Wizard`.
6. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.
7. The machine will search for available SSIDs. If a list of SSIDs is displayed, press ▲ or ▼ to choose the SSID you wrote down in step ❶. Press `OK`.
   Do one of the following:
   - If you are using an authentication and encryption method that requires a Network Key, go to step ❽.
   - If your authentication method is Open System and your encryption mode is None, go to step ❿.
   - 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 choose `No (Manual)`, go to ❽ to enter the Network Key.) 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`. Go to step ❾.

8 Enter the Network Key you wrote down in step ❶. (For information on how to enter text: see Quick Setup Guide.)
Press `OK`.
When you have entered all the characters, press `Yes` to apply your settings. Go to step ❾.

9 Your machine will now try to connect to your wireless network using the information you have entered.

10 If your wireless device is connected successfully, the display shows `Connected`.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)



(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

Configuring your machine when the SSID is not broadcast

1. Before configuring your machine, we recommend you write down your wireless network settings. You will need this information before you continue with the configuration.
   Check and record 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. Press .
3. Press `Network`.
4. Press `WLAN`.
5. Swipe up or down, or press ▲ or ▼ to display `Setup Wizard`.
   Press `Setup Wizard`.
6. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.
7. The machine will search for your network and display a list of available SSIDs. Choose `<New SSID>` using ▲ or ▼.
   Press `OK`.

8 Enter the SSID name. (For information on how to enter text: see Quick Setup Guide.)
Press OK.

9 Press Infrastructure when instructed.

10 Choose and press the Authentication method.
Do one of the following:
If you chose Open System, go to step ⓫.
If you chose Shared Key, go to step ⓬.
If you chose WPA/WPA2-PSK, go to step ⓭.

11 Choose and press the Encryption type None or WEP.
Do one of the following:
If you chose None, go to step ⓯.
If you chose WEP, go to step ⓬.

12 Enter the WEP key you wrote down in step ❶. Press OK. Go to step ⓯. (For information on how to enter text: see Quick Setup Guide.)

13 Choose and press the Encryption type TKIP or AES. Go to step ⓮.

14 Enter the WPA key you wrote down in step ❶. Press OK. Go to step ⓯. (For information on how to enter text: see Quick Setup Guide.)

15 To apply the settings, press Yes. To cancel, press No.
Do one of the following:
If you chose Yes, go to step ⓰.
If you chose No, go back to step ❼.

16 The machine will attempt to connect to the wireless network you have chosen.

17 If your wireless device is connected successfully, the display shows Connected.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)

OK!

(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

Configuring your machine for an enterprise wireless network

1. Before configuring your machine, we recommend you write down your wireless network settings. You will need this information before you continue with the configuration.

   Check and record the current wireless network settings.

Network name: (SSID)

Communication Mode	Authentication method	Encryption mode	User ID	Password
Infrastructure	LEAP	CKIP		
	EAP-FAST/NONE	AES		
		TKIP		
	EAP-FAST/MS-CHAPv2	AES		
		TKIP		
	EAP-FAST/GTC	AES		
		TKIP		
	PEAP/MS-CHAPv2	AES		
		TKIP		
	PEAP/GTC	AES		
		TKIP		
	EAP-TTLS/CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAP	AES		
		TKIP		
	EAP-TTLS/MS-CHAPv2	AES		
		TKIP		
	EAP-TTLS/PAP	AES		
		TKIP		
	EAP-TLS	AES		—
		TKIP		—

For example:

Network name: (SSID)
HELLO

Communication Mode	Authentication method	Encryption mode	User ID	Password
Infrastructure	EAP-FAST/MS-CHAPv2	AES	Brother	12345678

NOTE

- If you configure your machine using EAP-TLS Authentication, you must install the Client Certificate issued by a CA before you start configuration. Contact your network administrator about the Client Certificate. If you have installed more than one certificate, we recommend you write down the certificate name you want to use. For installing the certificate, see *Using Certificates for device security* on page 84.
- If you verify your machine using the Common Name of the Server Certificate, we recommend you write down the Common Name before you start configuration. Contact your network administrator about the Common Name of the Server Certificate.

2. Press .
3. Press `Network`.
4. Press `WLAN`.
5. Swipe up or down, or press ▲ or ▼ to display `Setup Wizard`.
   Press `Setup Wizard`.
6. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.
7. The machine will search for your network and display a list of available SSIDs.
   You should see the SSID you wrote down earlier. If the machine finds more than one network, swipe up or down, or press ▲ or ▼ to choose your network. Go to step ⓫. Press `OK`.
   If your access point is set to not broadcast the SSID, you will have to add the SSID name manually. Go to step ❽.
8. Swipe up or down, or press ▲ or ▼ to choose `<New SSID>`. Press `OK`.
   Go to step ❾.
9. Enter the SSID name. (For information on how to enter text: see Quick Setup Guide.)
   Press `OK`. Go to step ❿.
10. Choose `Infrastructure` when instructed.
11. Choose the Authentication method using ▲ or ▼.
    Do one of the following:
    If you chose `LEAP`, go to step ⓱.
    If you chose `EAP-FAST`, go to step ⓬.
    If you chose `PEAP`, go to step ⓬.
    If you chose `EAP-TTLS`, go to step ⓬.
    If you chose `EAP-TLS`, go to step ⓭.

12 Choose the Inner Authentication method `NONE`, `CHAP`, `MS-CHAP`, `MS-CHAPv2`, `GTC` or `PAP`.
Go to step 13.

NOTE

Depending on your Authentication method, the Inner Authentication method selections differ.

13 Choose encryption type `TKIP` or `AES`.
Do one of the following:
If your Authentication method is EAP-TLS, go to step 14.
For other Authentication methods, go to step 15.

14 The machine will display a list of available Client Certificates. Choose the certificate and go to step 15.

15 Choose the verification method `No Verification`, `CA` or `CA + Server ID`.
Do one of the following:
If you chose `CA + Server ID`, go to step 16.
For other selections, go to step 17.

NOTE

If you have not imported a CA certificate on your machine, the machine will display `No Verification`.
To import a CA certificate, see *Using Certificates for device security* on page 84.

16 Enter the server ID. (For information on how to enter text: see Quick Setup Guide.)
Press `OK`. Go to step 17.

17 Enter the user ID you wrote down in step ❶. Press OK. (For information on how to enter text: see Quick Setup Guide.)
Do one of the following:
If your Authentication method is EAP-TLS, go to step ⓳.
For other Authentication methods, go to step ⓲.

18 Enter the Password you wrote down in step ❶. Press OK. Go to step ⓳.

19 To apply the settings, choose Yes. To cancel, choose No.
Do one of the following:
If you chose Yes, go to step ⓴.
If you chose No, go back to step ❼.

20 The machine will attempt to connect to the wireless network you have chosen.

21 If your wireless device is connected successfully, the display shows Connected.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)

OK!

(Windows®)

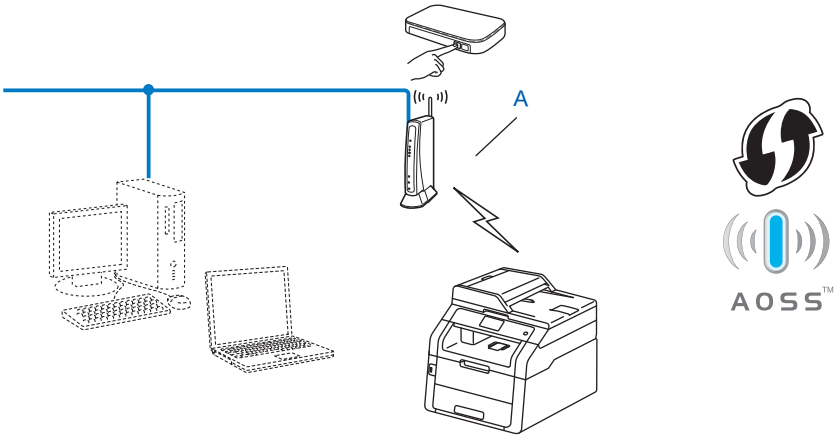
You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

One push configuration using WPS (Wi-Fi Protected Setup) or AOSS™

You can use WPS or AOSS™ from the control panel menu to configure your wireless network settings if your WLAN access point/router (A) supports either WPS (PBC [1]) or AOSS™.



[1] Push Button Configuration

IMPORTANT

- If you are going to connect your Brother machine to your network, we recommend that you contact your system administrator prior to installation. **You must know your wireless network settings before you proceed with this installation.**
- If you have previously configured the wireless settings of the machine, you must reset the LAN settings before you can configure the wireless settings again.

  To reset the LAN settings, see *Reset the network settings to the factory default* on page 47.

1. Press .
2. Press `Network`.
3. Press `WLAN`.
4. Swipe up or down, or press ▲ or ▼ to display `WPS/AOSS`.
   Press `WPS/AOSS`.
5. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.

6 When the Touchscreen shows `Start WPS or AOSS on your wireless access point/router, then press [OK].`, press the WPS or AOSS™ button on your wireless access point/router. See the user's guide for your wireless access point/router for instructions.
Then press `OK` and your machine will now automatically detect which mode (WPS or AOSS™) your wireless access point/router uses and try to connect to your wireless network.

7 If your wireless device is connected successfully, the display shows `Connected`.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)



(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

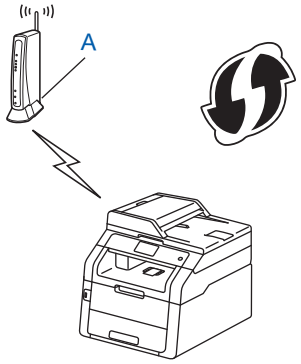
(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

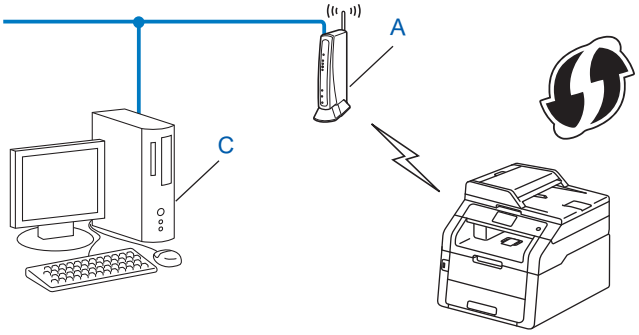
Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)

If your WLAN access point/router supports WPS (PIN Method), you can configure the machine easily. The PIN (Personal Identification Number) Method is one of the connection methods developed by the Wi-Fi Alliance®. By inputting a PIN which is created by an Enrollee (your machine) to the Registrar (a device that manages the wireless LAN), you can setup the WLAN network and security settings. See the user's guide supplied with your WLAN access point/router for instructions on how to access the WPS mode.

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



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



[1] The Registrar is a device that manages the wireless LAN.

NOTE

Routers or access points that support WPS have a symbol as shown below.



1. Press .
2. Press `Network`.
3. Press `WLAN`.
4. Swipe up or down, or press ▲ or ▼ to display `WPS w/ PIN Code`.
   Press `WPS w/ PIN Code`.
5. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.
6. The Touchscreen will show an 8 digit PIN and the machine starts searching for an access point.
7. Using a computer that is on the network, type “http://access point’s IP address/” into your browser. (Where “access point’s IP address” is the IP address of the device that is used as the Registrar [1].) Go to the WPS setting page and input the PIN which the Touchscreen shows in ❻ to the Registrar. Follow the on-screen instructions.

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

NOTE

The setting page is different, depending on the brand of access point / router. See the instruction manual supplied with your access point / router.

Windows Vista®/Windows® 7/Windows® 8

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

NOTE

- To use a Windows Vista®, Windows® 7 or Windows® 8 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 or Windows® 8 as a Registrar, you can install the printer driver after the wireless configuration by following the on-screen instructions. If you want to install the full driver and software package: see Quick Setup Guide.

1 (Windows Vista®)
Click the button and then **Network**.

(Windows® 7)
Click the button, and then **Devices and Printers**.

(Windows® 8)
Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, and then click **Control Panel**. In the **Hardware and Sound** group, click **View devices and printers**.

2 (Windows Vista®)
Click **Add a wireless device**.

(Windows® 7/Windows® 8)
Click **Add a device**.

3 Choose your machine and click **Next**.

4 Type the PIN which the Touchscreen shows in step ❻, and then click **Next**.

5 Choose your network and then click **Next**.

6 Click **Close**.

8 If your wireless device is connected successfully, the display shows `Connected`.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)

OK!

(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

Configuration in Ad-hoc mode

Using configured SSID

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

1. Before configuring your machine, we recommend you write down your wireless network settings. You will need this information before you continue 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 a SSID already configured. For instructions on how to configure your computer to Ad-hoc mode, please 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. Press .
3. Press `Network`.
4. Press `WLAN`.

5 Swipe up or down, or press ▲ or ▼ to display `Setup Wizard`.
Press `Setup Wizard`.

6 When `Enable WLAN?` is displayed, press `Yes` to accept.
This will start the wireless setup wizard.
To cancel, press `No`.

7 The machine will search for your network and display a list of available SSIDs. Choose the SSID you wrote down in step ❶ using ▲ or ▼.
Press `OK`.
Do one of the following:
If the SSID is unencrypted, go to step ❿.
If the SSID is encrypted, go to step ❽.

8 Enter the WEP key you wrote down in step ❶. Press `OK`. Go to step ❾. (For information on how to enter text: see Quick Setup Guide.)

9 To apply the settings, press `Yes`. To cancel, press `No`.
Do one of the following:
If you chose `Yes`, go to step ❿.
If you chose `No`, go back to step ❼.

10 The machine will attempt to connect to the wireless device you have chosen.

11 If your wireless device is connected successfully, the display shows `Connected`.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)

OK!

(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

Using a New SSID

If you are using a new SSID then all other devices will connect using the SSID that you assign to the machine in the following steps. You will need to connect to this SSID from your computer when it is placed in Ad-hoc mode.

1. Press .
2. Press `Network`.
3. Press `WLAN`.
4. Swipe up or down, or press ▲ or ▼ to display `Setup Wizard`.
   Press `Setup Wizard`.
5. When `Enable WLAN?` is displayed, press `Yes` to accept.
   This will start the wireless setup wizard.
   To cancel, press `No`.
6. The machine will search for your network and display a list of available SSIDs. Choose `<New SSID>` using ▲ or ▼. Press `OK`.
7. Enter the SSID name. (For information on how to enter text: see Quick Setup Guide.)
   Press `OK`.
8. Press `Ad-hoc` when instructed.
9. Choose and press the Encryption type `None` or `WEP`.
   Do one of the following:
   If you chose `None`, go to step ⓫.
   If you chose `WEP`, go to step ⓾.
10. Enter the WEP key. Press `OK`. Go to step ⓫. (For information on how to enter text: see Quick Setup Guide.)

NOTE

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

11 To apply the settings, press `Yes`. To cancel, press `No`.
Do one of the following:
If you chose `Yes`, go to step ⓬.
If you chose `No`, go back to step ❻.

12 The machine will attempt to connect to the wireless device you have chosen.

13 If your wireless device is connected successfully, the display shows `Connected`.
The machine will print your machine's wireless status report. If the connection failed, check the error code on the printed report. (See Quick Setup Guide: *Troubleshooting*.)



(Windows®)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Install MFL-Pro Suite from the CD-ROM menu.

(Macintosh)

You have completed the wireless network setup. If you would like to continue installing drivers and software necessary for operating your device, please choose Start Here OSX from the CD-ROM menu.

4 Control panel setup

Network menu

The Network menu selections of the control panel allow you to set up the Brother machine for your network configuration. (For more information on how to use the control panel: see Basic User's Guide.) Press , All Settings and then press Network. Proceed to the menu selection you wish to configure. (For additional information on the menu, see *Function table and default factory settings* on page 49.)

Please note that the machine is supplied with the BRAdmin Light utility [1], Web Based Management or Remote Setup [2] applications, which also can be used to configure many aspects of the network. (See *Other Management Utilities* on page 8.)

[1] For Macintosh users, you can download Brother's latest BRAdmin Light utility from http://solutions.brother.com/.

[2] Not available for DCP models.

TCP/IP

If you connect the machine with a network cable to your network, use the Wired LAN menu selections. If you connect the machine to a wireless Ethernet network, use the WLAN menu selections.

Boot Method

This selection controls how the machine obtains an IP address.

Auto mode

In this mode, the machine will scan the network for a DHCP server. If it can find one, and if the DHCP server is configured to allocate an IP address to the machine, then the IP address supplied by the DHCP server will be used. If no DHCP server is available, the IP Address is set using the APIPA protocol. After the machine is initially powered ON, it may take a few minutes for the machine to scan the network for a server.

Static mode

In this mode the machine's IP address must be manually assigned. Once entered the IP address is locked to the assigned address.

NOTE

If you do not want your print server configured via DHCP, BOOTP, or RARP, you must set the BOOT Method to Static so that the print server has a static IP address. This will prevent the print server from trying to obtain an IP address from any of these systems. To change the Boot Method, use the machine's control panel, BRAdmin Light utility, Web Based Management, or Remote Setup.

IP Address

This field displays the current IP address of the machine. If you have chosen a `BOOT Method` of `Static`, enter the IP address that you wish to assign to the machine (check with your network administrator for the IP address to use). If you have chosen a method other than `Static`, the machine will attempt to determine its IP address using the DHCP or BOOTP protocols. The default IP address of your machine will probably be incompatible with the IP address numbering scheme of your network. We recommend that you contact your network administrator for an IP address for the network the unit will be connected on.

Subnet Mask

This field displays the current subnet mask used by the machine. If you are not using DHCP or BOOTP to obtain the subnet mask, enter the desired subnet mask. Check with your network administrator for the subnet mask to use.

Gateway

This field displays the current gateway or router address used by the machine. If you are not using DHCP or BOOTP to obtain the gateway or router address, enter the address you wish to assign. If you do not have a gateway or router, leave this field blank. Check with your network administrator if you are unsure.

Node Name

You can register the machine name on the Network. This name is often referred to as a NetBIOS name; it will be the name that is registered by the WINS server on your network. Brother recommends the name “BRNxxxxxxxxxxx” for a wired network or “BRWxxxxxxxxxxx” for a wireless network. (“xxxxxxxxxxx” is your machine’s MAC Address / Ethernet Address.)

WINS Config

This selection controls how the machine obtains the IP address of the WINS server.

Auto

Automatically uses a DHCP request to determine the IP addresses for the primary and secondary WINS servers. You must set the BOOT Method to `Auto` for this feature to work.

Static

Uses a specified IP address for the primary and secondary WINS servers.

WINS Server

Primary WINS Server IP Address

This field specifies the IP address of the primary WINS (Windows® Internet Name Service) server. If set to a non-zero value, the machine will contact this server to register its name with the Windows® Internet Name Service.

Secondary WINS Server IP Address

This field specifies the IP address of the secondary WINS server. It is used as a backup to the Primary WINS server address. If the Primary server is unavailable, the machine still can register itself with a secondary server. If set to a non-zero value, the machine will contact this server to register its name with the Windows® Internet Name Service. If you have a primary WINS server, but no secondary WINS server, simply leave this field blank.

DNS Server

Primary DNS Server IP Address

This field specifies the IP address of the primary DNS (Domain Name System) server.

Secondary DNS Server IP Address

This field specifies the IP address of the secondary DNS server. It is used as a backup to the Primary DNS server address. If the Primary server is unavailable, the machine will contact the Secondary DNS server. If you have a primary DNS server, but no secondary DNS server, simply leave this field blank.

APIPA

The setting of `On` will cause the print server to automatically allocate a Link-Local IP address in the range (169.254.1.0 - 169.254.254.255) when the print server cannot obtain an IP address through the Boot Method you have set. (See *Boot Method* on page 36.) Choosing `Off` means the IP address does not change, when the print server cannot obtain an IP address through the Boot Method you have set.

IPv6

This machine is compatible with IPv6, the next generation Internet protocol. If you want to use the IPv6 protocol, choose `On`. The default setting for IPv6 is `Off`. For more information on the IPv6 protocol, visit http://solutions.brother.com/.

NOTE

- If you set IPv6 to `On`, turn off the power switch and then turn it back on to enable this protocol.
- After you choose IPv6 `On`, this setting will be applied to both the wired and wireless LAN interface.

Ethernet (wired network only)

Ethernet link mode auto allows the print server to operate in 100BASE-TX full or half duplex or in 10BASE-T full or half duplex mode by auto negotiation.

NOTE

If you set this value incorrectly, you may not be able to communicate with your print server.

Wired Status (For HL-3180CDW, DCP-9015CDW, DCP-9020CDN, DCP-9020CDW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)

This field displays the current wired network status.

Setup Wizard (wireless network only)

The `Setup Wizard` guides you through the wireless network configuration. (For more information: see Quick Setup Guide or *Manual configuration from the control panel* on page 19.)

WPS (Wi-Fi Protected Setup)/AOSS™ (wireless network only)

If your WLAN access point/router supports either WPS (PBC [1]) or AOSS™ (Automatic Wireless mode), you can configure the machine easily. (For more information: see Quick Setup Guide or *One push configuration using WPS (Wi-Fi Protected Setup) or AOSS™* on page 27.)

[1] Push Button Configuration

WPS (Wi-Fi Protected Setup) w/PIN Code (wireless network only)

If your WLAN access point/router supports WPS (PIN Method), you can configure the machine easily. (For more information, see *Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)* on page 29.)

WLAN Status (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)

Status

This field displays the current wireless network status.

Signal

This field displays the current wireless network signal strength.

SSID

This field displays the current wireless network SSID. The display shows up to 32 characters of the SSID name.

Comm. Mode

This field displays the current wireless network communication mode.

MAC Address

The MAC address is a unique number assigned for the machine's network interface. You can check your machine's MAC address from the control panel.

Set to Default

The `Set to Default` allows you to reset each wired or wireless settings to the factory default. If you want to reset both wired and wireless settings, see *Reset the network settings to the factory default* on page 47.

Wired Enable (For DCP-9020CDW, MFC-9330CDW and MFC-9340CDW)

If you want to use the wired network connection, set `Wired Enable` to `On`.

WLAN Enable

If you want to use the wireless network connection, set `WLAN Enable` to `On`.

NOTE

If a network cable is connected to your machine, set `Wired Enable` to `Off`.

E-mail / IFAX (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)

This menu has five selections: `Mail Address`, `Setup Server`, `Setup Mail RX`, `Setup Mail TX` and `Setup Relay`. As this section requires you to enter a lot of text characters, you may find that it is more convenient to use Web Based Management and your favorite web browser to configure these settings (see *Web Based Management* on page 56). These settings must be configured for the IFAX feature to work. (For more details about Internet fax, see *Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)* on page 72.)

You can also access the character you want by repeatedly pressing the appropriate number key using the machine's control panel. (For information on how to enter text: see Basic User's Guide.)

Mail Address

You can set your machine's E-mail address.

Setup Server

SMTP

- SMTP Server

  This field displays the node name or IP address of an SMTP mail server (outgoing E-mail server) on your network.

  (e.g. "mailhost.brothermail.net" or "192.000.000.001")

- SMTP Port

  This field displays the SMTP port number (for outgoing E-mails) on your network.

- Auth. for SMTP

  You can specify the security method for E-mail notification. (For details on the security methods for E-mail notification, see *Sending or Receiving an E-mail securely* on page 99.)

- SMTP SSL/TLS

  You can choose the encryption method between the machine and the SMTP server.

- Verify Cert.

  You can enable or disable the use of the security certificate between the machine and the SMTP server.

POP3

- POP3 Server

  This field displays the node name or IP address of the POP3 server (incoming E-mail server) used by the Brother machine. This address is necessary for the Internet fax features to function correctly.

  (e.g. "mailhost.brothermail.net" or "192.000.000.001")

- POP3 Port

  This field displays the POP3 port number (for incoming E-mails) used by the Brother machine.

- Mailbox Name

  You can specify a mailbox name on the POP3 server where the Internet print jobs are to be retrieved.

- Mailbox Pwd

  You can specify the password for the POP3 server account where the Internet print jobs are to be retrieved.

NOTE

To set for no password, enter a single space.

- POP3 SSL/TLS

  You can choose the encryption method between the machine and the POP3 server.

- Verify Cert.

  You can enable or disable the use of the security certificate between the machine and the POP3 server.
- APOP

  You can enable or disable the APOP (Authenticated Post Office Protocol).

Setup Mail RX

Auto Polling

When set to `On`, the machine automatically checks the POP3 server for new messages.

Poll Frequency

Sets the interval for checking for new messages on the POP3 server (default is 10 minutes).

Header

This selection allows the contents of the mail header to be printed when the received message is printed.

Delete Error Mail

When set to `On`, the machine automatically deletes error mails that the machine cannot receive from the POP3 server.

Notification

The notification feature allows a confirmation of receipt message to be transmitted to the sending station when the Internet Fax has been received.

This feature only works on Internet Fax machines that support the “MDN” specification.

Setup Mail TX

Sender Subject

This field displays the subject that is attached to the Internet fax data being sent from the Brother machine to a computer (default is “`Internet Fax Job`”).

Size Limit

Some E-mail servers do not allow you to send large E-mail documents (the system administrator will often place a limit on the maximum E-mail size). With this function enabled, the machine will display `Out of Memory` when trying to send E-mail documents over 1 Mbyte in size. The document will not be sent and an error report will be printed. The document you are sending should be separated into smaller documents that will be accepted by the mail server. (For your information, a 42 page document based on the ITU-T Test Chart #1 test chart is approximately 1 Mbyte in size.)

Notification

The notification feature allows a confirmation of receipt message to be transmitted to the sending station when the Internet Fax has been received.

This feature only works on Internet Fax machines that support the “MDN” specification.

Setup Relay

Relay Broadcast

This function allows the machine to receive a document over the Internet, and then relay it to other fax machines through conventional analog landlines.

Relay Domain

You can register the Domain Names (Max. 10) that are allowed to request a Relay Broadcast.

Relay Report

A Relay Broadcast Report can be printed at the machine that will act as a Relay Station for all Relay Broadcasts.

Its primary function is to print reports of any relayed broadcasts that have been sent through the machine. Please note: In order to use this function, you must assign the relay domain in the “Trusted Domains” section of the Relay function settings.

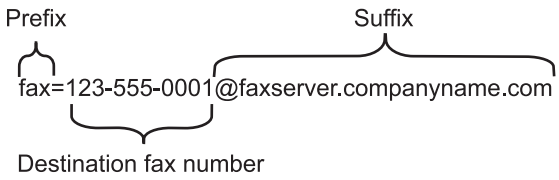
NOTE

For more information on Relay Broadcast, see *Relay broadcasting* on page 77.

Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)

The Fax to Server feature allows the machine to scan a document and send it over the network to a separate fax server. The document will then be sent from the server as fax data to the destination fax number over standard phone lines. When the Fax to Server feature is set to `On`, all automatic fax transmissions from the machine will be sent to the fax server for fax transmission. You can also continue to send a fax directly from the machine using the manual fax feature.

To send a document to the fax server, the correct syntax for that server must be used. The destination fax number must be sent with a prefix and a suffix that match the parameters used by the fax server. In most cases, the syntax for the prefix is “fax=” and the syntax for the suffix would be the domain name of the fax server E-mail gateway. The suffix must also include the “@” symbol at the beginning of the suffix. The prefix and the suffix information must be stored in the machine before you can use the Fax to Server function. Destination fax numbers can be saved in the Speed Dial locations or entered using the dial pad (up to 20 digit numbers). For example, if you wanted to send a document to a destination fax number of 123-555-0001, use the following syntax:



NOTE

Your fax server application must support an E-mail gateway.

Setting Fax to Server to On

You can store the prefix/suffix address for the fax server in the machine.

1. Press .
2. Press `All Settings`.
3. Swipe up or down, or press ▲ or ▼ to display `Network`.
   Press `Network`.
4. Swipe up or down, or press ▲ or ▼ to display `Fax to Server`.
   Press `Fax to Server`.
5. Press `On`.
6. Press `Prefix`.
7. Enter the prefix using the on-screen keyboard.
8. Press `OK`.
9. Press `Suffix`.
10. Enter the suffix using the on-screen keyboard.
11. Press `OK`.
12. Press .

NOTE

- You can enter the prefix and suffix address using a total of up to 40 characters.
- For information on how to enter text: see Basic User's Guide.

How to operate Fax to Server

1. Place the document in the ADF or on the scanner glass.
2. Enter the fax number.
3. Press `Fax Start`.
   The machine will send the message over a TCP/IP network to the fax server.

How to set a new default for Scan to FTP

You can choose the default color and file type for the Scan to FTP function. (For how to operate Scan to FTP: see Software User's Guide.)

How to set a new default for Scan to Network (Windows®)

You can choose the default color and file type for the Scan to Network function to scan a document directly to a server supporting CIFS on your local network or on the Internet. (For information about the CIFS protocol, see *CIFS* on page 119.) (For how to operate Scan to Network: see Software User's Guide.)

Reset the network settings to the factory default

You can reset the print server back to its default factory settings (resetting all information such as the password and IP address information).

NOTE

- This function resets all wired and wireless network settings to the factory default.
- You can also reset the print server back to its factory default settings using the BRAdmin applications or Web Based Management. (For more information, see *Other Management Utilities* on page 8.)

1. Press .
2. Press `All Settings`.
3. Swipe up or down, or press ▲ or ▼ to display `Network`.
   Press `Network`.
4. Swipe up or down, or press ▲ or ▼ to display `Network Reset`.
   Press `Network Reset`.
5. Press `Yes`.
6. Press `Yes` for 2 seconds to confirm.

Printing the Network Configuration Report

NOTE

Node name: The Node name appears on the Network Configuration Report. The default node name is “BRNxxxxxxxxxxx” for a wired network or “BRWxxxxxxxxxxx” for a wireless network. (“xxxxxxxxxxx” is your machine’s MAC Address / Ethernet Address.)

The Network Configuration Report prints a report listing all the current network configuration including the network print server settings.

1. Press .
2. Press `All Settings`.
3. Swipe up or down, or press ▲ or ▼ to display `Print Reports`.
   Press `Print Reports`.
4. Press `Network Configuration`.
5. Press `OK`.

NOTE

If the **IP Address** on the Network Configuration Report shows **0.0.0.0**, wait for one minute and try again.

Printing the WLAN report (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)

The `WLAN Report` prints your machine’s wireless status report. If the wireless connection failed, check the error code on the printed report. See Quick Setup Guide: *Troubleshooting*.

1. Press .
2. Press `All Settings`.
3. Swipe up or down, or press ▲ or ▼ to display `Print Reports`.
   Press `Print Reports`.
4. Swipe up or down, or press ▲ or ▼ to display `WLAN Report`.
   Press `WLAN Report`.
5. Press `OK`.

Function table and default factory settings

The factory settings are shown in Bold with an asterisk.

NOTE

(For MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)

- Internet Fax, Fax to Server and Scan to E-mail Server functions are available as downloads.
- In order to use this function, please download the necessary firmware from the “Downloads” page for your model on the Brother Solutions Center at http://solutions.brother.com/.

Main Menu	Submenu	Menu Selections		Options
Network	**Wired LAN** (DCP-9020CDN, DCP-9020CDW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)	**TCP/IP**	**BOOT Method**	**Auto*** Static RARP BOOTP DHCP (If you choose Auto, RARP, BOOTP or DHCP, you will be asked to enter how many times the machine tries to obtain the IP address.)
			IP Address	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]
			Subnet Mask	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]
			Gateway	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			Node Name	BRNxxxxxxxxxxx (up to 32 characters)
			WINS Configuration	**Auto*** Static
			WINS Server	Primary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** Secondary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***

Main Menu	Submenu	Menu Selections		Options
Network (continued)	**Wired LAN** (DCP-9020CDN, DCP-9020CDW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW) (continued)	**TCP/IP** (continued)	**DNS Server**	Primary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** Secondary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			APIPA	**On*** Off
			IPv6	On **Off***
		Ethernet	—	**Auto*** 100B-FD 100B-HD 10B-FD 10B-HD
		Wired Status	—	Active 100B-FD Active 100B-HD Active 10B-FD Active 10B-HD Inactive Wired OFF (Not available for DCP-9020CDN)
		MAC Address	—	—
		Set to Default	—	Yes No
		Wired Enable (DCP-9020CDW, MFC-9330CDW and MFC-9340CDW)	—	**On*** Off
	WLAN (HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)	**TCP/IP**	**BOOT Method**	**Auto*** Static RARP BOOTP DHCP (If you choose Auto, RARP, BOOTP or DHCP, you will be asked to enter how many times the machine tries to obtain the IP address.)

Main Menu	Submenu	Menu Selections		Options
Network (continued)	**WLAN** (HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) (continued)	**TCP/IP** (continued)	**IP Address**	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]
			Subnet Mask	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** [1]
			Gateway	[000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			Node Name	BRWxxxxxxxxxxx (up to 32 characters)
			WINS Configuration	**Auto*** Static
			WINS Server	Primary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** Secondary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			DNS Server	Primary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]*** Secondary [000-255].[000-255].[000-255].[000-255] **[000].[000].[000].[000]***
			APIPA	**On*** Off
			IPv6	On **Off***
		Setup Wizard	—	—
		WPS/AOSS	—	—
		WPS w/ PIN Code	—	—

Main Menu	Submenu	Menu Selections		Options
Network (continued)	**WLAN** (HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) (continued)	**WLAN Status**	**Status**	Active(11n) Active(11b) Active(11g) Wired LAN Active (Not available for HL-3180CDW, DCP-9015CDW, MFC-9130CW) WLAN Off AOSS Active Connection Fail
			Signal	Strong Medium Weak None
			SSID	—
			Comm. Mode	Ad-hoc Infrastructure None
		MAC Address	—	—
		Set to Default	—	Yes No
		WLAN Enable	—	On **Off***
	Wi-Fi Direct[2] (HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)	**Push Button**	—	—
		PIN Code	—	—
		Manual	—	—
		Group Owner	—	On **Off***
		Device Information	**Device Name**	—
			SSID	—
			IP Address	—

Main Menu	Submenu	Menu Selections			Options
Network (continued)	**Wi-Fi Direct** [2] (HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW) (continued)	**Status Information**		**Status**	G/O Active(**) ** = number of devices Client Active Not Connected Off Wired LAN Active (Not available for HL-3180CDW, DCP-9015CDW, MFC-9130CW)
				Signal	Strong Medium Weak None (When Group Owner is On, the signal is set to Strong.)
		I/F Enable		—	On **Off***
	E-mail/IFAX (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)	**Mail Address**		—	Name (Up to 60 characters)
		Setup Server	**SMTP**	**SMTP Server**	Name (Up to 64 characters) IP Address [000-255].[000-255].[000-255].[000-255]
				SMTP Port	**25*** [00001-65535]
				Auth. for SMTP	**None*** SMTP-AUTH POP bef. SMTP
				SMTP SSL/TLS	**None*** SSL TLS
				Verify SMTPCert.	On **Off***

Main Menu	Submenu	Menu Selections			Options
Network (continued)	**E-mail/IFAX** (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW) (continued)	**Setup Server** (continued)	**POP3**	**POP3 Server**	Name (Up to 64 characters) IP Address [000-255].[000-255].[000-255].[000-255]
				POP3 Port	**110*** [00001-65535]
				Mailbox Name	(Up to 60 characters)
				Mailbox Password	(Up to 32 characters)
				POP3 SSL/TLS	**None*** SSL TLS
				Verify POP3Cert.	On **Off***
				APOP	On **Off***
		Setup Mail RX	**Auto Polling**	**Auto Polling**	**On*** Off
				Poll Frequency (When **Auto Polling** is set to On.)	**10 minutes*** (1 minute to 60 minutes)
			Header	—	All Subject+From+To **None***
			Delete Error Mail	—	**On*** Off
			Notification	—	On MDN **Off***

Main Menu	Submenu	Menu Selections			Options
Network (continued)	**E-mail/IFAX** (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW) (continued)	**Setup Mail TX**	**Sender Subject**	—	**Internet Fax Job*** (Up to 40 characters)
			Size Limit	—	On **Off***
			Notification	—	On **Off***
		Setup Relay	**Relay Broadcast**	—	On **Off***
			Relay Domain	—	RelayXX: Relay(01 - 10)
			Relay Report	—	On **Off***
		Manual POP3 Receive		—	—
	Web Connect Settings [3]	**Proxy Settings**		**Proxy Connection**	On **Off***
				Address	—
				Port	**8080***
				User Name	—
				Password	—
	Fax to Server (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW)	**Fax to Server**	—	—	On **Off***
		Prefix **Suffix**	—	—	—
	Network Reset	—	—	—	Yes No

[1] On connection to the network, the machine will automatically set the IP address and Subnet Mask to values appropriate for your network.

[2] For details, please see the Wi-Fi Direct™ Guide located on the Manuals download page for your model on the Brother Solutions Center (http://solutions.brother.com/).

[3] For details, please see the Web Connect Guide located on the Manuals download page for your model on the Brother Solutions Center (http://solutions.brother.com/).

5 Web Based Management

Overview

A standard Web Browser can be used to manage your machine using the HTTP (Hyper Text Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer). You can perform the function listed or get the following information from a machine on your network using a web browser.

- Machine status information
- Change Fax configuration items, such as General Setup, Address Book settings and Remote Fax (for MFC models).
- Change network settings such as TCP/IP information
- Configure Secure Function Lock 2.0 (see *Secure Function Lock 2.0* on page 59).
- Configure Store Print Log to Network (see *Store Print Log to Network* on page 64).
- Configure Scan to FTP (see *Changing the Scan to FTP configuration using a web browser* on page 68).
- Configure Scan to Network (see *Changing the Scan to Network configuration using a web browser (Windows®)* on page 70).
- Software version information of the machine and print server
- Change network and machine configuration details

NOTE

We recommend to use Windows® Internet Explorer® 8.0/9.0 or Safari 5.0 for Macintosh. Please also make sure that JavaScript and Cookies are always enabled in whichever browser you use. If a different web browser is used, 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 programmed into the print server and your computer.

How to configure the machine settings using Web Based Management (web browser)

A standard web browser can be used to change your print server settings using the HTTP (Hyper Text Transfer Protocol) or HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer).

NOTE

- We recommend to use HTTPS protocol for your security when configuring the settings using Web Based Management.
- When you use the HTTPS protocol for Web Based Management configuration, your browser will display a warning dialog box.

1. Start your web browser.
2. Type “http://machine’s IP address/” into your browser’s address bar (where “machine’s IP address” is the IP address of the machine or the print server name).
   - For example: http://192.168.1.2/

NOTE

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

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

  The NetBIOS name can be seen in the Network Configuration Report (see *Printing the Network Configuration Report* on page 48).
- For Macintosh users, you can have easy access to the Web Based Management System by clicking the machine icon on the **Status Monitor** screen. For more information: see Software User's Guide.

3. No password is required by default. If you have previously set a password, enter it and press →.
4. You can now change the print server settings.

NOTE

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

Setting a password

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

1. Click **Administrator**.
2. Enter the password you want to use (up to 32 characters).
3. Re-enter the password in **Confirm New Password** box.
4. Click **Submit**.
   From the next time you access the Web Based Management, enter the password in the **Login** box, and then click .
   After configuring the settings, logout by clicking .

NOTE

You can also set a password by clicking **Please configure the password** on the machine's web page if you are not setting a login password.

Secure Function Lock 2.0

Secure Function Lock 2.0 from Brother helps you to save money and increase security by restricting the functions available on your Brother machine.

Secure Function Lock allows you to configure passwords for selected users. You can grant access to some or all of these functions, or restrict them to a page limit. This means that only authorized people can use them.

You can configure and change the following Secure Function Lock 2.0 settings using Web Based Management or BRAdmin Professional 3 (Windows® only).

- **Print** [1] [2]
- **USB Direct Print** [3]
- **Copy**
- **Color Print** [1] [2] [5]
- **Page Limit** [5]
- **Fax TX** [3]
- **Fax RX** [3]
- **Scan** [4]
- **Web Connect** (**Upload**) [3]
- **Web Connect** (**Download**) [3]
- **Page Counter** [5]

[1] **Print** includes print jobs sent via AirPrint, Google Cloud Print and Brother iPrint&Scan.

[2] If you register the PC user login names, you can restrict PC print without the user entering a password. For more detail, see *Restricting PC print by PC user login name* on page 61.

[3] Supported models only.

[4] Scan includes scan jobs sent via Brother iPrint&Scan.

[5] Available for **Print**, **USB Direct Print**, **Copy** and **Web Connect** (**Download**).

How to configure the Secure Function Lock 2.0 settings using Web Based Management (web browser)

Basic configuration

1. Click **Administrator** on the machine's web page, and then click **Secure Function Lock**.
2. Choose **On** from **Function Lock**.
3. Enter an alphanumeric group name or user name of up to 15 digits in the **ID Number/Name** box, and then enter a four-digit password in the **PIN** box.
4. Uncheck the functions that you want to restrict in the **Print Activities** box or the **Others** box. If you want to configure the maximum page count, check the **On** check box in **Page Limit**, and then enter the number in the **Max.** box. Then click **Submit**.

NOTE

If you want to restrict the PC printing by PC user login name, click **PC Job Restriction by Login Name** and configure the settings. (See *Restricting PC print by PC user login name* on page 61.)

Scanning when using Secure Function Lock 2.0

The Secure Function Lock 2.0 feature allows the administrator to restrict which users are allowed to scan. When the scan feature is set to off for the public user setting, only users who have scan selected in the check box will be able to scan. To push scan from the control panel of the machine, users must enter their PIN to access the scan mode. To pull scan from their computer, restricted users must also enter their PIN on the control panel of the machine before they can scan from their computer. If the PIN is not entered at the machine's control panel, the user will get an error message on their computer when they attempt to pull scan.

Setting up public mode

You can set up the public mode to restrict what functions are available for public users. Public users do not need to enter a password to access the features made available through this setting.

NOTE

Public mode includes print jobs sent via AirPrint, Google Cloud Print and Brother iPrint&Scan.

1. Uncheck the check box for the function that you want to restrict in the **Public Mode** box.
2. Click **Submit**.

Restricting PC print by PC user login name

By configuring this setting, the machine can authenticate by PC user login name to allow a print job from a registered computer.

1. Click **PC Job Restriction by Login Name**.
2. Choose **On** from **PC Job Restriction**.
3. Choose the ID Number you set in the **ID Number/Name** in step ❸. See *Basic configuration* on page 60 from the **ID Number** drop-down list for each Login Name and then enter the PC user login name in the **Login Name** box.
4. Click **Submit**.

NOTE

- If you want to restrict PC print per group, choose the same ID Number for each PC login name you want in the group.
- If you are using the PC login name feature, you must also make sure that the **Use PC Login Name** box in the printer driver is checked. For more information about the printer driver: see Software User's Guide.
- The Secure Function Lock feature does not support the BR-Script3 driver for printing.

Other features

You can set up the following features in Secure Function Lock 2.0:

■ **All Counter Reset**

You can reset the page counter by clicking **All Counter Reset**.

■ **Export to CSV file**

You can export the current page counter, including **ID Number/Name** information, as a CSV file.

■ **Last Counter Record**

The machine retains the page count after the counter has been reset.

■ **Counter Auto Reset**

You can automatically reset the page counters by configuring the time interval based on Daily, Weekly, or Monthly settings.

Synchronize with SNTP server

SNTP is the protocol used to synchronize the time used by the machine for authentication with the SNTP time server (this time is not the time displayed on the Touchscreen of the machine). You can synchronize the time used by the machine on a regular basis with the Coordinated Universal Time (UTC) provided by the SNTP time server.

NOTE

This function is not available in some countries.

1. Click **Network**, and then click **Protocol**.
2. Select the **SNTP** check box to activate the setting.
3. Click **Advanced Setting**.

   ■ **Status**

   Displays whether the SNTP server settings are enabled or disabled.

   ■ **SNTP Server Method**

   Choose **AUTO** or **STATIC**.

   - **AUTO**

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

   - **STATIC**

     Enter the address you want to use.

   ■ **Primary SNTP Server Address**, **Secondary SNTP Server Address**

   Enter 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. If you have a Primary SNTP server, but no Secondary SNTP server, simply leave this field blank.

   ■ **Primary SNTP Server Port**, **Secondary SNTP Server Port**

   Enter the Port number (1 to 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. If you have a Primary SNTP port, but no Secondary SNTP port, simply leave this field blank.

■ **Synchronization Interval**

Enter the number of hours between server synchronization attempts (1 to 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. You can also configure the date and time from the machine's control panel.



- Choose the **Synchronize with SNTP server** check box. You also need to verify your time zone settings correctly. Choose 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-05:00.

■ **Synchronization Status**

You can confirm the latest synchronization status.

4 Click **Submit** to apply the settings.

Store Print Log to Network

The Store Print Log to Network feature allows you to save the print log file from your Brother machine to a network server using CIFS [1]. You can record the ID, type of print job, job name, user name, date, time and the number of printed pages for every print job.

[1] CIFS is the Common Internet File System protocol that runs over TCP/IP allowing computers on a network to share files over an intranet or the Internet.

The following print functions are recorded in the print log:

- Print jobs from your computer
- USB Direct Print (Supported models only)
- Copy
- Received Fax (Supported models only)
- Web Connect Print

NOTE

- The Store Print Log to Network feature supports **Kerberos** Authentication and **NTLMv2** Authentication.

  You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly on the control panel for Authentication. (For information about setting SNTP, see *Synchronize with SNTP server* on page 62. For information about setting the date, time and time zone: see Quick Setup Guide.)
- You can set the file type to **TXT** or **CSV** when storing a file to the server.

How to configure the Store Print Log to Network settings using Web Based Management (web browser)

1. Click **Administrator** on the machine's web page, and then click **Store Print Log to Network**.
2. Choose **On** from **Print Log**.
3. You can configure the following settings using a web browser.
   - **Host Address**

     The Host Address is the Host name of the CIFS server. Enter the Host Address (for example: mypc.example.com) (up to 64 characters) or the IP address (for example: 192.168.56.189).
   - **Store Directory**

     Enter the destination folder where your log will be stored on the CIFS server (for example: brother\abc) (up to 60 characters).
   - **File Name**

     Enter the file name you want to use for the print log (up to 15 characters).
   - **File Type**

     Choose the file type **TXT** or **CSV** for the print log.

■ **Auth. Method**

Choose the authentication method required for access to the CIFS server **Auto**, **Kerberos** [1], or **NTLMv2** [2].

[1] Kerberos is an authentication protocol which allows devices or individuals to securely prove their identity to network servers using a single sign-on.

[2] NTLMv2 is the authentication method used by Windows to log into servers.

- **Auto**: If you choose Auto, the machine will initially search for a Kerberos server. If the Kerberos server is not detected, NTLMv2 will be used for the authentication method.
- **Kerberos**: Choose Kerberos to use Kerberos Authentication only.
- **NTLMv2**: Choose NTLMv2 to use NTLMv2 Authentication only.

For Kerberos and NTLMv2 Authentication, you must also configure the Date&Time settings or the SNTP protocol (network time server).

For configuring the Date&Time and the SNTP settings, see *Synchronize with SNTP server* on page 62.

You can also configure the Date&Time settings from the machine's control panel. See Quick Setup Guide.

■ **Username**

Enter the Username for the authentication (up to 96 characters).

NOTE

If the username is part of a domain, please input the username in one of the following styles: user@domain or domain\user.

■ **Password**

Enter the password for the authentication (up to 32 characters).

■ **Kerberos Server Address** (if needed)

Enter the KDC Host Address (for example: mypc.example.com) (up to 64 characters) or the IP address (for example: 192.168.56.189).

■ **Error Detection Setting** (See *Error Detection Setting* on page 66.)

4 In the **Connection Status**, you can confirm the last log status. For more information, see *Understanding Error Messages* on page 67.

5 Click **Submit** to display the **Test Print Log to Network** page.
To test your settings, click **Yes** and go to step ❻.
To skip the test, click **No**. Your settings will be submitted automatically.

6 The machine will test your settings.

7 If your settings are accepted, **Test OK** appears on the page.
If **Test Error** appears, check all settings, and then click **Submit** to display the Test page again.

Error Detection Setting

You can choose what action is taken when the print log cannot be stored to the server due to a network error.

1. Choose **Cancel Print** or **Ignore Log & Print** in the **Error Detection Setting** of **Store Print Log to Network**.

   ■ **Cancel Print**

   If you choose **Cancel Print**, the print jobs are canceled when the print log cannot be stored to the server.

NOTE

Even if you choose **Cancel Print**, your machine will print a received fax.

   ■ **Ignore Log & Print**

   If you choose **Ignore Log & Print**, the machine prints the document even if the print log cannot be stored to the server.

   When the store print log function has recovered, the print log is recorded as follows:

   - If the log cannot be stored at the end of printing, the print log except the number of printed pages will be recorded. (1)
   - If the Print Log cannot be stored at the beginning and the end of printing, the print log of the job will not be recorded. When the function has recovered, the occurrence of an error is shown in the log. (2)

   Example of the print log:

```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52, 21
2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?, ?      (1)
3, <Error>, ?, ?, ?, ?, ?, ?                                                  (2)
4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4, 4
```

2. Click **Submit** to display the **Test Print Log to Network** page.
   To test your settings, click **Yes** and go to step ❸.
   To skip the test, click **No**. Your settings will be submitted automatically.
3. The machine will test your settings.
4. If your settings are accepted, **Test OK** appears on the page.
   If **Test Error** appears, check all settings, and then click **Submit** to display the Test page again.

Understanding Error Messages

You can confirm the error status on the Touchscreen of your machine or **Connection Status** in Web Based Management.

■ `Server Timeout, contact your administrator.`

This message will appear when you cannot connect to the server.
Make sure that:

- Your server address is correct.
- Your server is connected to the network.
- The machine is connected to the network.

■ `Authentication Error, contact your administrator.`

The message will appear when your **Authentication Setting** is not correct.
Make sure that:

- The Username [1] and Password in Authentication Setting are correct.

  [1] If the username is part of a domain, please input the username in one of the following styles: user@domain or domain\user.

- The time of the log file server matches the time from the SNTP server, or the **Date&Time** settings.
- The SNTP time server settings are configured correctly so the time matches the time used for authentication by Kerberos or NTLMv2. If there is no SNTP server, make sure the **Date&Time** and **Time Zone** settings are set correctly using Web Based Management or the control panel so the machine matches the time being used by the server providing the authentication.

■ `File Access Error, contact your administrator.`

This message will appear when you cannot access the destination folder.
Make sure that:

- The store directory name is correct.
- The store directory is write-enabled.
- The File is not locked.

■ `Wrong Date&Time, contact your administrator.`

This message will appear when your machine does not obtain the time from the SNTP time server. Make sure that:

- The settings to access the SNTP time are correct using Web Based Management.
- In Web Based Management, confirm the **Date & Time** settings of your machine are correct.

NOTE

If you choose the **Cancel Print** option in Web Based Management, the `Log Access Error` message will remain on the Touchscreen for about 60 seconds.

Using Store Print Log to Network with Secure Function Lock 2.0

When Secure Function Lock 2.0 is active, the names of the registered users for copy, Fax RX, Web Connect Print and USB Direct Print (if available) functions will be recorded in the Store Print Log to Network report.

Example of the Print Log with Secure Function Lock 2.0 users:

```
Id, Type, Job Name, User Name, Date, Time, Print Pages, Color Pages
1, Copy, -, -, 04/04/20xx, 09:05:12, 3, 3
2, Fax, -, -, 04/04/20xx, 09:45:30, 5, 0
3, Copy, -, "Bob", 04/04/20xx, 10:20:30, 4, 0
4, Fax, -, "Bob", 04/04/20xx, 10:35:12, 3, 0
5, USB Direct, -, "John", 04/04/20xx, 11:15:43, 6, 6
```


Changing the Scan to FTP configuration using a web browser

Scan to FTP allows you to scan a document directly to an FTP server on your local network or on the Internet. For more details on Scan to FTP: see Software User's Guide.

1. Click **Scan** on the machine's web page, and then click **Scan to FTP/Network**.
2. You can choose what profile numbers (1 to 10) to use for Scan to FTP settings.
   You can also store two user defined file names that can be used for creating an FTP Server Profile in addition to the seven preset file names in **Create a User Defined File Name**. A maximum of 15 characters can be entered in each of the two fields.
3. Click **Submit**.

4 Click **Scan to FTP/Network Profile** on the **Scan** page.
Now you can configure and change the following Scan to FTP settings using a web browser:

- **Profile Name** (Up to 15 characters)
- **Host Address** (FTP server address)
- **Username**
- **Password**
- **Store Directory**
- **File Name**
- **Quality**
- **File Type**
- **Glass Scan Size**
- **File Size**
- **Remove Background Color**
- **Passive Mode**
- **Port Number**

You can 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.

NOTE

Scan to FTP is available when FTP server profiles are configured using Web Based Management.

5 Click **Submit**.

Changing the Scan to Network configuration using a web browser (Windows®)

Scan to Network allows you to scan documents directly to a shared folder on a CIFS [1] server located on your local network or the Internet: see Software User's Guide for more details on Scan to Network

[1] The Common Internet File System (CIFS) is the standard way that computer users share files and printers in Windows®.

NOTE

Scan to Network supports Kerberos Authentication and NTLMv2 Authentication.

You must configure the SNTP protocol (network time server), or you must set the date, time and time zone correctly on the control panel for authentication. (For information about setting SNTP, see *Synchronize with SNTP server* on page 62. For information about setting the date, time and time zone: see Quick Setup Guide.)

1. Click **Scan** on the machine's web page, and then click **Scan to FTP/Network**.
2. Choose **Network** in the profile numbers (1 to 10) you want to use for Scan to Network settings. You can also store two user defined file names that can be used for creating a Scan to Network Profile in addition to the seven preset file names in **Create a User Defined File Name**. A maximum of 15 characters can be entered in each of the two fields.
3. Click **Submit**.

4 Click **Scan to FTP/Network Profile** on the **Scan** page.
Now you can configure and change the following Scan to Network settings using a web browser:

- **Profile Name** (Up to 15 characters)
- **Host Address**
- **Store Directory**
- **File Name**
- **Quality**
- **File Type**
- **Glass Scan Size**
- **File Size**
- **Remove Background Color**
- **Use PIN for Authentication**
- **PIN Code**
- **Auth. Method**
- **Username**
- **Password**
- **Kerberos Server Address**

NOTE

Scan to Network is available when Network server profiles are configured using Web Based Management.

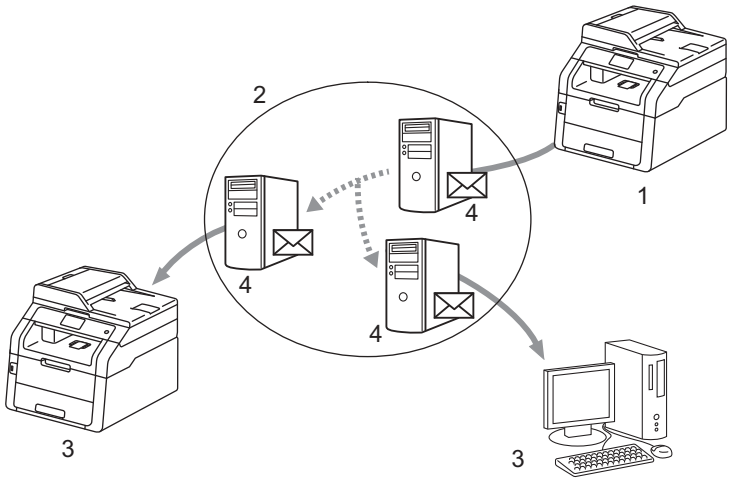
5 Click **Submit**.

6 Internet fax (MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download)

Internet fax overview

Internet faxing (IFAX) allows you to send and receive fax documents using the Internet as the transport mechanism. Documents are transmitted in E-mail messages as attached TIFF-F files. This means that computers are also able to receive and send documents, providing that the computer has as an application that can generate and view TIFF-F files, you can use any TIFF-F viewer application. Any documents sent via the machine will automatically be converted into a TIFF-F format. If you wish to send and receive messages to and from your machine, your mail application on the computer must be able to support the MIME format.

In order to use this function, please download the necessary firmware from the “Downloads” page for your model on the Brother Solutions Center at http://solutions.brother.com/.



1 Sender

2 Internet

3 Receiver

4 E-mail server

NOTE

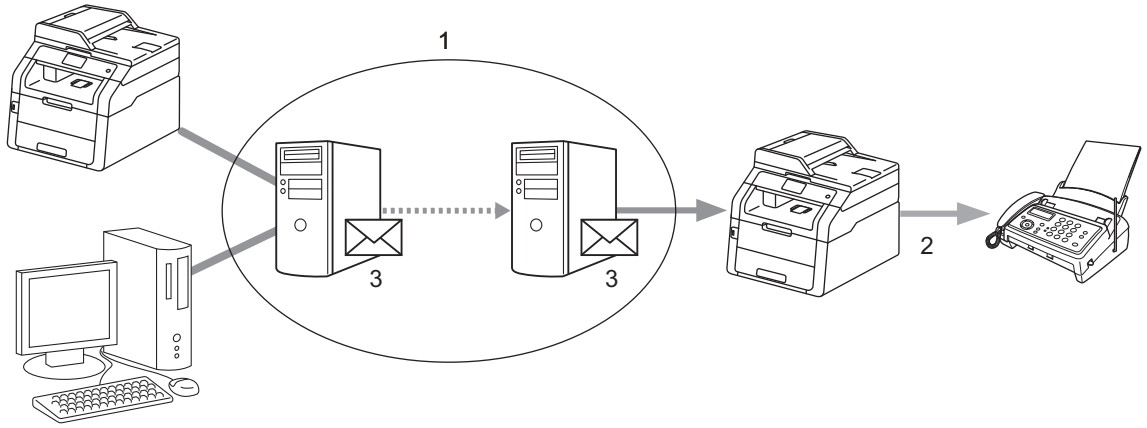
Internet Fax is available in Black & White only.

■ Forwarding received E-mail and fax messages

You can forward received E-mail or standard fax messages to another E-mail address or fax machine. For more information see *Forwarding received E-mail and fax messages* on page 77.

■ Relay broadcast

If you want to fax the document long distance (such as abroad), the "relay broadcast" function allows you to save the communication fee. This function allows the Brother machine to receive the document over the Internet, and then relay it to other fax machines through conventional telephone lines. For more information see *Relay broadcasting* on page 77.



1 Internet

2 Telephone line

3 E-mail server

Important information on Internet fax

Internet fax communication on a LAN system is basically the same as communication via E-mail; however, it is different from fax communication using standard phone lines. The following is important information for using Internet fax:

■ Factors such as the receiver's location, structure of the LAN system, and how busy the circuit (such as the Internet) is may cause the system to take a long time. (normally 20 sec. to 30 sec.)

■ In the case of transmission through the Internet, due to its low level of security, we recommend that you use standard phone lines to send confidential documents.

■ If the receiver's mail system is not compatible with the MIME format, you cannot transmit a document to the receiver. Depending on the receiver's server, there may be some cases in which the error mail will not be sent back.

■ If the size of a document's image data is too large, there is a possibility of unsuccessful transmission.

■ You cannot change the font or character size of Internet mail that you received.

How to Internet fax

Before using Internet fax you must configure your Brother machine to communicate with your network and mail server. You can configure these items from the control panel, Web Based Management, Remote setup, or BRAdmin Professional 3. You must ensure 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.)
- E-mail address
- SMTP, POP3 server address/port/Authentication method/Encryption method/Server Certificate Verification
- Mailbox name and password

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

Sending an Internet fax

Before sending an Internet fax

To send an Internet fax, you can configure the following items from the control panel, Web Based Management or Remote Setup.

- Sender Subject (if needed)
- Size Limit (if needed)
- Notification (if needed) (For more information, see *TX Verification Mail* on page 81.)

How to send an Internet fax

Sending an Internet fax is the same as sending a normal fax (for more information: see Basic User's Guide: *Sending a fax*). If you have already programmed the addresses of the destination Internet fax machines as Speed-Dial locations, you can send the Internet fax by loading the document into the machine. If you want to change the resolution, choose `Fax Resolution` from the FAX menu to set the preferred resolution, choose a Speed Dial (`S.Fine` is not supported for Internet fax).

NOTE

- If you wish to manually enter the Internet fax address, load the document into the machine and do one of the following.
  - Press  and then press  to choose numbers, characters, or special characters. Enter the address, and then press `Fax Start`.

  For more information to manually enter the Internet fax address: see Basic User's Guide.
- You can register the E-mail address information from Web Based Management or Remote Setup.

After the document is scanned, it is transmitted to the recipient Internet fax machine automatically via your SMTP server. You can cancel the send operation by pressing  during scanning. After the transmission is finished, the machine will return to standby mode.

NOTE

Some E-mail servers do not allow you to send large E-mail documents (the system administrator will often place a limit on the maximum E-mail size). With this function enabled, the machine will display `Out of Memory` when trying to send E-mail documents over 1 Mbyte in size. The document will not be sent and an error report will be printed. The document you are sending should be separated into smaller documents that will be accepted by the mail server. (For your information, a 42 page document based on the ITU-T Test Chart #1 test chart is approximately 1 Mbyte in size.)

Receiving E-mail or Internet fax

Before receiving an Internet fax

To receive an Internet fax, you should configure the following items from the control panel, Web Based Management or Remote Setup:

- Auto Polling (if needed)
- Poll Frequency (if needed)
- Header (if needed)
- Delete Error Mail (if needed)
- Notification (if needed) (For more information, see *TX Verification Mail* on page 81.)

How to receive an Internet fax

There are 2 ways you can receive E-mail messages:

- POP3 receiving at regular intervals
- POP3 receiving (manually initiated)

Using POP3 receiving the machine must poll the E-mail server to receive the data. This polling can occur at set intervals (for example, you can configure the machine to poll the E-mail server at 10 minute intervals) or you can manually poll the server by pressing , `All Settings`, `Network`, `E-mail/IFAX`, and then `Manual POP3 Receive`.

If your machine starts to receive E-mail data, the Touchscreen will reflect this activity. For example, you will see `Receiving` on the Touchscreen followed by `XX/XX E-mail(s)`. If you press , `All Settings`, `Network`, `E-mail/IFAX`, and then `Manual POP3 Receive` to manually poll the E-mail server for E-mail data and there are no mail documents waiting to be printed, the machine will display `No Mail` on the Touchscreen for two seconds.

NOTE

- If your machine is out of paper when receiving data, the received data will be held in the machine's memory. This data will be printed automatically after paper is re-inserted into the machine.
- If the received mail is not in a plain text format or an attached file is not in the TIFF-F format, the following error message will be printed: "**ATTACHED FILE FORMAT NOT SUPPORTED. FILE NAME:XXXXXX.doc**" If the received mail is too large, the following error message will be printed: "**E-MAIL FILE TOO LARGE.**". If Delete POP Receive Error Mail is ON (default) then the error mail is automatically deleted from the E-mail server.

Receiving an Internet fax to your computer

When a computer receives an Internet fax document, the document is attached to a mail message that informs the computer that it has received a document from an Internet fax. This is notified in the subject field of the received mail message.

NOTE

If the computer to which you wish to send a document is not running Windows® XP, Windows Server® 2003/2008/2012, Windows Vista®, Windows® 7 or Windows® 8, please inform the computer's owner that they may need to install some software that can view TIFF-F files.

Additional Internet Fax options

Forwarding received E-mail and fax messages

You can forward received E-mail or standard fax messages to another E-mail address or fax machine. Received messages can be forwarded via E-mail to a computer or Internet fax. They can also be forwarded via standard phone lines to another machine.

The setting can be enabled using a web browser or through the control panel of the machine. The steps for configuring fax forward can be found in the Advanced User's Guide if supported by your machine.

Relay broadcasting

This function allows the Brother machine to receive a document over the Internet, and then relay it to other fax machines through conventional telephone lines.

Before relaying broadcast

To relay broadcast, you must configure the following items from the control panel, Web Based Management, or Remote Setup:

- Relay Broadcast

  You must enable the relay broadcast.

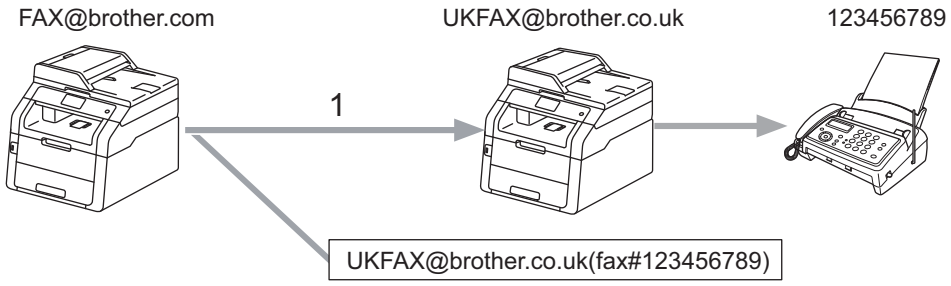
- Relay Domain

  You must configure your machine’s domain name on the machine that will broadcast the document to the conventional fax machine. If you wish to use your machine as a relay broadcast device, you must specify the domain name that you trust at the machine, in other words, the portion of the name after the “@” sign. Use care in selecting a trusted domain since any user on a trusted domain will be able to send a relay broadcast.

  You can register up to 10 domain names.

- Relay Report

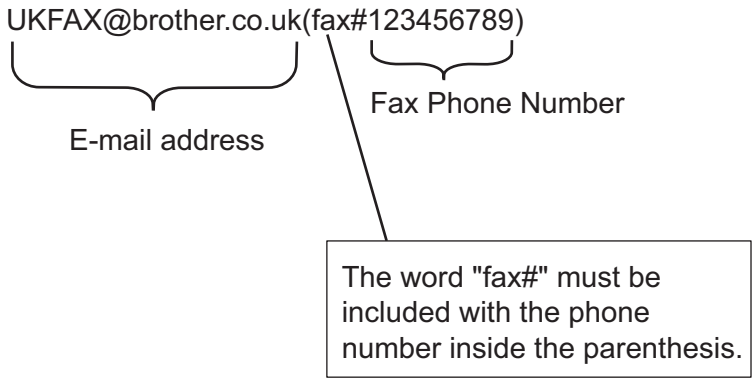
Relay broadcast from a machine



1 Internet

In this example, your machine has an E-mail address of FAX@brother.com, you wish to send a document from this machine to another machine in England with an E-mail address of UKFAX@brother.co.uk, this machine will then forward the document to a standard fax machine using a conventional telephone line. If your E-mail address is FAX@brother.com, you must configure a trusted domain name of brother.com on the machine in England that will broadcast the document to the conventional fax machine. If you do not enter the domain name information, then the machine in the middle (the machine that will broadcast the document) will not trust any Internet jobs that it receives from the machine in the @brother.com domain.

After the trusted domain is set you can send the document from your machine [e.g. FAX@brother.com] by entering the E-mail address of the machine [e.g. UKFAX@brother.co.uk] that will forward the document followed by the phone number of the fax that will receive the document. The following is an example of how to enter the E-mail address and phone number.

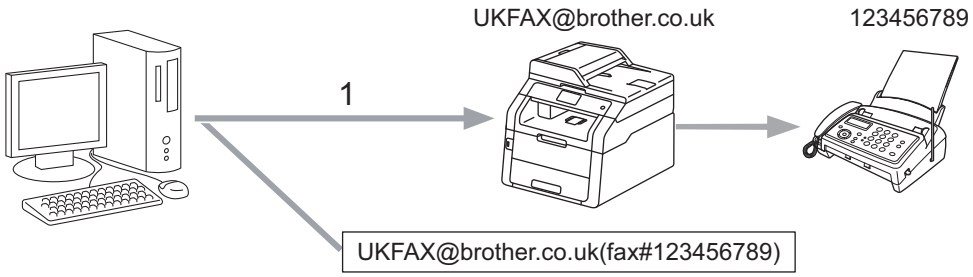


Sending to multiple phone numbers:

If you want to have the document relayed to more than one standard fax machine, the address can be entered using the following method:

1. Press `Fax`.
2. Load your document.
3. Press `Options`.
4. Swipe up or down, or press ▲ or ▼ to display `Broadcasting`.
   Press `Broadcasting`.
5. Press `Add Number`.
6. You can add E-mail addresses to the broadcast in the following ways:
   - Press `Add Number` and press , enter the E-mail address and press `OK`.
   - Press `Add from Address book`.
     Press the check boxes of the E-mail address you want to add to the broadcast.
     After you have checked all the E-mail address you want, press `OK`.
   - Press `Search in Address book`.
     Enter the name and press `OK`.
     The search results will be displayed. Press the name and then press the E-mail address you want to add to the broadcast.
7. After you have entered all the E-mail addresses by repeating step ❻, press `OK`.
8. Press `Fax Start`.

Relay broadcast from a computer



1 Internet

You can also send E-mail from your computer and have it relayed to a conventional fax machine. The method of entering the phone number of the conventional fax machine that will receive the relayed E-mail will vary depending on the mail application you are using. The following are some examples of different mail applications:

Some E-mail applications do not support sending to multiple phone numbers. If your E-mail application cannot support multiple phone numbers you will only be able to relay to one fax machine at a time.

Enter the address of the relay machine and phone number of the fax in the “TO” box using the same method used when sending from a machine.

UKFAX@brother.co.uk(fax#123456789)

NOTE

For Microsoft® Outlook® 97 or greater, the address information must be entered into the address book as follows:

Name: fax#123456789

E-mail address: UKFAX@brother.co.uk

TX Verification Mail

Transmission Verification Mail supports two separate functions. Verification Mail for sending allows you to request notification from the receiving station that the Internet Fax or E-mail was received and processed. Verification Mail for receiving allows you to transmit a default report back to the sending station after successfully receiving and processing an Internet Fax or E-mail.

To use this feature you must set the `Notification` option within the `Setup Mail RX` and `Setup Mail TX` options.

Setup Mail TX

You can set the `Notification` option in the `Setup Mail TX` option to either `On` or `Off`. When switched to `On` an additional field of information is sent with the image data. This field is named “MDN”.

MDN (Message Disposition Notification):
This field requests the status of the Internet Fax/E-mail message after delivery through the SMTP (Simple Mail Transfer Protocol) transport system. Once the message has arrived at the receiver this data is used when the machine or user reads or prints the received Internet Fax or E-mail. For example, if the message is opened for reading or is printed the receiver sends back a notification to the original sending machine or user.

The receiver must support the MDN field in order to be able to send a notification report, otherwise the request will be ignored.

Setup Mail RX

There are three possible settings for this option `On`, `MDN` or `Off`.

Receive Notification “`On`”

When switched to “`On`” a fixed message is sent back to the sender to indicate successful reception and processing of the message. These fixed messages depend on the operation requested by the sender.

Report messages consist of:

`SUCCESS: Received From <mail address>`

Receive Notification “`MDN`”

When switched to “`MDN`” a report as described above is sent back to the sender if the originating station sent the “`MDN`” field to request confirmation.

Receive Notification “`Off`”

Off switches all forms of receive notification `Off`, no message is sent back to the sender regardless of the request.

NOTE

To receive the TX verification mail properly, you must configure the following settings.

- Sender
  - Switch Notification in the Setup Mail TX to on.
  - Switch Header in the Setup Mail RX to All or Subject+From+To.
- Receiver
  - Switch Notification in the Setup Mail RX to on.

Error mail

If there is a mail delivery error while sending an Internet fax, the mail server will send an error message back to the machine and the error message will be printed. If there is an error while receiving mail, an error message will be printed (Example: “The message being sent to the machine was not in a TIFF-F format.”).

To receive the error mail properly, you must switch Header in the Setup Mail RX to All or Subject+From+To.

7 Security features

Overview

In today's world, there are many security threats to your network and the data that travels over it. Your Brother machine employs some of the latest network security and encryption protocols available today. These network features can be integrated into your overall network security plan to help protect your data and prevent unauthorized access to the machine. This chapter explains how to configure them.

You can configure the following security features:

- Managing your network machine securely using SSL/TLS (See *Managing your network machine securely using SSL/TLS* on page 95.)
- Managing your network machine securely using SNMPv3 protocol (See *Secure Management using Web Based Management (web browser)* on page 95 or *Secure Management using BRAdmin Professional 3 (Windows®)* on page 97.)
- Secure Management using BRAdmin Professional 3 (Windows®) (See *Secure Management using BRAdmin Professional 3 (Windows®)* on page 97.)
- Printing documents securely using SSL/TLS (See *Printing documents securely using SSL/TLS* on page 98.)
- Sending and Receiving an E-mail securely (See *Sending or Receiving an E-mail securely* on page 99.)
- Using IEEE 802.1x authentication (See *Using IEEE 802.1x authentication* on page 102.)
- Certificate for secure management (See *Using Certificates for device security* on page 84.)
- Managing multiple certificates (See *Managing multiple certificates* on page 94.)

NOTE

We recommend to disable the Telnet, FTP and TFTP protocols. Accessing the machine using these protocols is not secure. (For how to configure the protocol settings, see *How to configure the machine settings using Web Based Management (web browser)* on page 57.) If you disable FTP, the Scan to FTP function will be disabled.

Using Certificates for device security

Your Brother machine supports the use of multiple security certificates allowing secure management, authentication and communication with the machine. The following security certificate features can be used with the machine.

- SSL/TLS communication
- IEEE 802.1x authentication
- SSL communication for SMTP/POP3

The Brother machine supports the following certificates.

- Pre-installed certificate

  Your machine has a pre-installed self-signed certificate.

  Using this certificate, you can easily use the SSL/TLS communication without creating or installing a certificate.

NOTE

The pre-installed self-signed certificate cannot protect your communication from spoofing. We recommend using a certificate that is issued by a trusted organization for better security.

- Self-signed certificate

  This print server issues its own certificate. Using this certificate, you can easily use the SSL/TLS communication without having a certificate from a CA. (See *Creating and installing a certificate* on page 86.)

- Certificate from a CA

  There are two methods for installing a certificate from a CA. If you already have a certificate from a CA or if you want to use a certificate from an external trusted CA:

  - When using a CSR (Certificate Signing Request) from this print server. (See *How to create a CSR* on page 87.)
  - When importing a certificate and a private key. (See *Import and export the certificate and private key* on page 93.)

- CA certificate

  If you use a CA certificate that identifies the CA (Certificate Authority) itself and owns its private key, you must import a CA certificate from the CA prior to the configuration. (See *Import and export a CA certificate* on page 94.)

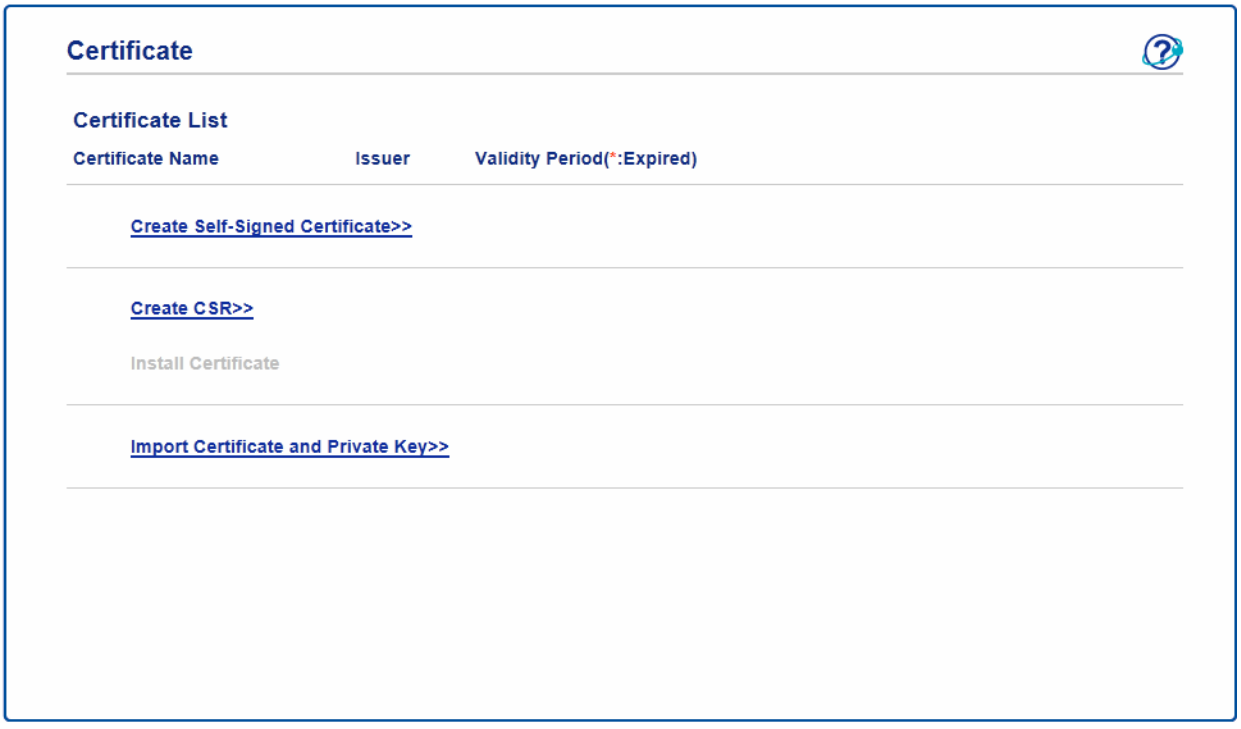
NOTE

- If you are going to use SSL/TLS communication, we recommend that you contact your system administrator first.
- When you reset the print server back to its default factory settings, the certificate and the private key that are installed will be deleted. If you want to keep the same certificate and the private key after resetting the print server, export them before resetting and re-install them. (See *How to export the self-signed certificate, the certificate issued by a CA, and the private key* on page 93.)

Configure certificate using Web Based Management

This feature can be configured using Web Based Management only. Follow these steps to access the configure certificate page using Web Based Management.

1. Start your web browser.
2. Type “http://machine’s IP address/” into your browser’s address bar (where “machine’s IP address” is the IP address of the machine or the print server name).
   - For example: http://192.168.1.2/
3. No password is required by default. If you have previously set a password, enter it and press →.
4. Click **Network**.
5. Click **Security**.
6. Click **Certificate**.
7. You can configure the certificate settings from the screen below.



NOTE

- The functions that are grayed and unlinked indicate they are not available.
- For more information on configuration, see the Help text in the Web Based Management.

Creating and installing a certificate

Step by step chart for creating and installing a certificate

self-signed certificate	or	**certificate from a CA**
↓		↓
Create a self-signed certificate using Web Based Management. (See page 86.)		Create a CSR using Web Based Management. (See page 87.)
↓		↓
Install the self-signed certificate to your computer. (See page 89.)		Install the certificate issued by the CA to your Brother machine using Web Based Management. (See page 88.)
↓		↓
You have completed creating and installing the certificate.		Install the certificate to your computer. (See page 88.)
		↓
		You have completed creating and installing the certificate.

How to create and install a self-signed certificate

1. Click **Create Self-Signed Certificate** on the **Certificate** page.
2. Enter a **Common Name** and a **Valid Date**.

NOTE

- The length of the **Common Name** must be less than 64 characters. Enter an identifier such as an IP address, node name, or domain name to use when accessing this machine through SSL/TLS communication. The node name is displayed by default.
- A warning will pop-up if you use the IPPS or HTTPS protocol and enter a different name in the URL than the **Common Name** that was used for the self-signed certificate.

3. You can choose the **Public Key Algorithm** and **Digest Algorithm** settings from the drop-down list. The default settings are **RSA(2048bit)** for **Public Key Algorithm** and **SHA256** for **Digest Algorithm**.
4. Click **Submit**.
5. The self-signed certificate is created and saved in your machine's memory successfully.
   To use SSL/TLS communication, the self-signed certificate also needs to be installed on your computer.
   For more information, see *How to install the self-signed certificate on your computer* on page 89.

How to create a CSR

1. Click **Create CSR** on the **Certificate** page.
2. Enter a **Common Name** and your information, such as **Organization**.

NOTE

- We recommend that the Root Certificate from the CA be installed on your computer before creating the CSR.
- The length of the **Common Name** must be less than 64 characters. Enter an identifier such as an IP address, node name, or domain name to use when accessing this printer through SSL/TLS communication. The node name is displayed by default. The **Common Name** is required.
- A warning will pop-up if you enter a different name in the URL than the Common Name that was used for the certificate.
- The length of the **Organization**, the **Organization Unit**, the **City/Locality** and the **State/Province** must be less than 64 characters.
- The **Country/Region** should be an ISO 3166 country code composed of two characters.
- If you are configuring X.509v3 certificate extension, choose the **Configure extended partition** check box and then choose **Auto (Register IPv4)** or **Manual**.

3. You can choose the **Public Key Algorithm** and **Digest Algorithm** settings from the drop-down list. The default settings are **RSA(2048bit)** for **Public Key Algorithm** and **SHA256** for **Digest Algorithm**.
4. Click **Submit**.
5. When the contents of the CSR appear, click **Save** to save the CSR file to your computer.
6. The CSR is created.

NOTE

- Follow your CA policy regarding the method to send a CSR to your CA.
- If you are using Enterprise root CA of Windows Server® 2003/2008/2012, we recommend using the **Web Server** for the certificate template when creating the Client Certificate for secure management. If you are creating a Client Certificate for an IEEE 802.1x environment with EAP-TLS authentication, we recommend using **User** for the certificate template. For more information, see the SSL communication page from the top page for your model at http://solutions.brother.com/.

How to install the certificate to your machine

When you receive the certificate from a CA, follow the steps below to install it into the print server.

NOTE

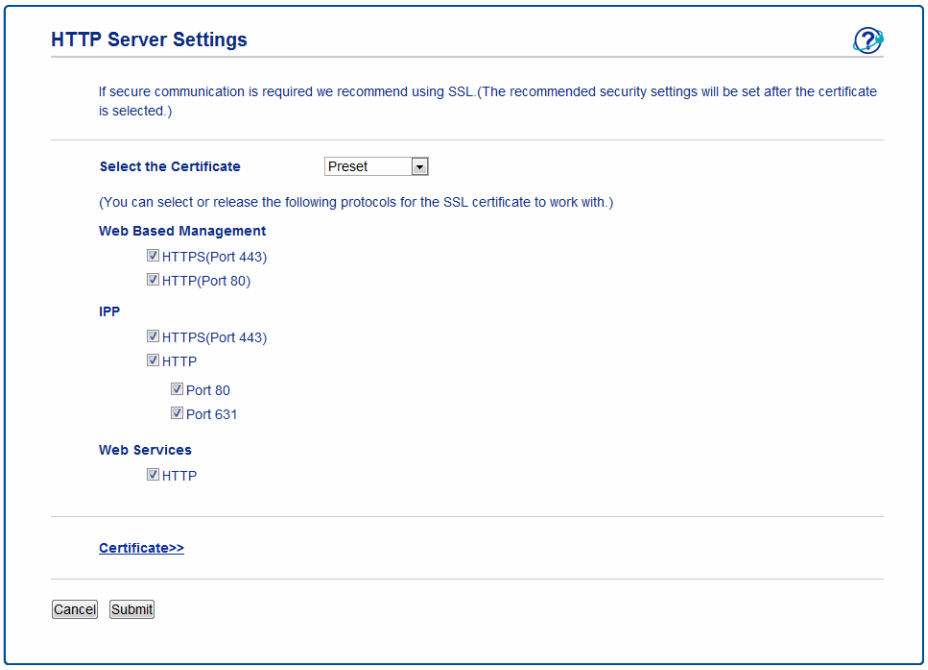
Only a certificate issued with this machine's CSR can be installed. When you want to create another CSR, make sure that the certificate is installed before creating another CSR. Create another CSR after installing the certificate to the machine; Otherwise the CSR you have made before installing will be invalid.

1. Click **Install Certificate** on the **Certificate** page.
2. Specify the file of the certificate that has been issued by a CA, and then click **Submit**.
3. Now the certificate is created and saved in your machine memory successfully.
   To use SSL/TLS communication, the Root Certificate from the CA needs to be installed on your computer. Contact your network administrator about installation.

Choosing the certificate

After you install the certificate, follow the steps below to choose the certificate you want to use.

1. Click **Network**.
2. Click **Protocol**.
3. Click **HTTP Server Settings** and then choose the certificate from the **Select the Certificate** drop-down list.



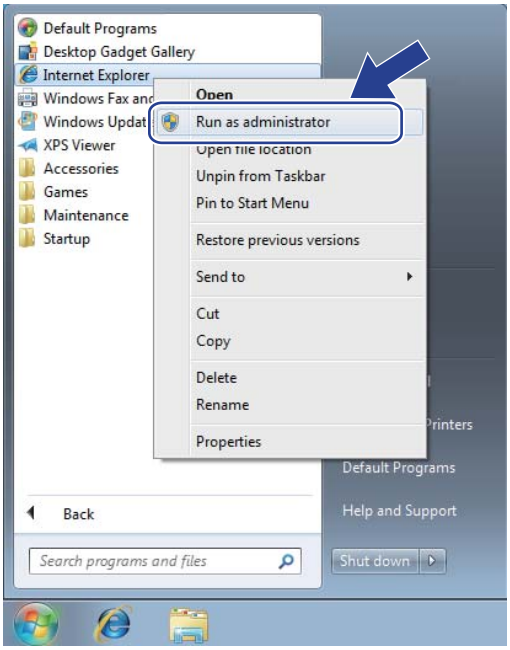
How to install the self-signed certificate on your computer

NOTE

- The following steps are for Windows® Internet Explorer®. If you use another web browser, follow the help text of the web browser itself.
- You must have administrator rights to install the self-signed certificate.

For Windows Vista®, Windows® 7, Windows® 8, Windows Server® 2008 and Windows Server® 2012 users that have administrator rights

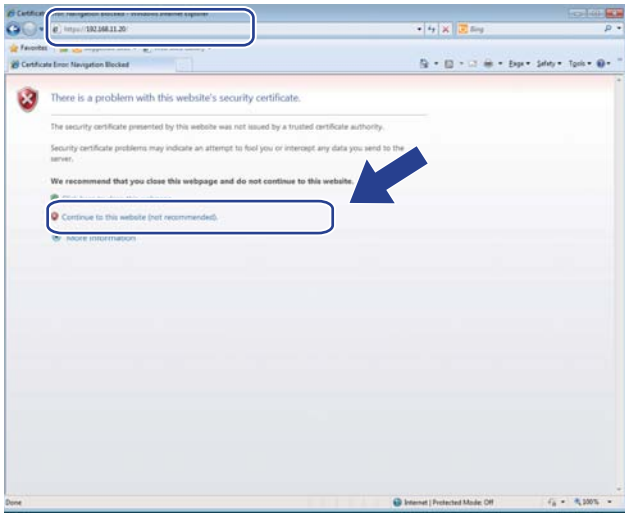
1. (Windows Vista®/Windows® 7/Windows Server® 2008)
   Click the button and **All Programs**.
   (Windows® 8)
   Right-click on the (**Internet Explorer**) icon on the taskbar.
   (Windows Server® 2012)
   Click (**Internet Explorer**), and then right-click on the (**Internet Explorer**) icon appeared on the taskbar.
2. Right-click **Internet Explorer**, and then click **Run as administrator**.



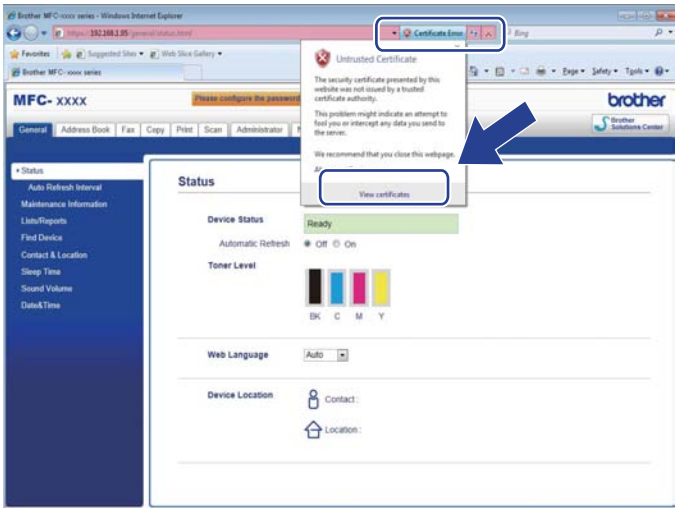
NOTE

If the **User Account Control** screen appears,
(Windows Vista®) Click **Continue (Allow)**.
(Windows® 7/Windows® 8) Click **Yes**.

3 Type “https://machine’s IP address/” into your browser to access your machine (where “machine’s IP address” is the machine’s IP address or the node name that you assigned for the certificate).
Then click **Continue to this website (not recommended).**.



4 Click **Certificate Error**, and then click **View certificates**. For the rest of the instructions, follow the steps from step ❹ in *For Windows® XP and Windows Server® 2003 users* on page 91.

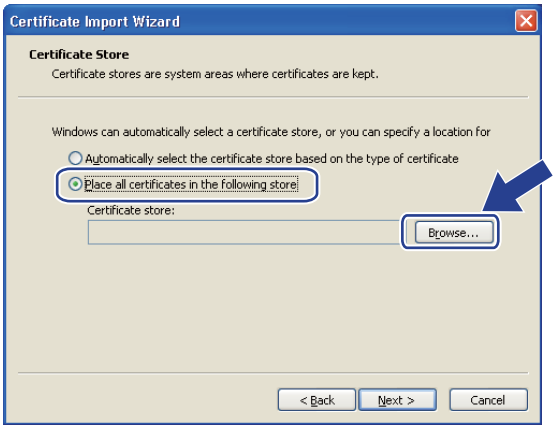


For Windows® XP and Windows Server® 2003 users

1. Start your web browser.
2. Type “https://machine’s IP address/” into your browser to access your machine (where “machine’s IP address” is the IP address or the node name that you assigned for the certificate).
3. When the security alert dialog box appears, do one of the following:
   - Click **Continue to this website (not recommended).**. Click **Certificate Error**, and then click **View certificates**.
4. Click **Install Certificate...** from the **General** tab.



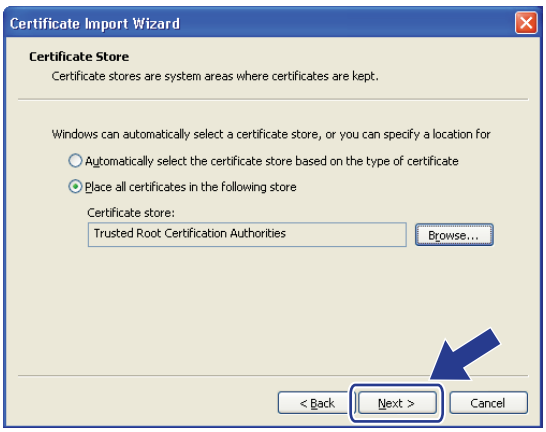
5. When the **Certificate Import Wizard** appears, click **Next**.
6. You need to specify a location to install the certificate. We recommend you choose **Place all certificates in the following store**, and then click **Browse...**.



7 Choose **Trusted Root Certification Authorities**, and then click **OK**.



8 Click **Next**.



9 Click **Finish**.

10 Click **Yes**, if the fingerprint (thumbprint) is correct.



NOTE

The fingerprint (thumbprint) is printed on the Network Configuration Report (See *Printing the Network Configuration Report* on page 48).

11 Click **OK**.

12 The self-signed certificate is now installed on your computer, and SSL/TLS communication is available.

Import and export the certificate and private key

You can store the certificate and private key on the machine and manage them by importing and exporting.

How to import the self-signed certificate, the certificate issued by a CA, and the private key

1 Click **Import Certificate and Private Key** on the **Certificate** page.

2 Specify the file that you want to import.

3 Enter the password if the file is encrypted, and then click **Submit**.

4 Now the certificate and private key are imported to your machine successfully.
To use SSL/TLS communication, the Root Certificate from the CA needs to also be installed on your computer. Contact your network administrator about the installation.

How to export the self-signed certificate, the certificate issued by a CA, and the private key

1 Click **Export** shown with **Certificate List** on the **Certificate** page.

2 Enter the password if you want to encrypt the file.

NOTE

If a blank password is used, the output is not encrypted.

3 Enter the password again for confirmation, and then click **Submit**.

4 Specify the location where you want to save the file.

5 Now the certificate and private key are exported to your computer.

NOTE

You can import the file that you exported.

Import and export a CA certificate

You can store a CA certificate on the machine by importing and exporting.

How to import a CA certificate

1. Click **CA Certificate** on the **Security** page.
2. Click **Import CA Certificate** and choose the certificate. Click **Submit**.

How to export a CA certificate

1. Click **CA Certificate** on the **Security** page.
2. Choose the certificate you want to export and click **Export**. Click **Submit**.
3. Click **Save** to choose the destination folder.
4. Choose the destination you want to save the exported certificate and then save the certificate.

Managing multiple certificates

This multiple certificate feature allows you to manage each certificate that you have installed using Web Based Management. After installing certificates, you can view what certificates are installed from the **Certificate** page and then view each certificate's content, delete, or export the certificate. For information on how to access the **Certificate** page, see *Configure certificate using Web Based Management* on page 85. The Brother machine allows you to store up to four self-signed certificates or up to four certificates issued by a CA. You can use the stored certificates for using the HTTPS/IPPS protocol, IEEE 802.1x authentication, or a Signed PDF.

You can also store up to four CA certificates for using IEEE 802.1x authentication and SSL for SMTP/POP3.

We recommend you store one certificate less and keep the last free to deal with certificate expiration. For example, if you want to store a CA certificate, store three certificates and leave one storage as a backup. In the case of re-issuing the certificate, such as when the certificate is expired, you can import a new certificate to the backup and then you can delete the expired certificate to avoid configuration failure.

NOTE

- When you use HTTPS/IPPS, IEEE 802.1x, or Signed PDF, you must choose which certificate you are using.
- When you use SSL for SMTP communications, you do not have to choose the certificate. The necessary certificate will be chosen automatically.

Managing your network machine securely using SSL/TLS

To manage your network machine securely, you need to use the management utilities with security protocols.

Secure Management using Web Based Management (web browser)

We recommend to use HTTPS protocol for secure management. To use these protocols, the following machine settings are required.

NOTE

HTTPS protocol is enabled by default.

You can change the HTTPS protocol settings and the certificate on the Web Based Management screen by clicking **Network**, **Protocol** and then **HTTP Server Settings**.

1. Start your web browser.
2. Type “http://machine’s IP address/” into your browser. (If you use the created certificate, type “http://Common Name/” into your browser. Where “Common Name” is the Common Name that you assigned for the certificate, such as an IP address, node name, or domain name. For how to assign a Common Name for the certificate, see *Using Certificates for device security* on page 84.)
   - For example:

     http://192.168.1.2/ (if the Common Name is the machine’s IP address)
3. No password is required by default. If you have previously set a password, enter it and press .
4. You can now access the machine using HTTPS.
   If you use the SNMPv3 protocol, follow the steps below.

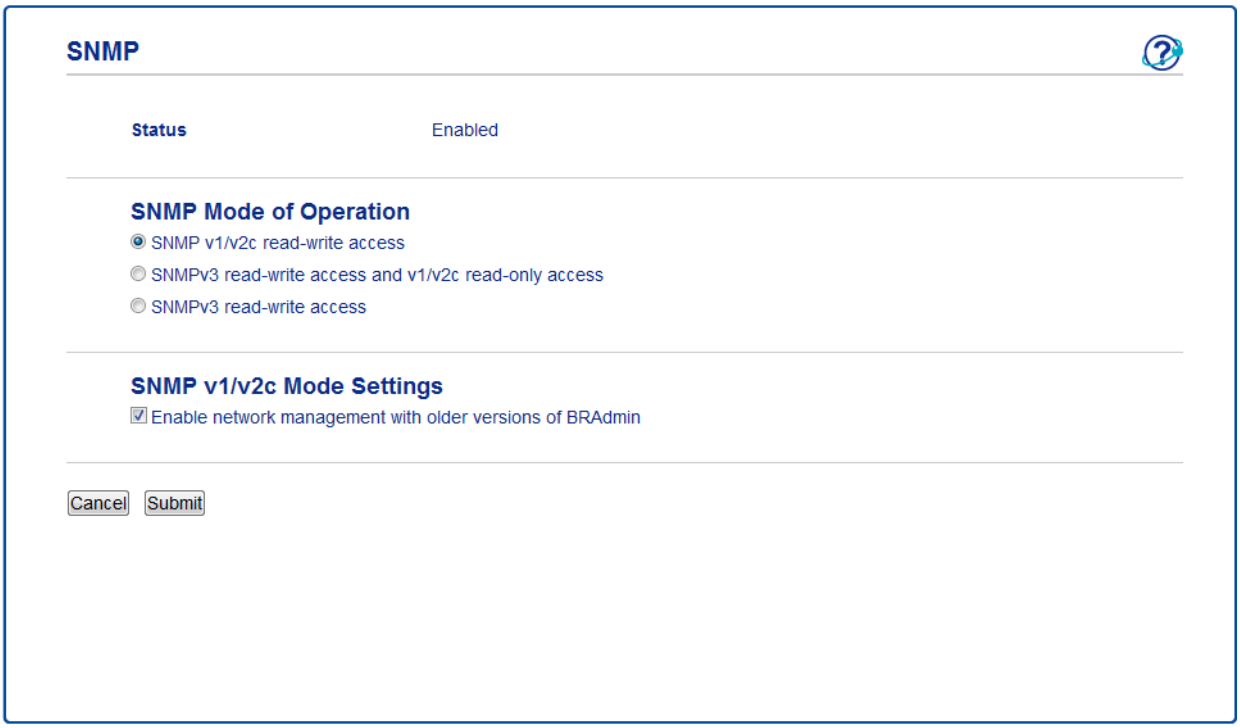
NOTE

You can also change the SNMP settings by using BRAdmin Professional 3.

5. Click **Network**.
6. Click **Protocol**.

7 Make sure that the **SNMP** setting is enabled, and then click **Advanced Setting** of **SNMP**.

8 You can configure the SNMP settings from the screen below.



There are three SNMP connection modes of operation.

■ **SNMP v1/v2c read-write access**

In this mode, the print server uses version 1 and version 2c of the SNMP protocol. You can use all Brother applications under this mode. However, it is not secure since it will not authenticate the user and the data will not be encrypted.

■ **SNMPv3 read-write access and v1/v2c read-only access**

In this mode, the print server uses the read-write access of version 3 and the read-only access of version 1 and version 2c of the SNMP protocol.

NOTE

When you use the **SNMPv3 read-write access and v1/v2c read-only access** mode, some Brother applications (e.g. BRAdmin Light) that access to the print server do not work properly since they authorize the read-only access of version 1 and version 2c. If you want to use all applications, use the **SNMP v1/v2c read-write access** mode.

■ **SNMPv3 read-write access**

With this mode, the print server uses version 3 of the SNMP protocol. If you want to manage the print server securely, use this mode.

NOTE

- When you use the **SNMPv3 read-write access** mode, please note the following.
  - You can manage the print server by using BRAdmin Professional 3 or Web Based Management only.
  - Except for BRAdmin Professional 3, all applications that use SNMPv1/v2c will be restricted. To allow the use of SNMPv1/v2c applications, use **SNMPv3 read-write access and v1/v2c read-only access** or **SNMP v1/v2c read-write access** mode.
- For more information, see the Help text in Web Based Management.

Secure Management using BRAdmin Professional 3 (Windows®)

To use the BRAdmin Professional 3 utility securely, you need to follow the points below

■ We strongly recommend to use the latest version of the BRAdmin Professional 3 utility that is available as a download from http://solutions.brother.com/. If you use an older version of BRAdmin [1] to manage your Brother machines the user authentication will not be secure.

■ If you want to avoid access to your machine from older versions of BRAdmin [1], you need to disable the access from older versions of BRAdmin [1] from **Advanced Setting** of **SNMP** on the **Protocol** page using Web Based Management. (See *Secure Management using Web Based Management (web browser)* on page 95.)

■ If you use BRAdmin Professional 3 and Web Based Management together, use Web Based Management with the HTTPS protocol.

■ If you are managing a mixed group of older print servers [2] and print servers with BRAdmin Professional 3, we recommend using a different password in each group. This will ensure security is maintained on the new print servers.

[1] BRAdmin Professional older than Ver. 2.80, BRAdmin Light for Macintosh older than Ver. 1.10

[2] NC-2000 series, NC-2100p, NC-3100h, NC-3100s, NC-4100h, NC-5100h, NC-5200h, NC-6100h, NC-6200h, NC-6300h, NC-6400h, NC-8000, NC-100h, NC-110h, NC-120w, NC-130h, NC-140w, NC-8100h, NC-9100h, NC-7100w, NC-7200w, NC-2200w

Printing documents securely using SSL/TLS

To print documents securely with IPP protocol, you can use the IPPS protocol.

To Configure IPPS settings using a web browser:

1. On the machine's web page, click **Network**, and then click **Protocol**. If the **IPP** check box is already selected, go to step ❺.
2. Select the **IPP** check box, and then click **Submit**.
3. Restart the machine to activate the configuration.
4. On the machine's web page, click **Network**, and then click **Protocol**.
5. Click **HTTP Server Settings**.
6. Select the **HTTPS(Port443)** check box, and then click **Submit**.
7. Restart the machine to activate the configuration.

NOTE

Communication using IPPS cannot prevent unauthorized access to the print server.

Sending or Receiving an E-mail securely

Configuration using Web Based Management (web browser)

You can configure secured E-mail sending with user authentication or E-mail sending and receiving using SSL/TLS on the Web Based Management screen.

1. Start your web browser.
2. Type “http://machine’s IP address/” into your browser’s address bar (where “machine’s IP address” is the IP address of the machine or the print server name).
   - For example: http://192.168.1.2/
3. No password is required by default. If you have previously set a password, enter it and press →.
4. Click **Network**.
5. Click **Protocol**.
6. Click **Advanced Setting** of **POP3/SMTP** and make sure that the status of **POP3/SMTP** is **Enabled**.
7. You can configure the **POP3/SMTP** settings on this page.

NOTE

- For more information, see the Help text in Web Based Management.
- You can also confirm whether the E-mail settings are correct after configuration by sending a test E-mail.
- If you do not know the POP3/SMTP server settings, please contact your system administrator or ISP (Internet Service Provider) for details.

8. After configuring, click **Submit**. The Test E-mail Send/Receive Configuration dialog box appears.
9. Follow the instructions on-screen if you want to test with the current settings.

Sending an E-mail with user authentication

This machine supports POP before SMTP and SMTP-AUTH methods to send an E-mail via an E-mail server that requires user authentication. These methods prevent an unauthorized user from accessing the E-mail server. You can use Web Based Management or BRAdmin Professional 3 to configure these settings. You can use POP before SMTP and SMTP-AUTH methods for E-mail Notification, E-mail reports and Internet fax sending.

E-mail server settings

You need to match the settings of SMTP authentication method with the method used by your E-mail server. Contact your network administrator or your ISP (Internet Service Provider) about the E-mail server configuration.

You will also need to check **SMTP-AUTH** of **SMTP Server Authentication Method** to enable the 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 which your ISP is using for the SMTP server (for example, port 587), you would then be able to send an E-mail via the SMTP server.
- If you can use both POP before SMTP and SMTP-AUTH, we recommend choosing SMTP-AUTH.
- If you choose POP before SMTP for the SMTP Server Authentication Method, you need to configure the POP3 settings. You can also use the APOP method if needed.

Sending or Receiving an E-mail securely using SSL/TLS

This machine supports SSL/TLS methods to send or receive an E-mail via an E-mail server that requires secure SSL/TLS communication. To send or receive E-mail via an E-mail server that is using SSL/TLS communication, you must configure SMTP over SSL/TLS or POP3 over SSL/TLS correctly.

Verifying Server Certificate

- If you choose SSL or TLS for **SMTP over SSL/TLS** or **POP3 over SSL/TLS**, the **Verify Server Certificate** check box will be automatically checked to verify the Server Certificate.
  - Before you verify the Server Certificate, you must import the CA certificate that has been issued by the CA that signed the Server Certificate. Contact your network administrator or your ISP (Internet Service Provider) to confirm whether a CA certificate import is necessary. For importing the certificate, see *Import and export a CA certificate* on page 94.
  - If you do not need to verify the Server Certificate, uncheck **Verify Server Certificate**.

Port Number

- If you choose SSL, the **SMTP Port** or **POP3 Port** value will be changed to match the protocol. If you want to change the port number manually, enter the port number after you choose **SMTP over SSL/TLS** or **POP3 over SSL/TLS**.
- You must configure the POP3/SMTP communication method to match the E-mail server. For details of the E-mail server settings, contact your network administrator or ISP (Internet Service Provider).

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

  (SMTP)

  SMTP Port: 587

  SMTP Server Authentication Method: SMTP-AUTH

  SMTP over SSL/TLS: TLS

  (POP3)

  POP3 Port: 995

  POP3 over SSL/TLS: SSL

Using IEEE 802.1x authentication

You can configure IEEE 802.1x authentication for a wired or a wireless network.

IEEE 802.1x authentication configuration using Web Based Management (web browser)

If you are configuring IEEE 802.1x authentication for a wired or a wireless network using Web Based Management, follow the instructions below.

You can also configure IEEE 802.1x authentication using:

(Wired network)

- BRAdmin Professional 3

(Wireless network)

- Wireless setup wizard from the control panel (For details, see *Configuring your machine for an enterprise wireless network* on page 23.)
- Wireless setup wizard on the CD-ROM (For details, see *Wireless configuration temporarily using a USB cable (Recommended)* on page 13.)
- BRAdmin Professional 3

NOTE

- If you configure your machine using EAP-TLS Authentication, you must install the Client Certificate issued by a CA before you start configuration. Contact your network administrator about the Client Certificate. If you have installed more than one certificate, we recommend you write down the certificate you want to use. For details on installing the certificate, see *Using Certificates for device security* on page 84.
- Before you verify the Server Certificate, you must import the CA certificate that has been issued by the CA that signed the Server Certificate. Contact your network administrator or your ISP (Internet Service Provider) to confirm whether a CA certificate import is necessary. For details on importing the certificate, see *Import and export a CA certificate* on page 94.
- For the details of each certificate, see *Using Certificates for device security* on page 84.

1. Start your web browser.
2. Type “http://machine’s IP address/” into your browser’s address bar (where “machine’s IP address” is the IP address of the machine or the print server name).
   - For example: http://192.168.1.2/

NOTE

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

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

  The NetBIOS name can be seen in the Network Configuration Report (See *Printing the Network Configuration Report* on page 48).
- For Macintosh users, you can have easy access to the Web Based Management System by clicking the machine icon on the **Status Monitor** screen. For more information: see Software User's Guide.

3. No password is required by default. If you have previously set a password, type it and press .
4. Click **Network**.
5. (Wired) Click **Wired** and then choose **Wired 802.1x Authentication**.
   (Wireless) Click **Wireless** and then choose **Wireless (Enterprise)**.

6 Now you can configure the IEEE 802.1x authentication settings.

- If you want to enable IEEE 802.1x authentication for wired network, check **Enabled** for **Wired 802.1x status** on the **Wired 802.1x Authentication** page.
- For the details of IEEE 802.1x authentication and the inner authentication methods, see *IEEE 802.1x Authentication* on page 122.
- If you are using EAP-TLS authentication, you must choose the Client Certificate that has been installed (shown with Certificate Name) for verification from the **Client Certificate** drop-down list.
- If you choose EAP-FAST, PEAP, EAP-TTLS, or EAP-TLS authentication, you can choose the verification method from the **Server Certificate Verification** drop-down list. You can verify the Server Certificate by using the CA certificate, imported to the machine in advance, that has been issued by the CA that signed the Server Certificate.

You can choose one of the following verification methods from the **Server Certificate Verification** drop-down list.

- **No Verification**

  The Server Certificate can always be trusted. The verification is not performed.

- **CA Cert.**

  The verification method to check the CA reliability of the Server Certificate, using the CA certificate that has been issued by the CA that signed the Server Certificate.

- **CA Cert. + ServerID**

  The verification method to check the Common Name [1] value of the Server Certificate, in addition to the CA reliability of the Server Certificate.

[1] The Common Name verification compares the Common Name of the Server Certificate to the character string configured for the **Server ID**. Before you use this method, contact your system administrator about the Server Certificate's Common Name and then configure **Server ID**.

7 After configuring, click **Submit**.
(Wired)
After configuring, connect your machine to the IEEE 802.1x supported network. After a few minutes, print the Network Configuration Report to check the **<Wired IEEE 802.1x> Status.** (See *Printing the Network Configuration Report* on page 48.)

- **Success**

  The wired IEEE 802.1x function is enabled and the authentication was successful.

- **Failed**

  The wired IEEE 802.1x function is enabled, however, the authentication failed.

- **Off**

  The wired IEEE 802.1x function is not available.

(Wireless)
Shortly after configuring, the WLAN report will be printed automatically. Check your wireless configuration on the report. See *Printing the WLAN report (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)* on page 48.

8 Troubleshooting

Overview

This chapter explains how to resolve typical network problems you may encounter when using the Brother machine. If, after reading this chapter, you are unable to resolve your problem, please visit the Brother Solutions Center at: http://solutions.brother.com/.

Please go to the Brother Solutions Center at http://solutions.brother.com/ and click Manuals on your model page to download the other manuals.

Identifying your problem

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

First check the following:
The power cord is connected properly and the Brother machine is turned on.
The access point (for wireless), router or hub are turned on and its link button is blinking.
All protective packaging has been removed from the machine.
The toner cartridges and drum unit are installed properly.
The top and back covers are fully closed.
Paper is inserted properly in the paper tray.
(For wired networks) A network cable is securely connected to the Brother machine and the router or hub.

Go to the page for your solution from the lists below

- I cannot complete the wireless network setup configuration. (See page 106.)
- The Brother machine is not found on the network during the MFL-Pro Suite installation. (See page 107.)
- The Brother machine cannot print or scan over the network. (See page 108.)
- The Brother machine is not found on the network even after successful installation. (See page 108.)
- I'm using security software. (See page 111.)
- I want to check that my network devices are working properly. (See page 112.)

I cannot complete the wireless network setup configuration.

Question	Interface	Solution
My machine does not connect during wireless setup?	wireless	Turn your wireless router Off and back On. Then try and configure the wireless settings again.
Are your security settings (SSID/Network Key) correct?	wireless	■ Reconfirm and choose the correct 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 or ask your Internet provider or network administrator. ■ For information on what the SSID and Network Key are, see *Wireless network terms and concepts (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)* on page 124.
Are you using MAC address filtering?	wireless	Confirm the MAC address of the Brother machine is allowed in the filter. You can find the MAC address from the Brother machine's control panel. (See *Function table and default factory settings* on page 49.)
Is your WLAN access point/router in a stealth mode? (not broadcasting the SSID)	wireless	■ You should type the correct SSID name or Network Key by hand. ■ Check the SSID name or the Network Key in the instructions supplied with your WLAN access point/router and reconfigure the wireless network setup. (See *Configuring your machine when the SSID is not broadcast* on page 21.)
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 print or scan over the network. The Brother machine is not found on the network even after successful installation.* on page 108.)

The Brother machine is not found on the network during MFL-Pro Suite installation.

Question	Interface	Solution
Is your machine connected to the network and does it have a valid IP address?	wired/ wireless	Print the Network Configuration Report and check that **Ethernet Link Status** or **Wireless Link Status** is **Link OK**. See *Printing the Network Configuration Report* on page 48. If the report shows **Failed To Associate** or **Link DOWN**, ask your network administrator whether your IP address is valid or not.
Are you using security software?	wired/ wireless	■ Choose to search for the Brother machine again on the installer dialog box. ■ Allow access when the alert message of the security software appears during the MFL-Pro Suite installation. ■ For more information about security software, see *I'm using security software.* on page 111.
Is your Brother machine placed too far from the WLAN access point/router?	wireless	Place your Brother machine within about 3.3 feet (1 meter) from 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 print or 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'm using security software.* on page 111.
Is your Brother machine assigned with an available IP address?	wired/ wireless	■ (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 details, and then follow the steps below: **NOTE** • (Windows® XP/XP Professional x64 Edition/Windows Vista®/Windows® 7/Windows® 8) 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.

The Brother machine cannot print or scan over the network.
The Brother machine is not found on the network even after successful installation. (continued)

Question	Interface	Solution
Is your Brother machine assigned with an available IP address? (continued)	wired/ wireless	1 (Windows® XP) Click the **Start** button, **All Programs**, **Accessories** and **Windows Explorer**, and then **My Computer**. (Windows Vista®/Windows® 7) Click the button and **Computer**. (Windows® 8) Click the (**File Explorer**) icon on the taskbar, and then click **Computer** in the left navigation bar. 2 Double-click **XXX (C:)**, **Program Files** or **Program Files (x86)** for 64-bit OS users, **Browny02**, **Brother**, **BrotherNetTool.exe** to run the program. **NOTE** If the **User Account Control** screen appears, (Windows Vista®) Click **Continue**. (Windows® 7/Windows® 8) Click **Yes**. 3 Follow the on-screen instructions. 4 Make sure that you can print or scan. **NOTE** The Network Connection Repair Tool will start automatically if you check the **Enable Connection Repair Tool** box using Status Monitor. Right-click on the Status Monitor screen, click **Options**, **Details**, and then click the **Diagnostic** tab. This is not recommended when your network administrator has set the IP address to static, since it will automatically change the IP address. If the correct IP address and the Subnet mask are still not assigned even after using the Network Connection Repair Tool, ask the network administrator for this information, or visit the Brother Solutions Center at http://solutions.brother.com/.

The Brother machine cannot print or scan over the network.
The Brother machine is not found on the network even after successful installation. (continued)

Question	Interface	Solution
Did your previous printing job fail?	wired/ wireless	If the failed printing job is still in the print queue of your computer, delete it. Otherwise, try one of the following: (Windows® XP/Windows Vista®/ Windows® 7/Windows Server® 2003) Double-click the printer icon in the following folder and then choose **Cancel All Documents** in the **Printer** menu: (Windows® XP/Windows Server® 2003) **Start** and **Printers and Faxes**. (Windows Vista®) , **Control Panel**, **Hardware and Sound**, and then **Printers**. (Windows® 7) , **Devices and Printers**, and then **Printers and Faxes**. (Windows® 8) Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, and then click **Control Panel**. In the **Hardware and Sound** group, click **View devices and printers**. Right-click your Brother machine, select **See what's printing**, and then select your printer driver. (Windows Server® 2008) **Start**, **Control Panel** and **Printers**. (Windows Server® 2012) Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, and then click **Control Panel**. In the **Hardware** group, click **View devices and printers**. Right-click your Brother machine, select **See what's printing**, and then select your printer driver.
Are you connecting the Brother machine to the network using wireless capabilities?	wireless	■ Print the WLAN report to confirm the state of the wireless connection. (For how to print, see *Printing the WLAN report (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)* on page 48.) If there is an error code on the printed WLAN report: see Quick Setup Guide: *Troubleshooting*. ■ See *The Brother machine is not found on the network during MFL-Pro Suite installation.* on page 107.
I have checked and tried all of above, however the Brother machine does not print/scan. Is there anything else I can do?	wired/ wireless	Uninstall MFL-Pro Suite and reinstall it.

I'm using security software.

Question	Interface	Solution
Did you choose to accept the security alert dialog box during the MFL-Pro Suite installation, application start-up process, or when using the printing/scanning features?	wired/ wireless	If you did not choose to accept the security alert dialog box, the firewall function of your security software may be rejecting access. Some security software might block access without showing a security alert dialog box. To allow access, see the instructions of your security software 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 ■ PC-FAX RX [1] → Port number 54926 / Protocol UDP ■ Network scanning/printing [1], PC-FAX RX [1], Remote Setup [1]→ Port number 161 and 137/ Protocol UDP ■ BRAdmin Light [1] → Port number 161 / Protocol UDP [1] Windows® only. For details on how to open the port, see the instructions of the security software or ask the manufacturer.

I want to check 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 *First check the following:* on page 105.
Where can I find my Brother machine's network settings, such as IP address?	wired/ wireless	Print the Network Configuration Report. (See *Printing the Network Configuration Report* on page 48.)
How can I check the link status of my Brother machine?	wired/ wireless	Print the Network Configuration Report and check that **Ethernet Link Status** or **Wireless Link Status** is **Link OK**. (See *Printing the Network Configuration Report* on page 48.) If the report shows **Link DOWN** or **Failed To Associate**, start over again from the *First check the following:* on page 105.
Can I “ping” the Brother machine from my computer?	wired/ wireless	Ping the Brother machine from your computer using the IP address or the node name. ■ 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 the network administrator and use the Network Connection Repair Tool to fix the IP address and the subnet mask automatically. For the detail of the Network Connection Repair Tool, see *(Windows®) Confirm the IP address and the Subnet Mask using the Network Connection Repair Tool.* in *Is your Brother machine assigned with an available IP address?* on page 108.
Is the Brother machine connecting to the wireless network?	wireless	Print the WLAN report to confirm the state of the wireless connection. For how to print, see *Printing the WLAN report (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)* on page 48. If there is an error code on the printed WLAN report: see Quick Setup Guide: *Troubleshooting*.
I have checked and tried all of the above, however, I'm 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 details of 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 106.

Section II

Network Glossary

Types of network connections and protocols	114
Configuring your machine for a network	120
Wireless network terms and concepts (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)	124
Additional network settings from Windows®	128
Security terms and concepts	133

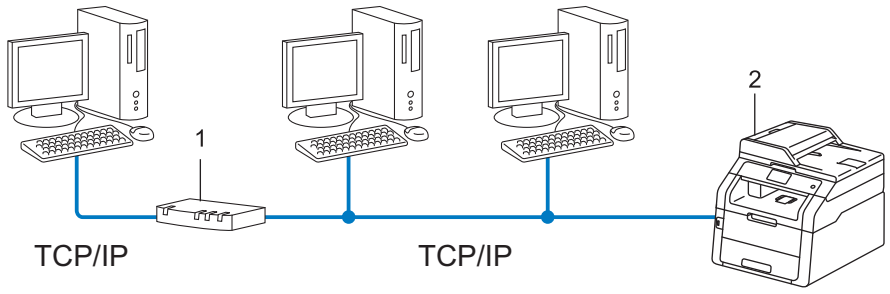
9 Types of network connections and protocols

Types of network connections

Wired network connection example

Peer-to-Peer printing using TCP/IP

In a Peer-to-Peer environment, each computer directly sends and receives data to each device. There is no central server controlling file access or machine sharing.



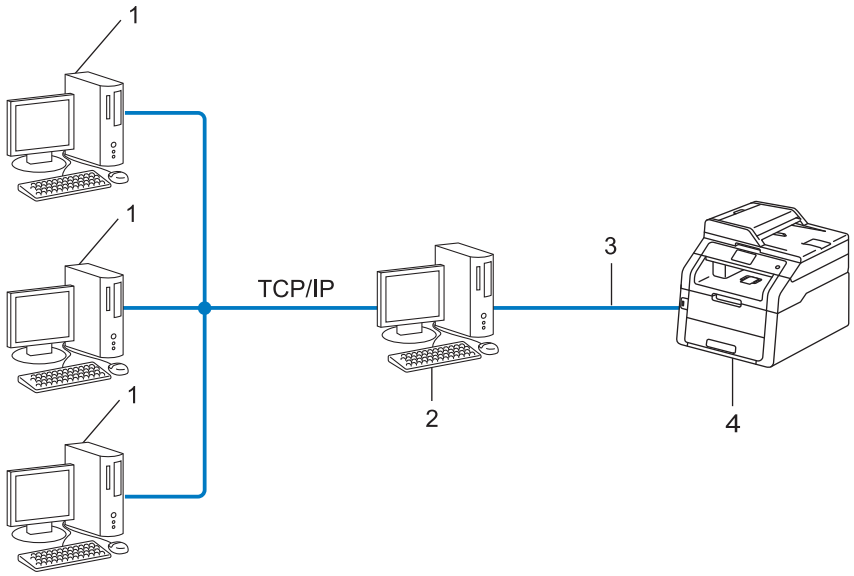
1 Router

2 Network machine (your machine)

- In a smaller network of 2 or 3 computers, we recommend the Peer-to-Peer printing method as it is easier to configure than the Network Shared printing method. See *Network Shared printing* on page 115.
- Each computer must use the TCP/IP Protocol.
- The Brother machine needs an appropriate IP address configuration.
- If you are using a router, the Gateway address must be configured on the computers and the Brother machine.

Network Shared printing

In a Network Shared environment, each computer sends data via a centrally controlled computer. This type of computer is often called a “Server” or a “Print Server”. Its job is to control the printing of all print jobs.



1 Client computer

2 Computer known as “Server” or “Print server”

3 TCP/IP, USB, or parallel (where available)

4 Network machine (your machine)

- In a larger network, we recommend a Network Shared printing environment.
- The “server” or the “print server” must use the TCP/IP print protocol.
- The Brother machine needs to have an appropriate IP address configuration unless the machine is connected via the USB or the parallel interface at the server.

Protocols

TCP/IP protocols and functions

Protocols are the standardized sets of rules for transmitting data on a network. Protocols allow users to gain access to network connected resources.

The print server used on the Brother machine supports the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol.

TCP/IP is the most popular set of protocols used for communication such as Internet and E-mail. This protocol can be used in almost all operating systems such as Windows®, Windows Server®, Mac OS X and Linux®. The following TCP/IP protocols are available on the Brother machine.

NOTE

- You can configure the protocol settings by using the HTTP interface (web browser). (See *How to configure the machine settings using Web Based Management (web browser)* on page 57.)
- To find what protocols your Brother machine supports, see *Supported protocols and security features* on page 137.
- For information about supported security protocols, see *Security protocols* on page 134.

DHCP/BOOTP/RARP

By using the DHCP/BOOTP/RARP protocols, the IP address can be automatically configured.

NOTE

To use the DHCP/BOOTP/RARP protocols, please contact your network administrator.

APIPA

If you do not assign an IP address manually (using the control panel of the machine or the BRAdmin software) or automatically (using a DHCP/BOOTP/RARP server), the Automatic Private IP Addressing (APIPA) protocol will automatically assign an IP address from the range 169.254.1.0 to 169.254.254.255.

ARP

Address Resolution Protocol performs mapping of an IP address to a MAC address in a TCP/IP network.

DNS client

The Brother print server supports the Domain Name System (DNS) client function. This function allows the print server to communicate with other devices by using its DNS name.

NetBIOS name resolution

Network Basic Input/Output System name resolution enables you to obtain the IP address of the other device using its NetBIOS name during the network connection.

WINS

Windows® Internet Name Service is an information providing service for the NetBIOS name resolution by consolidating an IP address and a NetBIOS name that is in the local network.

LPR/LPD

Commonly used printing protocols on a TCP/IP network.

SMTP client

Simple Mail Transfer Protocol (SMTP) client is used to send E-mails via the Internet or Intranet.

Custom Raw Port (Default is Port 9100)

Another commonly used printing protocol on a TCP/IP network. It enables interactive data transmission.

IPP

The Internet Printing Protocol allows you to print documents directly to any accessible machine via the Internet.

NOTE

For details of the IPPS protocol, see *Security protocols* on page 134.

mDNS

mDNS allows the Brother print server to automatically configure itself to work in a Mac OS X Simple Network Configuration system.

TELNET

The TELNET protocol allows you to control the remote network devices on a TCP/IP network from your computer.

SNMP

The Simple Network Management Protocol (SNMP) is used to manage network devices including computers, routers and Brother network ready machines. The Brother print server supports SNMPv1, SNMPv2c and SNMPv3.

NOTE

For details of the SNMPv3 protocol, see *Security protocols* on page 134.

LLMNR

The Link-Local Multicast Name Resolution protocol (LLMNR) resolves the names of neighboring computers if the network does not have a Domain Name System (DNS) server. The LLMNR Responder function works in both the IPv4 or IPv6 environment when using a computer that has the LLMNR Sender function such as Windows Vista®, Windows® 7 and Windows® 8.

Web Services

The Web Services protocol enables Windows Vista®, Windows® 7 or Windows® 8 users to install the drivers used for printing and scanning by right-clicking the machine icon from the **Network** folder. (See *Installing drivers used for printing and scanning via Web Services (Windows Vista®, Windows® 7 and Windows® 8)* on page 128.) For details about scanning using Web Services: see Software User's Guide. The Web Services also lets you check the current status of the machine from your computer.

HTTP

The HTTP protocol is used to transmit the data between a web server and a web browser.

NOTE

For details of the HTTPS protocol, see *Security protocols* on page 134.

FTP (for the Scan to FTP feature)

The File Transfer Protocol (FTP) allows the Brother machine to scan black and white or color documents directly to an FTP server located locally on your network or on the Internet.

SNTP

The Simple Network Time Protocol is used to synchronize computer clocks on a TCP/IP network. You can configure the SNTP settings using Web Based Management (web browser). (For the details, see *Synchronize with SNTP server* on page 62.)

CIFS

The Common Internet File System is the standard way that computer users share files and printers in Windows®.

IPv6

IPv6 is the next generation Internet protocol. For more information on the IPv6 protocol, visit the model page for the machine you are using at http://solutions.brother.com/.

10 Configuring your machine for a network

IP addresses, subnet masks and gateways

To use the machine in a networked TCP/IP environment, you need to configure its IP address and subnet mask. The IP address you assign to the print server must be on the same logical network as your host computers. If it is not, you must properly configure the subnet mask and the gateway address.

IP address

An IP address is a series of numbers that identifies each device connected to a network. An IP address consists of four numbers separated by dots. Each number is between 0 and 255.

■ Example: In a small network, you would normally change the final number.

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

How the IP address is assigned to your print server:

If you have a DHCP/BOOTP/RARP server in your network the print server will automatically obtain its IP address from that server.

NOTE

On smaller networks, the DHCP server may also be the router.

For more information on DHCP, BOOTP and RARP, see:
Using DHCP to configure the IP address on page 138.
Using BOOTP to configure the IP address on page 140.
Using RARP to configure the IP address on page 139.

If you do not have a DHCP/BOOTP/RARP server, the Automatic Private IP Addressing (APIPA) protocol will automatically assign an IP address from the range 169.254.1.0 to 169.254.254.255. For more information on APIPA, see *Using APIPA to configure the IP address* on page 140.

Subnet mask

Subnet masks restrict network communication.

■ Example: Computer 1 can talk to Computer 2

- Computer 1

  IP Address: 192.168. 1. 2

  Subnet Mask: 255.255.255.000

- Computer 2

  IP Address: 192.168. 1. 3

  Subnet Mask: 255.255.255.000

Where the 0 is in the Subnet mask, there is no limit to communication at this part of the address. What this means in the above example is, we can communicate with any device that has an IP address that begins with 192.168.1.x. (where x. are numbers between 0 and 255).

Gateway (and router)

A gateway is a network point that acts as an entrance to another network and sends data transmitted via the network to an exact destination. The router knows where to direct data that arrives at the gateway. If a destination is located on an external network, the router transmits data to the external network. If your network communicates with other networks, you may need to configure the Gateway IP address. If you do not know the Gateway IP address, then contact your Network Administrator.

IEEE 802.1x Authentication

IEEE 802.1x is an IEEE standard for wired and wireless networks that limits access from unauthorized network devices. Your Brother machine (supplicant) sends an authentication request to a RADIUS server (Authentication server) through your access point (authenticator). After your request has been verified by the RADIUS server, your machine can access the network.

Authentication methods

- LEAP (For wireless network)

  Cisco LEAP (Lightweight Extensible Authentication Protocol) has been developed by Cisco Systems, Inc. which uses a user ID and password for authentication.

- EAP-FAST

  EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling) has been developed by Cisco Systems, Inc. which uses a user ID and password for authentication, and symmetric key algorithms to achieve a tunneled authentication process.

  The Brother machine supports the following inner authentication methods:

  - EAP-FAST/NONE
  - EAP-FAST/MS-CHAPv2
  - EAP-FAST/GTC

- EAP-MD5 (For wired network)

  EAP-MD5 (Extensible Authentication Protocol-Message Digest Algorithm 5) uses a user ID and password for challenge-response authentication.

- PEAP

  PEAP (Protected Extensible Authentication Protocol) has been developed by Microsoft Corporation, Cisco Systems and RSA Security. PEAP creates an encrypted SSL (Secure Sockets Layer)/TLS (Transport Layer Security) tunnel between a client and an authentication server, for sending a user ID and password. PEAP provides mutual authentication between the server and the client.

  The Brother machine supports the following inner authentications:

  - PEAP/MS-CHAPv2
  - PEAP/GTC

■ EAP-TTLS

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) has been developed by Funk Software and Certicom. EAP-TTLS creates a similar encrypted SSL tunnel to PEAP, between a client and an authentication server, for sending a user ID and password. EAP-TTLS provides mutual authentication between the server and the client.

The Brother machine supports the following inner authentications:

- EAP-TTLS/CHAP
- EAP-TTLS/MS-CHAP
- EAP-TTLS/MS-CHAPv2
- EAP-TTLS/PAP

■ EAP-TLS

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) requires digital certificate authentication both at a client and an authentication server.

11 Wireless network terms and concepts (For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW)

Specifying your network

SSID (Service Set Identifier) and channels

You need to configure the SSID and a channel to specify the wireless network you want to connect to.

■ SSID

Each wireless network has its own unique network name and it is technically referred to as an SSID. The SSID is a 32-byte or less value and is assigned to the access point. The wireless network devices you want to associate to the wireless network should match the access point. The access point and wireless network devices regularly send wireless packets (referred to as beacons), which have the SSID information. When your wireless network device receives a beacon, you can identify wireless networks that are close enough to connect to.

■ Channels

Wireless networks use channels. Each wireless channel is on a different frequency. There are up to 14 different channels that can be used when using a wireless network. However, in many countries the number of channels available is restricted.

Security terms

Authentication and encryption

Most wireless networks use some kind of security settings. These security settings define the authentication (how the device identifies itself to the network) and encryption (how the data is encrypted as it is sent on the network). **If you do not correctly specify these options when you are configuring your Brother wireless machine, it will not be able to connect to the wireless network.** Therefore care must be taken when configuring these options. Please see *Supported protocols and security features* on page 137 for which authentication and encryption methods your Brother wireless machine supports.

Authentication and Encryption methods for a personal wireless network

A personal wireless network is a small network, such as a home wireless network, without IEEE 802.1x support.

If you want to use your machine in an IEEE 802.1x supported wireless network, see *Authentication and Encryption methods for an enterprise wireless network* on page 126.

Authentication methods

- Open system

  Wireless devices are allowed to access the network without any authentication.

- Shared key

  A secret pre-determined key is shared by all devices that will access the wireless network.

  The Brother wireless machine uses the WEP key as the pre-determined key.

- WPA-PSK/WPA2-PSK

  Enables a Wi-Fi Protected Access™ Pre-shared key (WPA-PSK/WPA2-PSK), which enables the Brother wireless machine to associate with access points using TKIP for WPA-PSK or AES for WPA-PSK and WPA2-PSK (WPA-Personal).

Encryption methods

- None

  No encryption method is used.

- WEP

  When using WEP (Wired Equivalent Privacy), the data is transmitted and received with a secure key.

- TKIP

  TKIP (Temporal Key Integrity Protocol) provides per-packet key mixing, a message integrity check and rekeying mechanism.

- AES

  AES (Advanced Encryption Standard) provides stronger data protection by using a symmetric-key encryption.

NOTE

- IEEE 802.11n does not support WEP or TKIP for the encryption method.
- If you want to connect to your wireless network using IEEE 802.11n, we recommend to choose AES.

Network key

- Open system/Shared key with WEP

  This key is a 64-bit or 128-bit value that must be entered in an ASCII or hexadecimal format.

  - 64 (40) bit ASCII:

    Uses 5 text characters. e.g. “WSLAN” (this is case sensitive)
  - 64 (40) bit hexadecimal:

    Uses 10 digits of hexadecimal data. e.g. “71f2234aba”
  - 128 (104) bit ASCII:

    Uses 13 text characters. e.g. “Wirelesscomms” (this is case sensitive)
  - 128 (104) bit hexadecimal:

    Uses 26 digits of hexadecimal data. e.g. “71f2234ab56cd709e5412aa2ba”
- WPA-PSK/WPA2-PSK and TKIP or AES

  Uses a Pre-Shared Key (PSK) that is 8 or more characters in length, up to a maximum of 63 characters.

Authentication and Encryption methods for an enterprise wireless network

An enterprise wireless network is a large network, for example using your machine in a business enterprise wireless network, with IEEE 802.1x support. If you configure your machine in an IEEE 802.1x supported wireless network, you can use the following authentication and encryption methods.

Authentication methods

- LEAP

  For LEAP, see *LEAP (For wireless network)* on page 122.
- EAP-FAST

  For EAP-FAST, see *EAP-FAST* on page 122.
- PEAP

  For PEAP, see *PEAP* on page 122.
- EAP-TTLS

  For EAP-TTLS, see *EAP-TTLS* on page 123.
- EAP-TLS

  For EAP-TLS, see *EAP-TLS* on page 123.

Encryption methods

- TKIP

  For TKIP, see *TKIP* on page 125.

- AES

  For AES, see *AES* on page 125.

- CKIP

  The original Key Integrity Protocol for LEAP by Cisco Systems, Inc.

User ID and password

The following security methods use a user ID less than 64 characters and a password of less than 32 characters in length.

- LEAP
- EAP-FAST
- PEAP
- EAP-TTLS
- EAP-TLS (For user ID)

12 Additional network settings from Windows®

Types of additional network settings

The following features are available to use if you want to configure additional network settings.

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

NOTE

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

Installing drivers used for printing and scanning via Web Services (Windows Vista®, Windows® 7 and Windows® 8)

The Web Services feature allows you to monitor machines on the network. This also simplifies the driver installation process. (For details about scanning using Web Services: see Software User's Guide.)

NOTE

- You must configure the IP address on your machine before you configure this setting.
- For Windows Server® 2008/2012, you must install Print Services.

1. Insert the installer CD-ROM.
2. Choose your CD-ROM drive/**install**/**driver**/**gdi**/**32_64**.
3. Double-click **dpinst86.exe** or **dpinst64.exe**.

NOTE

If the **User Account Control** screen appears,

(Windows Vista®) Click **Allow**.

(Windows® 7/Windows® 8) Click **Yes**.

4 (Windows Vista®)

Click , then choose **Network**.

(Windows® 7)

Click , **Control Panel**, **Network and Internet**, and then **View network computers and devices**.

(Windows® 8)

Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, click **Change PC settings**, and then click **Devices**.

5 (Windows Vista®/Windows® 7)

The machine's Web Services Name will be shown with the printer icon. Right-click the machine you want to install.

(Windows® 8)

Click **Add a device**. The machine's Web Services Name will be shown.

NOTE

- The Web Services Name for the Brother machine is your model name and the MAC Address (Ethernet Address) of your machine (e.g. Brother MFC-XXXX (model name) [XXXXXXXXXXXX] (MAC Address / Ethernet Address)).
- (Windows® 8)

  Move your mouse over the machine name to display the machine's information.

6 (Windows Vista®/Windows® 7)

From the pull down menu, click **Install**.

(Windows® 8)

Double-click the machine you want to install.

Uninstalling drivers used for printing and scanning via Web Services (Windows Vista®, Windows® 7 and Windows® 8)

To uninstall Web Services from a computer, follow the instructions below.

1. (Windows Vista®)
   Click  , then choose **Network**.
   (Windows® 7)
   Click , **Control Panel**, **Network and Internet** and then **View network computers and devices**.
   (Windows® 8)
   Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, click **Change PC settings**, and then click **Devices**.

2. (Windows Vista®/Windows® 7)
   The machine's Web Services Name will be shown with the printer icon. Right-click the machine you want to uninstall.
   (Windows® 8)
   The machine's Web Service Name will be shown. Select the machine you want to uninstall, and then click  next to the device name.

3. (Windows Vista®/Windows® 7)
   From the pull down menu, click **Uninstall**.
   (Windows® 8)
   When the dialog box appears, click **Remove**.

Network printing and scanning installation for Infrastructure mode when using Vertical Pairing (Windows® 7 and Windows® 8)

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 printer driver and scanner driver installation, from the multi-function printer icon that is in the **Add a device** screen.

If you are in Infrastructure mode, you can connect your machine to the wireless network and then install the printer 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 by using Web Based Management (web browser) or BRAdmin Professional 3.
- Make sure your WLAN access point/router includes the Windows® 7 or Windows® 8 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 or Windows® 8 compatibility logo. If you are not sure about the compatibility logo, contact your computer 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 or Windows® 8 compatibility logo. For more information, contact your wireless NIC manufacturer.
- To use a Windows® 7 or Windows® 8 computer as a Registrar, you need to register it to your network in advance. See the instruction, supplied with your WLAN access point/router.

1. Turn on your machine.
2. Set your machine in WPS mode (PIN Method).
   For how to configure your machine to use the PIN Method, see *Configuration using the PIN Method of WPS (Wi-Fi Protected Setup)* on page 29.
3. (Windows® 7)
   Click the  button and then **Devices and Printers**.
   (Windows® 8)
   Move your mouse to the lower right corner of your desktop. When the menu bar appears, click **Settings**, and then click **Control Panel**. In the **Hardware and Sound** group, click **View devices and printers**.
4. (Windows® 7)
   Choose **Add a device** on the **Devices and Printers** dialog box.
   (Windows® 8)
   Click **Add a device** on the command bar.
5. Choose your machine and input the PIN which your machine has indicated.
6. Choose the Infrastructure network that you want to connect to, and then click **Next**.
7. When your machine appears in the **Devices and Printers** dialog box, the wireless configuration and the printer driver installation are successfully completed.

13 Security terms and concepts

Security features

Security terms

- CA (Certificate Authority)

  A CA is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

- CSR (Certificate Signing Request)

  A CSR is a message sent from an applicant to a CA in order to apply for the issue of a certificate. The CSR contains information identifying the applicant, the public key generated by the applicant and the digital signature of the applicant.

- Certificate

  A Certificate is the information that binds together a public key with an identity. The certificate can be used to verify that a public key belongs to an individual. The format is defined by the x.509 standard.

- CA Certificate

  A CA Certificate is the certification that identifies the CA (Certificate Authority) itself and owns its private key. It verifies a certificate issued by the CA.

- Digital signature

  A Digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

- Public key cryptosystem

  A Public key cryptosystem is a modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

- Shared key cryptosystem

  A Shared key cryptosystem is a branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption).

Security protocols

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

These security communication protocols encrypt data to prevent security threats.

HTTPS

The version of the Internet protocol Hyper text Transfer Protocol (HTTP) that uses SSL.

IPPS

The version of the printing protocol Internet Printing Protocol that uses SSL.

SNMPv3

The Simple Network Management Protocol version 3 (SNMPv3) provides user authentication and data encryption to manage network devices securely.

Security methods for E-mail Sending and Receiving

NOTE

You can configure the security methods settings using Web Based Management (web browser). For the details, see *How to configure the machine settings using Web Based Management (web browser)* on page 57.

POP before SMTP (PbS)

The user authentication method for sending E-mail from a client. The client is given permission to use the SMTP server by accessing the POP3 server before sending the E-mail.

SMTP-AUTH (SMTP Authentication)

SMTP-AUTH expands SMTP (the Internet E-mail sending protocol) to include an authentication method that ensures the true identity of the sender is known.

APOP (Authenticated Post Office Protocol)

APOP expands POP3 (the Internet E-mail receiving protocol) to include an authentication method that encrypts the password when the client receives E-mail.

SMTP over SSL

SMTP over SSL feature enables sending encrypted E-mail using SSL.

POP over SSL

POP over SSL feature enables receiving encrypted E-mail using SSL.

Section III

Appendixes

Appendix A 137
Appendix B 138

A Appendix A

Supported protocols and security features

Interface	Ethernet [3]	10BASE-T, 100BASE-TX
	Wireless [1]	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, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP Client and Server, TELNET Server, HTTP/HTTPS server, TFTP client and server, POP3 [2], SMTP Client, SNMPv1/v2c/v3, ICMP, Web Services (Print/Scan), CIFS client, SNTP client
	Protocol (IPv6)	NDP, RA, DNS resolver, mDNS, LLMNR responder, LPR/LPD, Custom Raw Port/Port9100, IPP/IPPS, FTP Client and Server, TELNET Server, HTTP/HTTPS server, TFTP client and server, POP3 [2], SMTP Client, SNMPv1/v2c, ICMPv6, Web Services (Print/Scan), CIFS Client, SNTP Client
Network (Security)	Wired [3]	SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (EAP-MD5, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
	Wireless [1]	WEP 64/128 bit, WPA-PSK (TKIP/AES), WPA2-PSK (AES), SSL/TLS (IPPS, HTTPS), SNMP v3, 802.1x (LEAP, EAP-FAST, PEAP, EAP-TLS, EAP-TTLS), Kerberos
E-mail (Security)	Wired [3] and Wireless [1]	APOP, POP before SMTP, SMTP-AUTH, SSL/TLS (SMTP/POP)
Network (Wireless) [1]	Wireless Certification	Wi-Fi Certification Mark License (WPA™/WPA2™ - Enterprise, Personal), Wi-Fi Protected Setup™ (WPS) Identifier Mark License, AOSS Logo, Wi-Fi CERTIFIED™ Wi-Fi Direct™

[1] For HL-3180CDW, DCP-9015CDW, DCP-9020CDW, MFC-9130CW, MFC-9330CDW and MFC-9340CDW

[2] For MFC-9130CW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW: available as a download.

[3] For DCP-9020CDN, DCP-9020CDW, MFC-9140CDN, MFC-9330CDW and MFC-9340CDW

B Appendix B

Using services

A service is a resource that can be accessed by computers that wish to print to the Brother print server. The Brother print server provides the following predefined services (do a SHOW SERVICE command in the Brother print server remote console to see a list of available services): Enter `HELP` at the command prompt for a list of supported commands.

Service (Example)	Definition
BINARY_P1	TCP/IP binary
TEXT_P1	TCP/IP text service (adds carriage return after each line feed)
PCL_P1	PCL service (switches PJL-compatible machine to PCL mode)
BRNxxxxxxxxxxx	TCP/IP binary
BRNxxxxxxxxxxx_AT	PostScript® service for Macintosh
POSTSCRIPT_P1	PostScript® service (switches PJL-compatible machine to PostScript® mode)

Where “xxxxxxxxxxx” is your machine’s MAC Address (Ethernet Address).

Other ways to set the IP address (for advanced users and administrators)

Using DHCP to configure the IP address

The Dynamic Host Configuration Protocol (DHCP) is one of several automated mechanisms for IP address allocation. If you have a DHCP server on your network, the print server will automatically obtain its IP address from the DHCP server and register its name with any RFC 1001 and 1002-compliant dynamic name services.

NOTE

If you do not want your print server configured via DHCP, you must set the Boot Method to static so that the print server has a static IP address. This will prevent the print server from trying to obtain an IP address from any of these systems. To change the Boot Method, use the machine’s control panel Network menu, BRAdmin applications, Remote Setup (For MFC models), or Web Based Management (web browser).

Using RARP to configure the IP address

Before you configure the IP address using RARP, you must set the machine's Boot Method to RARP. To change the Boot Method, use the machine's control panel Network menu, BRAdmin applications, Remote Setup (For MFC models), or Web Based Management (web browser).

The Brother print server's IP address can be configured using the Reverse ARP (RARP) facility on your host computer. This is done by editing the `/etc/ethers` file (if this file does not exist, you can create it) with an entry similar to the following:

`00:80:77:31:01:07  BRN008077310107` (or `BRW008077310107` for a wireless network)

Where the first entry is the MAC Address (Ethernet Address) of the print server and the second entry is the name of the print server (the name must be the same as the one you put in the `/etc/hosts` file).

If the RARP daemon is not already running, start it (depending on the system the command can be `rarpd`, `rarpd -a`, `in.rarpd -a`, or another command; type `man rarpd` or refer to your system documentation for additional information). To verify that the RARP daemon is running on a Berkeley UNIX based system, type the following command:

```
ps -ax | grep -v grep | grep rarpd
```

For AT&T UNIX-based systems, type:

```
ps -ef | grep -v grep | grep rarpd
```

The Brother print server will get the IP address from the RARP daemon when the machine is powered on.

Using BOOTP to configure the IP address

Before you configure the IP address using BOOTP, you must set the machine's Boot Method to BOOTP. To change the Boot Method, use the machine's control panel Network menu, BRAdmin applications, Remote Setup (For MFC models), or Web Based Management (web browser).

BOOTP is an alternative to RARP that has the advantage of allowing configuration of the subnet mask and gateway. In order to use BOOTP to configure the IP address make sure that BOOTP is installed and running on your host computer (it should appear in the `/etc/services` file on your host as a real service; type `man bootpd` or refer to your system documentation for information). BOOTP is usually started up via the `/etc/inetd.conf` file, so you may need to enable it by removing the "#" in front of the bootp entry in that file. For example, a typical bootp entry in the /etc/inetd.conf file would be:

```
#bootp dgram udp wait /usr/etc/bootpd bootpd -i
```

Depending on the system, this entry might be called "bootps" instead of "bootp".

NOTE

In order to enable BOOTP, simply use an editor to delete the "#" (if there is no "#", then BOOTP is already enabled). Then edit the BOOTP configuration file (usually `/etc/bootptab`) and enter the name, network type (1 for Ethernet), MAC Address (Ethernet Address) and the IP address, subnet mask and gateway of the print server. Unfortunately, the exact format for doing this is not standardized, so you will need to refer to your system documentation to determine how to enter this information (many UNIX systems also have template examples in the bootptab file that you can use for reference). Some examples of typical `/etc/bootptab` entries include: ("BRN" below is "BRW" for a wireless network.)

```
BRN310107 1  00:80:77:31:01:07 192.168.1.2
```

and:

```
BRN310107:ht=ethernet:ha=008077310107:\ip=192.168.1.2:
```

Certain BOOTP host software implementations will not respond to BOOTP requests if you have not included a download filename in the configuration file. If this is the case, simply create a null file on the host and specify the name of this file and its path in the configuration file.

As with RARP, the print server will load its IP address from the BOOTP server when the machine is powered on.

Using APIPA to configure the IP address

The Brother print server supports the Automatic Private IP Addressing (APIPA) protocol. With APIPA, DHCP clients automatically configure an IP address and subnet mask when a DHCP server is not available. The device chooses it's own IP address in the range 169.254.1.0 through to 169.254.254.255. The subnet mask is automatically set to 255.255.0.0 and the gateway address is set to 0.0.0.0.

By default, the APIPA protocol is enabled. If you want to disable the APIPA protocol, you can disable it using the control panel of the machine, BRAdmin Light, or Web Based Management (web browser).

Using ARP to configure the IP address

If you are unable to use the BRAdmin application and your network does not use a DHCP server, you can also use the ARP command. The ARP command is available on Windows® systems that have TCP/IP installed as well as UNIX systems. To use ARP enter the following command at the command prompt:

```
arp -s ipaddress ethernetaddress
ping ipaddress
```

Where `ethernetaddress` is the MAC Address (Ethernet Address) of the print server and `ipaddress` is the IP address of the print server. For example:

■ **Windows® systems**

Windows® systems require the dash “-” character between each digit of the MAC Address (Ethernet Address).

```
arp -s 192.168.1.2 00-80-77-31-01-07
ping 192.168.1.2
```

■ **UNIX/Linux systems**

Typically, UNIX and Linux systems require the colon “:” character between each digit of the MAC Address (Ethernet Address).

```
arp -s 192.168.1.2 00:80:77:31:01:07
ping 192.168.1.2
```

NOTE

You must be on the same Ethernet segment (that is, there cannot be a router between the print server and operating system) to use the arp -s command.

If there is a router, you may use BOOTP or other methods described in this chapter to enter the IP address. If your administrator has configured the system to deliver IP addresses using BOOTP, DHCP, or RARP your Brother print server can receive an IP address from any one of these IP address allocation systems. In which case, you will not need to use the ARP command. The ARP command only works once. For security reasons, once you have successfully configured the IP address of a Brother print server using the ARP command, you cannot use the ARP command again to change the address. The print server will ignore any attempts to do this. If you wish to change the IP address again, use the Web Based Management (web browser), TELNET (using the SET IP ADDRESS command) or factory reset the print server (which will then allow you to use the ARP command again).

Using the TELNET console to configure the IP address

You can also use the TELNET command to change the IP address.

TELNET is an effective method to change the machine's IP address. But a valid IP address must already be programmed into the print server.

Type `TELNET <command line>` at the command prompt of the system prompt, where `<command line>` is the IP address of the print server. When you are connected, push the Return or Enter key to get the "#" prompt. Enter the password "**access**" (the password will not appear on the screen).

You will be prompted for a user name. Enter anything in response to this prompt.

You will then get the `Local>` prompt. Type `SET IP ADDRESS ipaddress`, where `ipaddress` is the desired IP address you wish to assign to the print server (check with your network administrator for the IP address to use). For example:

```
Local> SET IP ADDRESS 192.168.1.3
```

You will now need to set the subnet mask by typing `SET IP SUBNET subnet mask`, where `subnet mask` is the desired subnet mask you wish to assign to the print server (check with your network administrator for the subnet mask to use). For example:

```
Local> SET IP SUBNET 255.255.255.0
```

If you do not have any subnets, use one of the following default subnet masks:

255.0.0.0 for class A networks

255.255.0.0 for class B networks

255.255.255.0 for class C networks

The leftmost group of digits in your IP address can identify the type of network you have. The value of this group ranges from 1 through 127 for Class A networks (e.g. 13.27.7.1), 128 through 191 for Class B networks (e.g.128.10.1.30), and 192 through 255 for Class C networks (e.g. 192.168.1.4).

If you have a gateway (router), enter its address with the command `SET IP ROUTER routeraddress`, where `routeraddress` is the desired IP address of the gateway you wish to assign to the print server. For example:

```
Local> SET IP ROUTER 192.168.1.4
```

Type `SET IP METHOD STATIC` to set the method of IP access configuration to static.

To verify that you have entered the IP information correctly, type `SHOW IP`.

Type `EXIT` or Ctrl-D (i.e. hold down the control key and type "D") to end the remote console session.

C Index

A

Ad-hoc mode 12, 32
AES 125
AOSS™ 27, 39
APIPA 38, 116, 140
APOP 135
ARP 116, 141
Authentication 125

B

BINARY_P1 138
BOOTP 116, 140
BRAdmin Light 3, 5
BRAdmin Professional 3 ..... 3, 8, 97
BRNxxxxxxxxxxx 138
BRNxxxxxxxxxxx_AT 138
BRPrint Auditor 9

C

CA 133
CA Certificate 133
Certificate 84, 133
Channels 124
CIFS 119
CKIP 127
Control Panel 36
CSR 133
Custom Raw Port 117

D

DHCP 116, 138
Digital signature 133
DNS client 117
DNS server 38
Driver Deployment Wizard 3

E

EAP-FAST 122
EAP-MD5 122
EAP-TLS 123
EAP-TTLS 123
Encryption 125
Ethernet 39

F

Factory default 47
FTP 68, 118

G

Gateway 37

H

HTTP 56, 118
HTTPS 95, 134

I

IEEE 802.1x 15, 18, 122
Infrastructure mode 11
IP address 37, 120
IPP 117
IPPS 98, 134
IPv6 ..... 38, 119

L

LEAP 122
LLMNR 118
LPR/LPD 117

M

MAC Address 6, 7, 8, 37, 40, 48, 129, 138, 139, 140, 141
mDNS 117

N

NetBIOS name resolution 117
Network Configuration Report 48
Network Connection Repair Tool 108
Network Key 126
Network shared printing 115
Node name 37

O

Open system 125

P

PBC 27, 39
PCL_P1 138
PEAP 122
Peer-to-Peer 114
PIN Method 29, 39
POP before SMTP 100, 135
POP over SSL 135
Port 9100 117
POSTSCRIPT_P1 138
Protocol 116
Public key cryptosystem 133

R

RARP 116, 139
Remote Setup 3
Reset the network settings 47
RFC 1001 138

S

Security terms 133
Service 138
Shared key 125
Shared key cryptosystem 133
SMTP client 117
SMTP over SSL 135
SMTP-AUTH 100, 135
SNMP 118
SNMPv3 ..... 95, 134
SNTP 119
SSID 124
SSL/TLS 84, 134
Status Monitor 3
Subnet mask 37, 121
Supported protocols and security features 137

T

TCP/IP 36, 116
TELNET 118, 142
TEXT_P1 138
TKIP 125

V

Vertical Pairing 3, 128

W

Web Based Management (web browser) 3, 8, 95
Web Services 118, 128, 130
WEP 125
WINS 117
WINS Config 37
WINS Server 37
Wireless network 10, 124
WLAN report 48, 110, 112
WPA-PSK/WPA2-PSK 125
WPS (Wi-Fi Protected Setup) 27, 29, 39