LDAP Operation Guide

(Lightweight Directory Access Protocol)

To find basic information about network and advanced network features of your Brother machine: See the ➤➤ *Network User's Guide*.

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.

5-line LCD models: MFC-8510DN/8520DN/8710DW/8810DW/8910DW

Touchscreen models: DCP-8250DN and MFC-8950DW(T)

(For MFC-8510DN, MFC-8520DN and MFC-8710DW)

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

Definitions of notes

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

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

Trademarks

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

Microsoft, Windows, Windows Server and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Each company whose software title is mentioned in this manual has a Software License Agreement specific to its proprietary programs.

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

IMPORTANT NOTE

■ 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

1 Introduction

Overview

The LDAP protocol allows you to search for information such as fax numbers and E-mail addresses from your server. When you use the Fax, I-Fax or Scan to E-mail server features, you can use the LDAP search to find fax numbers or E-mail addresses.

Every E-mail program has a personal address book, but how do you look up an address for someone who's never sent you an E-mail? How can an organization keep one centralized up-to-date phone book that everybody has access to? The solution is to have LDAP. LDAP, Lightweight Directory Access Protocol, is an Internet protocol that E-mail and other programs use to look up information from a directory server on your network. So, instead of having to write in the recipients E-mail address or have to find it from another source, you can search for it using LDAP direct from the control panel of the multifunction machine.

Benefits to the customer

■ It simplifies the process of sending a fax or scanning a document to E-mail through its effective search facility.

■ It can save time, particularly if the recipients E-mail address if unknown to the sender.

2 Configuration for LDAP using a Web Browser

Changing the LDAP configuration

> 📝 **Note**
>
> We recommend to use Windows® Internet Explorer® 7.0/8.0 or Firefox® 3.6 for Windows® and Safari 4.0/5.0 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.

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 Check **LDAP** and then click **Submit**.

⑦ Restart the machine to activate the configuration.

8 Make sure the machine is turned on and then choose **Advanced Setting** on the **Protocol** page. You can configure and change the following LDAP settings using a web browser.
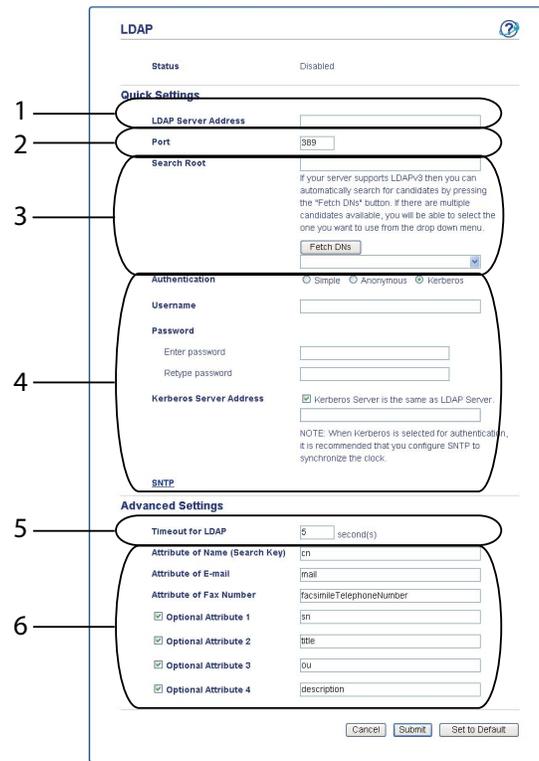
1 This is the location of your LDAP server.

2 Change the port if necessary. (389 is the typical port number of LDAP).

If you want to connect to the Global Catalog, enter the port number 3268.

3 Enter **Search Root**. This is the place to start a search. For example; if the domain name of the Active Directory server is set to "local.example.com", the Search Root could be such as "cn=Users, dc=local, dc=example, dc=com".

If your server supports LDAPv3, you can automatically obtain the Search Root by pressing **Fetch DNs**.

4 Select **Simple** method in the **Authentication** section, and specify **Username** [1] and **Password** [1]. In the case of connecting to the Active Directory server, enter the DN (Distinguished Name) format. (e.g. "cn=username, cn=Users, dc=local, dc=example, dc=com ")

5 This is how many seconds the machine will wait for a response from the LDAP server.

6 Enter the attribute type for name, E-mail address and fax number as used on the LDAP server.

[1]   This selection will only be available depending on the authentication method used.

i After you have configured the LDAP settings, click **Submit**. Make sure that the **Status** is **OK** on the Test Result page.

Note

- The LDAP function of this machine supports LDAPv3.

- You need to use Kerberos Authentication or Simple Authentication to communicate with your LDAP server.

  If the LDAP server supports Kerberos Authentication, we recommend to choose **Kerberos** for the **Authentication** setting. It provides strong authentication between the LDAP server and your machine.

  You must configure the protocol (network time server), or you must set the date, time and time zone correctly on the control panel for Kerberos Authentication. The time must match the time on the server used for the Kerberos Authentication. (For information about setting, see *Synchronize with SNTP server* >> page 8.)

- SSL/TLS is not supported.

- For the details of each item, see the Help Text in the Web Based Management.

Configuring your machine to communicate with your E-mail server

You must also configure your Brother machine to communicate with your E-mail server.

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. Make sure **POP3/SMTP** is checked and click **Advanced Setting**.

7 Change the E-mail server settings.

1   This is the location of your SMTP server and associated SMTP port address. The standard port number for SMTP is 25.

2   If your SMTP server requires authentication, input the necessary information here.

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

4   Some features of this machine, like I-Fax, allow you to send and receive E-mails to it. Assign your printer an E-mail address to make use of these features.

5   If you use POP3, enter your POP3 details in here. The standard port number for this E-mail system is 110.

6   Click here if you use APOP (a more secure version of POP3).

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

8   This is the time which the multifunction machine will wait for each section of a segmented message before sending them all. If the message is only part complete, the part complete message will be sent.

8 After you have finished changing the settings, click **Submit**.

⑨ After a short while you will be asked if you want to send a test E-mail to ensure a connection has been established with your E-mail server.
Do one of the following:
If you want to test the connectivity, enter an E-mail address and click **Submit**. Go to step ⑩.
If you want to send a test E-mail, click **Send Test E-mail**.
If you do not want to test the connectivity, uncheck both test E-mail check boxes and then click **Submit**.
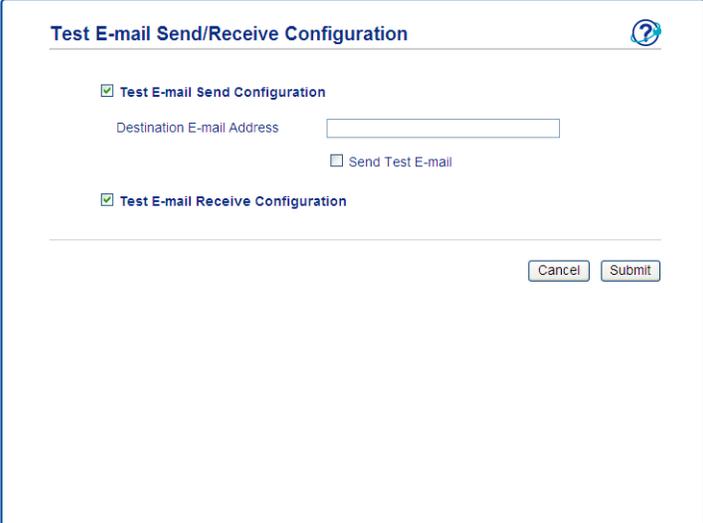
⑩ After a few moments the following screen appears if the connections to the E-mail server were successful. Click **OK**.
If they were not successful, go back and check your settings.
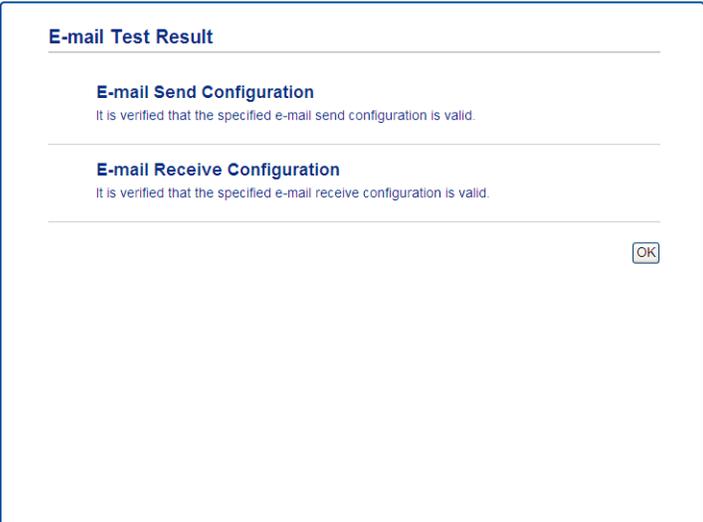
Synchronize with SNTP server

If the LDAP server supports Kerberos Authentication, and if you choose Kerberos for the 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 Kerberos Authentication. The time must match the time on the server used for the Kerberos Authentication.

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 LCD 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 time server.

Note

This function is not available in some countries.

a Start your web browser.

b 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/

c No password is required by default. If you have previously set a password, enter it and press ➡.

d Click **Network**, and then click **Protocol**.

e Select the **SNTP** check box to activate the setting.

f 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 time server. Click **Date&Time** and then configure **Date&Time** on the **General** screen. You can also configure the Date & Time from the machine's control panel.

Date&Time

Date	1 / 2 / 20xx
Time	xx : xx
Time Zone	UTC–xxxxx
Auto Daylight	⦿ Off ◯ On

☐ **Synchronize with SNTP server**

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

SNTP

Cancel　Submit

• 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** pull-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.

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

3

Machine operation

After you configure the LDAP settings, you can use the LDAP search to find fax numbers or E-mail addresses for the following features.

- Fax sending [1]

- I-Fax sending [1]

- Scan to E-mail server

[1] Not available for DCP-8250DN

LDAP operation using the control panel for MFC-8510DN, MFC-8520DN, MFC-8710DW, MFC-8810DW and MFC-8910DW

Fax or I-Fax sending

Note
- For more information on Fax sending: ▶▶ *Basic User's Guide* and *Advanced User's Guide*.
- For more information on I-Fax: ▶▶ *Network User's Guide*.

① Press ⬛ (**FAX**).

② Load your document.

③ Do one of the following:
If you want to change the fax resolution, press ▼ and press ◀ or ▶ to choose fax resolution. Press **OK**.
To send the document, go to step ④.

④ (For MFC-8520DN, MFC-8810DW and MFC-8910DW)
Do one of the following:
If you want to send a 2-sided document, press **Duplex**.
If you want to send a single-sided document, go to step ⑤.

Note
- You can send 2-sided documents from the ADF.
- When the machine is ready to scan 2-sided documents the LCD shows ⬛ for Duplex in the lower right corner.

⑤ Press ▲ to search.

f Enter the initial characters for your search by using the dial pad.

Note

You can enter up to 15 characters.

g Press ▲ or **OK**.
The LDAP search result will be shown on the LCD before the local address book search result with ▶. If there is no match on the server or the local address book, the LCD will show No Contact Found for 2 seconds.

h Press ▲ or ▼ to scroll until you find the name you are looking for.
To confirm details of the result information, highlight the result and press ▶.

i Press **OK**.

j If the result includes both a fax number and an E-mail address, the machine will prompt you to press ▲ or ▼ to choose either a fax number or an E-mail address.

k Do one of the following:
If you are sending a fax, choose a fax number and then press **OK**.
If you are sending an I-Fax, choose an E-mail address and then press **OK**.

l Press **Start**.

Scan to E-mail server

Note

- For information on PDF/A, Secure PDF and Signed PDF, see *PDF file format* ➤➤ page 28.

- If you choose Secure PDF, the machine will ask you to enter a 4 digit password using numbers 0-9 before it starts scanning.

- If you choose Signed PDF, you must install and then configure a certificate to your machine using Web Based Management.

  For the details on the certificate installation, see *Digital Certificate Installation* ➤➤ page 19.

1 Load your document.

2 Press ☰ (**SCAN**).

3 Press ▲ or ▼ to choose Scan to E-mail.
Press **OK**.

4 (For MFC-8520DN, MFC-8810DW and MFC-8910DW)
Do one of the following:
If you want to send a 2-sided document, press ▲ or ▼ to choose 1sided, 2sided (L)edge or 2sided (S)edge. Press **OK**.
If you want to send a single-sided document, go to step 5.

Note

- You can send 2-sided documents from the ADF.

- When the machine is ready to scan 2-sided documents the LCD shows [D] for Duplex in the lower right corner.

5 Press ▲ or ▼ to choose Change Setting. Press **OK**.
If you don't want to change the quality, go to step 10

6 Press ▲ or ▼ to choose Color 100 dpi, Color 200 dpi, Color 300 dpi, Color 600 dpi, Color Auto, Gray 100 dpi, Gray 200 dpi, Gray 300 dpi, Gray Auto, B&W 300 dpi, B&W 200 dpi or B&W 200x100 dpi. Press **OK**.
Do one of the following:
If you choose Color 100 dpi, Color 200 dpi, Color 300 dpi, Color 600 dpi, Color Auto, Gray 100 dpi, Gray 200 dpi, Gray 300 dpi or Gray Auto, go to step 7.
If you choose B&W 300 dpi, B&W 200 dpi or B&W 200x100 dpi, go to step 8.

7 Press ▲ or ▼ to choose PDF, PDF/A, Secure PDF, Signed PDF, JPEG or XPS.
Press **OK** and go to step 9.

8 Press ▲ or ▼ to choose PDF, PDF/A, Secure PDF, Signed PDF, JPEG or TIFF.
Press **OK** and go to step 10.

9 Press ▲ to choose the file size you want.
Press **OK** and go to step 10.

10 The LCD prompts you to enter an address. Press ▲ to search.

11 Enter the initial characters for your search by using the dial pad.

Note

You can enter up to 15 characters.

12 Press ▲ or **OK**.
The LDAP search result will be shown on the LCD before the local address book search result with ▶. If there is no match on the server or the local address book, the LCD will show No Contact Found for 2 seconds.

13 Press ▲ or ▼ to scroll until you find the name you are looking for.
To confirm details of the result information, highlight the result and press ▶.

14 Press **OK**.

15 If the result includes both a fax number and an E-mail address, the machine will prompt you to press ▲ or ▼ to choose either a fax number or an E-mail address.

16 If the result includes both a fax number and an E-mail address,choose an E-mail address and then press **OK**.

17 Press **Start**.

LDAP operation using the control panel for DCP-8250DN and MFC-8950DW(T)

Fax or I-Fax sending (For MFC-8950DW(T))

📝 **Note**

- For more information on Fax sending: ➤➤ *Basic User's Guide* and *Advanced User's Guide*.

- For more information on I-Fax: ➤➤ *Network User's Guide*.

1️⃣ Press `Fax`.

2️⃣ Load your document.

3️⃣ Set the scanner glass size, fax resolution or contrast if you want to change them.

4️⃣ Do one of the following:
If you want to send a 2-sided document, press `Duplex Fax` and choose `DuplexScan :LongEdge` or `DuplexScan :ShortEdge`.
If you want to send a single-sided document, go to step 6️⃣

📝 **Note**

You can send 2-sided documents from the ADF.

5️⃣ Press `Address Book`.

6️⃣ Press 🖥️🔍 to search.

7️⃣ Enter initial characters for your search by using the buttons on the LCD.

📝 **Note**

You can enter up to 15 characters.

8 Press OK.

The LDAP search result will be shown on the LCD with 🖥 before the local address book search result.

If there is no match on the server or the local address book, the LCD will show `Results cannot be found.` for about 60 seconds.

9 Press ▲ or ▼ to scroll until you find the name you are looking for and then press the name.
To confirm the details of the name, press `Detail`.

10 If the result includes more than one fax number or E-mail address, the machine will prompt you to choose either a fax number or an E-mail address.
Do one of the following:
If you are sending a fax, choose a fax number and then press `OK`.
If you are sending an I-Fax, choose an E-mail address and then press `OK`.

11 Press `Send a fax`.

12 Press **Start**.

Scan to E-mail server

✎ Note

- For information on PDF/A, Secure PDF and Signed PDF, see *PDF file format* ▶▶ page 28.
- If you choose Secure PDF, the machine will ask you to enter a 4 digit password using numbers 0-9 before it starts scanning.
- If you choose Signed PDF, you must install and then configure a certificate to your machine using Web Based Management.

    For the details on the certificate installation, see *Digital Certificate Installation* ▶▶ page 19.

1 Load your document.

2 Press Scan.

3 Press Scan to E-mail.

4 Press 🖥️🔍 to search.

5 Enter initial characters for your search by using the buttons on the LCD.

✎ Note

You can enter up to 15 characters.

6 Press OK.

The LDAP search result will be shown on the LCD with 🖥️ before the local address book search result.

If there is no match on the server and the local address book, the LCD will show Results cannot be found. for about 60 seconds.

7 Press ▲ or ▼ to scroll until you find the name you are looking for and then press the name.
To confirm the details of the name, press Detail.

8 If the result includes more than one fax number or E-mail address, the machine will prompt you to choose either a fax number or an E-mail address.
Choose an E-mail address and then press OK.

9 Press **Start**.

4

Digital Certificate for Signed PDF

Configure certificate for Signed PDF

If you choose Signed PDF, you must configure a certificate to your machine using Web Based Management.

To use Signed PDF, you must install a certificate to your machine and your computer.

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 **Administrator**.

⑤ Choose **Signed PDF** for a configuration.

⑥ Choose the certificate from the **Select the Certificate** pull-down list.
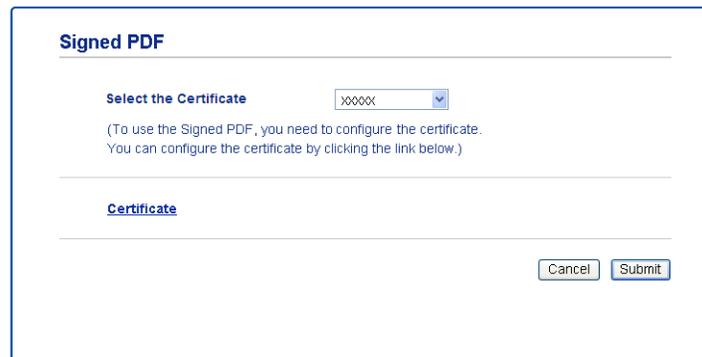
Signed PDF

Select the Certificate   XXXXX

(To use the Signed PDF, you need to configure the certificate.
You can configure the certificate by clicking the link below.)

Certificate

Cancel   Submit

⑦ Click **Submit**.

Supported Certificates

The Brother machine supports the following certificates.

■ 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 a self-signed certificate* ▶▶ page 20.)

■ Certificate from a CA

There are two methods for installing a certificate from a CA. If you already have 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 *Creating a Certificate Signing Request (CSR)* ▶▶ page 21.)

• When importing a certificate and a private key. (See *Import and export the certificate and private key* ▶▶ page 24.)

■ 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* ▶▶ page 25.)

4

Digital Certificate Installation

Signed PDF requires a digital certificate to be installed on both the machine and device which is sending data to the machine, e.g. a computer. In order to configure the certificate, the user needs to log onto the machine remotely through a web browser using its IP address.

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.
To create a self-signed certificate using Web Based Management, go to *Creating a self-signed certificate*
➤➤ page 20.
To create a Certificate Signing Request (CSR), go to *Creating a Certificate Signing Request (CSR)*
➤➤ page 21.
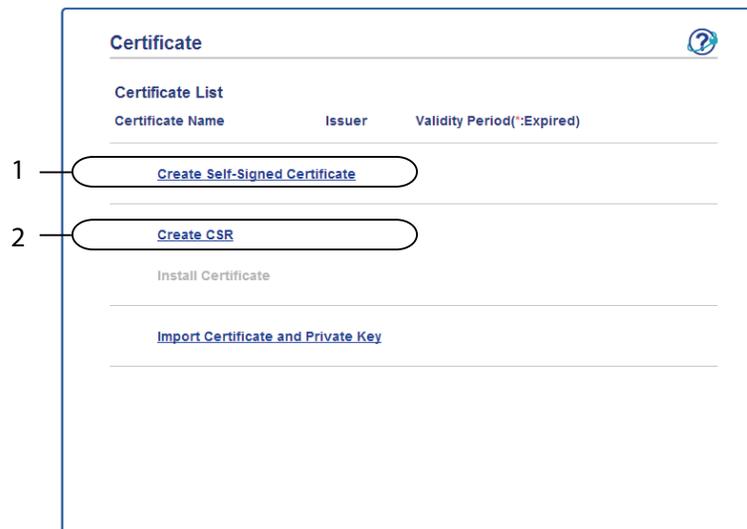
1 To create and install a self-signed certificate

2 To use a certificate from a Certificate Authority (CA)

📝**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 a self-signed certificate

a Click **Create Self-Signed Certificate**.

b Enter a **Common Name** and a **Valid Date**.

📝 **Note**

• The length of the **Common Name** can be up to 64 characters. 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.

c You can choose the **Public Key Algorithm** and **Digest Algorithm** settings from the pull-down list. The default settings are **RSA(2048bit)** for **Public Key Algorithm** and **SHA256** for **Digest Algorithm**.

d Click **Submit**.

e The self-signed certificate is created and saved in your machine's memory successfully.

Creating a Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is a request sent to a CA in order to authenticate the credentials contained within the certificate.

📝 **Note**

We recommend that the Root Certificate from the CA be installed on your computer before creating the CSR.

1️⃣ Click **Create CSR**.

2️⃣ Enter a **Common Name** and your information, such as **Organization**.
Your company details are required so that a CA can confirm your identity and attest to the outside world.

📝 **Note**

- The length of the **Common Name** can be up to 64 characters. 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** can be up to 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 pull-down list. The default settings are **RSA(2048bit)** for **Public Key Algorithm** and **SHA256** for **Digest Algorithm**.

④ Click **Submit**. The following screen will appear.

Create CSR

Please wait.

---
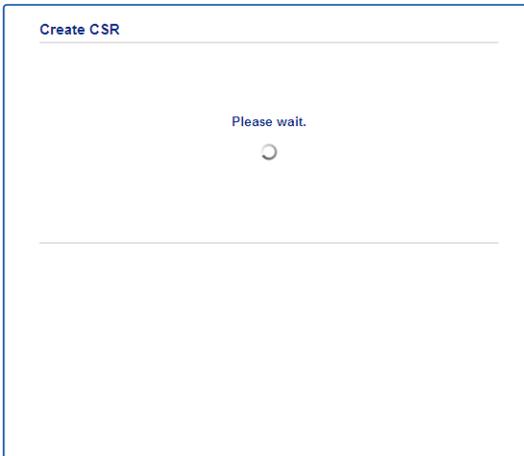
⑤ After a few moments, you will be presented with the certificate, which can be saved into a small file or copied and pasted directly into an online CSR form offered by a Certificate Authority. Click **Save** to save the CSR file to your computer.

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQChQAwdsEYMBYGA1UEAwMPQ1JOMDAwQkE5NkU5NDYwMSUwIwYDVQQK
ExwCcm80aGVyIEludGVybmF0aW9uYWwgRXVyb3B1MRIwEAYDVQQHEw1BdWR1bnNo
ZXcwEaARBgNVBAgTCb1hbmNoZXN0ZXIwCaAJBgNVBAYTAkdCMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2IfV80XY5tZ5+svRfR2dbyUUGdb9UsXGLQd1
8b8+IV0kx/BtF/yQ28cd9N6MfOLwVfsiesX4485vt07TQQ7jnV5jKxpnRP6T5Xvip
UShyNdi9IvFFsctuSDysReWCa895wGfb8cE5bBdIPN9wj2o0w0F8u9sJM2DABdQN
fXsN48XaS1Kp/WdY7sZ//gZ/SNrGV5VBeuJKkbo6vo2NPyYYxdHM2RKVeapCCTV8
1B2/1nrwayEaSi05rbhG1Mgjsi8M2BVnKshwhJswLp4fpi5Se8QjvkV6sOHaDLc6
t5M7jr1h5N2HYnOhIKoOmCHtswciKPJfC1r1XscQsP16v7AsaKwIDAQABoAAwDQYJ
KoIIhvcNAQELBQADggEBAM+IRNo+MUsbisfTsubscNG+60cF6sFIa8wQD/yTAssn
GIb8/5We2Y6vqkgfCveoE1YPPA5a3Rx+2SiFil0ieDMkQcbMjkrnOsv2v29v9NkbV
V7Zfi5LkKY16x6v1p8Ft9JhjGw4VKtsKTdTKsUVjrgmGlhif/8RuC/GjQP+ohdyvT
dq5oCHj+iqY5Ii0socS359BRSKRiKKerDT9hCSp4bOa0euMF+kpGsJGGILrffs03
MsNM0XgNggjYqldcPjHZ/41sCvaS+H3vj4q1+gNNIeVUgSQ1n/CsZdyy9OFNjsLy
2CYsHnsUUJ74kKb5MPKXvqksIoosiIsE7vJF4PZsQh8=
-----END CERTIFICATE REQUEST-----
```

Return Save

📝 **Note**

Follow your CA policy regarding the method to send a CSR to your CA.

---

⑥ The CSR is created. For instructions on how to install the certificate to your machine, go to *How to install the certificate to your machine* ➤➤ page 23.

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.
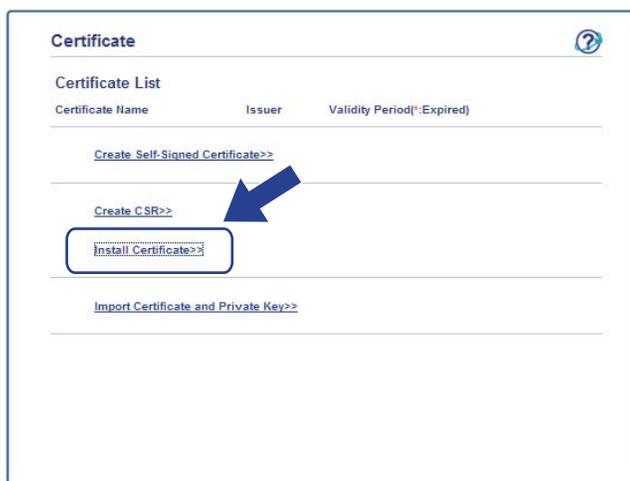
2. Specify the file of the certificate that has been issued by a CA, and then click **Submit**.

3. Now the certificate has been created successfully and saved in your machine memory successfully.

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

- a Click **Import Certificate and Private Key** on the **Certificate** page.

- b Specify the file that you want to import.

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

- d Now the certificate and private key are imported to your machine successfully.

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

- a Click **Export** shown with **Certificate List** on the **Certificate** page.

- b Enter a password if you want to encrypt the file.

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

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

- d Specify the location where you want to save the file.

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

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.

5   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 correctly and the Brother machine is turned on.
All protective packaging has been removed from the machine.
The toner cartridges and drum unit are installed correctly.
The front and back covers are fully closed.
Paper is inserted correctly in the paper tray.

Go to the page for your solution from the lists below

■ Error messages when using the LDAP operation

See *Error messages when using the LDAP operation* ▸▸ page 27

Error messages when using the LDAP operation

Error Message	Cause	Action
No LDAP Server	The Brother machine cannot connect to the LDAP server. However, the LDAP server configuration of the machine is correct.	■ Make sure your access point (for wireless), router or hub are turned on and its link button is blinking. ■ Make sure your local area network is running correctly. ■ Contact your network administrator for the information on the current network problems.
Confirm settings	The Brother machine cannot connect to the LDAP server due to the wrong LDAP server configuration of the machine.	Enter the correct LDAP server information on the LDAP configuration page of the Web Based Management. See *Changing the LDAP configuration* ▶▶ page 2.
	The Kerberos Authentication error.	Make sure you have entered a correct user name and a password for the Kerberos server. For more information on the Kerberos server settings, contact your network administrator.
	The date, time and time zone settings of the Brother machine is not correct.	Confirm your machine's date, time and time zone settings. See *Synchronize with SNTP server* ▶▶ page 8.
	The DNS server configuration is not correct.	Contact your network administrator for the information on the DNS server settings.
	The Kerberos Authentication configuration is correct. However, the user is not allowed to connect to the LDAP server.	Contact your network administrator for the information on your access rights.
No Kerberos Kerberos Error	The Brother machine cannot connect to the Kerberos server.	Contact your network administrator for the information on the Kerberos server settings.

5

Network terms and PDF file format

Network terms

- LDAP

The Lightweight Directory Access Protocol (LDAP) allows the Brother machine to search for information such as fax numbers and E-mail addresses from an LDAP server.

- 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).

PDF file format

- PDF/A

PDF/A is a PDF file format intended for long-term archiving. This format contains all the necessary information for reproducing the document after long-term storage.

- Secure PDF

Secure PDF is a PDF file format that has been password-protected.

- Signed PDF

Signed PDF is a PDF file format that helps prevent data tampering and the impersonation of an author by including a digital certificate within the document.

If you choose Signed PDF, you must install and then configure a certificate to your machine using Web Based Management.