Security Features Guide

Important Information for Security

- The default password to manage this machine’s settings is located on the bottom of the machine and marked "**Pwd:**". We recommend immediately changing the default password to protect your machine from unauthorized access.
- When connecting your machine to an outside network such as the Internet, make sure your network environment is protected by a separate firewall or other means in order to prevent information leaks due to inadequate settings or unauthorized access by malicious third parties.
- If there is a signal in the vicinity, wireless LAN allows you to freely make a LAN connection. However, if security settings are not correctly configured, the signal may be intercepted by malicious third-parties, possibly resulting in:
  - Theft of personal or confidential information
  - Improper transmission of information to parties impersonating the specified individuals
  - Dissemination of transcribed communication contents that were intercepted

Related Information

- Network

Configure Certificates for Device Security

You must configure a certificate to manage your networked machine securely using SSL/TLS. You must use Web Based Management to configure a certificate.

- Security Certificate Features Overview
- How to Create and Install a Certificate
- Create a Self-signed Certificate
- Create a Certificate Signing Request (CSR) and Install a Certificate from a Certificate Authority (CA)
- Import and Export the Certificate and Private Key
- Import and Export a CA Certificate

Security Certificate Features Overview

Your machine supports the use of multiple security certificates, which allows secure authentication and communication with the machine. The following security certificate features can be used with the machine:

Supported features, options, and settings may differ depending on your model.

- SSL/TLS communication
- IEEE 802.1x authentication
- IPsec

Your machine supports the following:

- Pre-installed certificate

  Your machine has a pre-installed self-signed certificate. This certificate enables you to use SSL/TLS communication without creating or installing a different certificate.

The pre-installed self-signed certificate protects your communication up to a certain level. 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 creating or installing a different certificate from a CA.

- Certificate from a Certificate Authority (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 Certificate Signing Request (CSR) from this print server.
  - When importing a certificate and a private key.

- Certificate Authority (CA) Certificate

  To use a CA certificate that identifies the CA and owns its private key, you must import that CA certificate from the CA before configuring Network security features.

- If you are going to use SSL/TLS communication, we recommend contacting 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 then reinstall them.

Related Information

- Configure Certificates for Device Security

Related Topics:

- Configure IEEE 802.1x Authentication for Your Network Using Web Based Management (Web Browser)

How to Create and Install a Certificate

There are two options when choosing a security certificate: use a self-signed certificate or use a certificate from a Certificate Authority (CA).

Option 1

Self-Signed Certificate

1. Create a self-signed certificate using Web Based Management.
2. Install the self-signed certificate on your computer.

Option 2

Certificate from a CA

1. Create a Certificate Signing Request (CSR) using Web Based Management.
2. Install the certificate issued by the CA on your Brother machine using Web Based Management.
3. Install the certificate on your computer.

Related Information

- Configure Certificates for Device Security

Create a Self-signed Certificate

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
4. In the left navigation bar, click **Network** > **Security** > **Certificate**.

   If the left navigation bar is not visible, start navigating from ☰.
5. Click **Create Self-Signed Certificate**.
6. Enter a **Common Name** and a **Valid Date**.
   - The length of the **Common Name** is less than 64 bytes. 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 appear 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.
7. Select your setting from the **Public Key Algorithm** drop-down list.
8. Select your setting from the **Digest Algorithm** drop-down list.
9. Click **Submit**.

Related Information

- Configure Certificates for Device Security

Create a Certificate Signing Request (CSR) and Install a Certificate from a Certificate Authority (CA)

If you already have a certificate from an external trusted Certificate Authority (CA) , you can store the certificate and private key on the machine and manage them by importing and exporting. If you do not have a certificate from an external trusted CA, create a Certificate Signing Request (CSR), send it to a CA for authentication, and install the returned certificate on your machine.

- Create a Certificate Signing Request (CSR)
- Install a Certificate on Your Machine

Create a Certificate Signing Request (CSR)

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

We recommend installing a Root Certificate from the CA on your computer before creating the CSR.

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network** > **Security** > **Certificate**.

If the left navigation bar is not visible, start navigating from ≡.

5. Click **Create CSR**.
6. Type a **Common Name** (required) and add other information about your **Organization** (optional).

- Your company details are required so that a CA can confirm your identity and verify it to an outsider.
- The length of the **Common Name** must be less than 64 bytes. 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. The **Common Name** is required.
- A warning will appear if you type 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 bytes.
- The **Country/Region** should be a two-character ISO 3166 country code.
- If you are configuring an X.509v3 certificate extension, select the **Configure extended partition** checkbox, and then select **Auto (Register IPv4)** or **Manual**.

7. Select your setting from the **Public Key Algorithm** drop-down list.
8. Select your setting from the **Digest Algorithm** drop-down list.
9. Click **Submit**.

   The CSR appears on your screen. Save the CSR as a file or copy and paste it into an online CSR form offered by a Certificate Authority.
10. Click **Save**.

- Follow your CA's policy regarding the method to send a CSR to your CA.
- If you are using the Enterprise Root CA of Windows Server, we recommend using the Web Server for the certificate template to securely create the Client Certificate. 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.

Related Information

- Create a Certificate Signing Request (CSR) and Install a Certificate from a Certificate Authority (CA)

Install a Certificate on Your Machine

When you receive a certificate from a Certificate Authority (CA), follow the steps below to install it on the print server:

Only a certificate issued with your machine's Certificate Signing Request (CSR) can be installed on your machine. When you want to create another CSR, make sure that the certificate is installed before creating the new CSR. Create another CSR only after installing the certificate on the machine, otherwise the CSR created before installing the new CSR will be invalid.

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
4. In the left navigation bar, click **Network** > **Security** > **Certificate**.

   If the left navigation bar is not visible, start navigating from ☰.
5. Click **Install Certificate**.
6. Browse to the file that contains the certificate issued by the CA, and then click **Submit**.

   The certificate is created and saved in your machine's memory.

To use SSL/TLS communication, the Root Certificate from the CA must be installed on your computer. Contact your network administrator.

Related Information

- Create a Certificate Signing Request (CSR) and Install a Certificate from a Certificate Authority (CA)

Import and Export the Certificate and Private Key

Store the certificate and private key on your machine and manage them by importing and exporting them.

- Import a Certificate and Private Key
- Export the Certificate and Private Key

Import a Certificate and Private Key

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

> The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network** > **Security** > **Certificate**.

> If the left navigation bar is not visible, start navigating from ≡.

5. Click **Import Certificate and Private Key**.
6. Browse and select to the file you want to import.
7. Type the password if the file is encrypted, and then click **Submit**.

The certificate and private key are imported to your machine.

Related Information

- Import and Export the Certificate and Private Key

Export the Certificate and Private Key

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

> The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network** > **Security** > **Certificate**.

> If the left navigation bar is not visible, start navigating from ≡.

5. Click **Export** shown with **Certificate List**.
6. Enter the password if you want to encrypt the file.

   If a blank password is used, the output is not encrypted.
7. Enter the password again for confirmation, and then click **Submit**.
8. Click **Save**.

The certificate and private key are exported to your computer.

You can also import the certificate to your computer.

Related Information

- Import and Export the Certificate and Private Key

Import and Export a CA Certificate

You can import, export, and store CA certificates on your Brother machine.

- Import a CA Certificate
- Export a CA Certificate

Import a CA Certificate

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
4. In the left navigation bar, click **Network** > **Security** > **CA Certificate**.

   If the left navigation bar is not visible, start navigating from ≡.
5. Click **Import CA Certificate**.
6. Browse to the file you want to import.
7. Click **Submit**.

Related Information

- Import and Export a CA Certificate

Export a CA Certificate

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
4. In the left navigation bar, click **Network** > **Security** > **CA Certificate**.

   If the left navigation bar is not visible, start navigating from ☰.
5. Select the certificate you want to export and click **Export**.
6. Click **Submit**.

Related Information

- Import and Export a CA Certificate

Use SSL/TLS

- Manage Your Network Machine Securely Using SSL/TLS
- Print Documents Securely Using SSL/TLS
- Send or Receive an Email Securely Using SSL/TLS

Manage Your Network Machine Securely Using SSL/TLS

Configure a Certificate for SSL/TLS and Available Protocols

Configure a certificate on your machine using Web Based Management before you use SSL/TLS communication.

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

> The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network** > **Network** > **Protocol**.

> If the left navigation bar is not visible, start navigating from ≡.

5. Click **HTTP Server Settings**.
6. Select the certificate you want to configure from the **Select the Certificate** drop-down list.
7. Click **Submit**.
8. Click **Yes** to restart your print server.

Related Information

- Manage Your Network Machine Securely Using SSL/TLS

Related Topics:

- Print Documents Securely Using SSL/TLS

Access Web Based Management Using SSL/TLS

To manage your network machine securely, you must use management utilities with security protocols.

- To use HTTPS protocol, HTTPS must be enabled on your machine. The HTTPS protocol is enabled by default.
- You can change the HTTPS protocol settings using the Web Based Management screen.

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

The default password to manage this machine’s settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. You can now access the machine using HTTPS.

Related Information

- Manage Your Network Machine Securely Using SSL/TLS

Install the Self-signed Certificate for Windows Users as Administrator

- The following steps are for Microsoft Edge. If you use another web browser, refer to your web browser's documentation or online help for instructions on how to install certificates.
- Make sure you have created your self-signed certificate using Web Based Management.

1. Right-click the **Microsoft Edge** icon, and then click **Run as administrator**.

   If the **User Account Control** screen appears, click **Yes**.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If your connection is not private, click the **Advanced** button, and then continue to the web page.
4. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
5. In the left navigation bar, click **Network** > **Security** > **Certificate**.

   If the left navigation bar is not visible, start navigating from ≡.
6. Click **Export**.
7. To encrypt the output file, type a password in the **Enter password** field. If the **Enter password** field is blank, your output file will not be encrypted.
8. Type the password again in the **Retype password** field, and then click **Submit**.
9. Click the downloaded file to open it.
10. When the **Certificate Import Wizard** appears, click **Next**.
11. Click **Next**.
12. If required, type a password, and then click **Next**.
13. Select **Place all certificates in the following store**, and then click **Browse...**.
14. Select the **Trusted Root Certification Authorities**, and then click **OK**.
15. Click **Next**.
16. Click **Finish**.
17. Click **Yes**, if the fingerprint (thumbprint) is correct.
18. Click **OK**.

Related Information

- Manage Your Network Machine Securely Using SSL/TLS

Print Documents Securely Using SSL/TLS

Print Documents Using IPPS

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

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

   The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.
4. In the left navigation bar, click **Network** > **Network** > **Protocol**.

   If the left navigation bar is not visible, start navigating from ≡.
5. Make sure the **IPP** checkbox is selected.

   If the **IPP** checkbox is not selected, select the **IPP** checkbox, and then click **Submit**.

   Restart your machine to activate the configuration.

   After the machine restarts, return to the machine's web page, type the password, and then in the left navigation bar, click **Network** > **Network** > **Protocol**.
6. Click **HTTP Server Settings**.
7. Select the **HTTPS** checkbox in the **IPP** area, and then click **Submit**.
8. Restart your machine to activate the configuration.

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

Related Information

- Print Documents Securely Using SSL/TLS

Use SNMPv3

- Manage Your Network Machine Securely Using SNMPv3

Manage Your Network Machine Securely Using SNMPv3

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

1. Start your web browser.
2. Type "https://Common Name" in your browser's address bar (where "Common Name" is the Common Name that you assigned to the certificate; this could be your IP address, node name, or domain name).
3. If required, type the password in the **Login** field, and then click **Login**.

The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network** > **Network** > **Protocol**.

If the left navigation bar is not visible, start navigating from ≡.

5. Make sure the **SNMP** setting is enabled, and then click **Advanced Settings**.
6. Configure the SNMPv1/v2c mode settings.

Option	Description
SNMP v1/v2c read-write access	The print server uses version 1 and version 2c of the SNMP protocol. You can use all of your machine's applications in this mode. However, it is not secure since it will not authenticate the user and data will not be encrypted.
SNMP v1/v2c read-only access	The print server uses the read-only access of version 1 and version 2c of the SNMP protocol.
Disabled	Disable version 1 and version 2c of the SNMP protocol. All applications that use SNMPv1/v2c will be restricted. To allow the use of SNMPv1/v2c applications, use the **SNMP v1/v2c read-only access** or **SNMP v1/v2c read-write access** mode.

7. Configure the SNMPv3 mode settings.

Option	Description
Enabled	The print server uses version 3 of the SNMP protocol. To manage the print server securely, use the SNMPv3 mode, and then configure the settings.
Disabled	Disable version 3 of the SNMP protocol. All applications that use SNMPv3 will be restricted. To allow the use of SNMPv3 applications, use the SNMPv3 mode.

8. Click **Submit**.

If your machine displays the protocol setting options, select the options you want.

9. Restart your machine to activate the configuration.

Related Information

- Use SNMPv3

Use IEEE 802.1x Authentication for Your Network

What Is IEEE 802.1x Authentication?

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

Related Information

- Use IEEE 802.1x Authentication for Your Network

Configure IEEE 802.1x Authentication for Your Network Using Web Based Management (Web Browser)

- 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 writing down the certificate name you want to use.
- Before you verify the server certificate, you must import the CA certificate issued by the CA that signed the server certificate. Contact your network administrator or your Internet Service Provider (ISP) to confirm whether a CA certificate import is necessary.

You can also configure IEEE 802.1x authentication using the Wireless Setup Wizard from the control panel (Wireless network).

1. Start your web browser.
2. Type "https://machine's IP address" in your browser's address bar (where "machine's IP address" is your machine's IP address).

   For example:

   https://192.168.1.2

   Your machine's IP address can be found in the Network Configuration Report.
3. If required, type the password in the **Login** field, and then click **Login**.

The default password to manage this machine's settings is located on the back or base of the machine and marked "**Pwd**". Change the default password by following the on-screen instructions when you first log in.

4. In the left navigation bar, click **Network**.

If the left navigation bar is not visible, start navigating from ≡.

5. Do one of the following:
   - For the wired network

     Click **Wired** > **Wired 802.1x Authentication**.
   - For the wireless network

     Click **Wireless** > **Wireless (Enterprise)**.
6. Configure the IEEE 802.1x authentication settings.

- To enable IEEE 802.1x authentication for wired networks, select **Enabled** for **Wired 802.1x status** on the **Wired 802.1x Authentication** page.
- If you are using **EAP-TLS** authentication, you must select the client certificate installed (shown with certificate name) for verification from the **Client Certificate** drop-down list.
- If you select **EAP-FAST**, **PEAP**, **EAP-TTLS**, or **EAP-TLS** authentication, select the verification method from the **Server Certificate Verification** drop-down list. Verify the server certificate using the CA certificate, imported to the machine in advance, issued by the CA that signed the server certificate.

Select one of the following verification methods from the **Server Certificate Verification** drop-down list:

Option	Description
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 issued by the CA that signed the server certificate.

Option	Description
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.

7. When finished with configuration, click **Submit**.

   For wired networks: 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.

Option	Description
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.

Related Information

- Use IEEE 802.1x Authentication for Your Network

Related Topics:

- Security Certificate Features Overview
- Configure Certificates for Device Security

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**.

IEEE 802.1x Authentication Methods

EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secured Tunneling (EAP-FAST) 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.

Your Brother machine supports the following inner authentication methods:

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

EAP-MD5 (Wired network)

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

PEAP

Protected Extensible Authentication Protocol (PEAP) is a version of EAP method developed by Cisco Systems, Inc., Microsoft Corporation and RSA Security. PEAP creates an encrypted Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 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.

Your Brother machine supports the following inner authentication methods:

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) 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.

Your Brother machine supports the following inner authentication methods:

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

EAP-TLS

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

Related Information

- Use IEEE 802.1x Authentication for Your Network