# Security Features Guide

# Table of Contents

# Introduction

# Definitions of Notes

We use the following symbols and conventions 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** | NOTE specifies the operating environment, conditions for installation, or special conditions of use. |
|  | Tips icons indicate helpful hints and supplementary information. |
| **Bold** | Bold style identifies buttons on the machine's control panel or computer screen. |
| *Italics* | Italicized style emphasizes an important point or refers you to a related topic. |

## Related Information

- Introduction

# Trademarks

Adobe® and Reader® are either registered trademarks or trademarks of Adobe Systems Incorporated 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.**

## Related Information

- Introduction

# Copyright



## Related Information

- Introduction

# Before Using Network Security Features

Your 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.

We recommend disabling the FTP and TFTP protocols. Accessing the machine using these protocols is not secure.

## Related Information

- Introduction
  - Disable Unnecessary Protocols

# Disable Unnecessary Protocols

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. Clear any unnecessary protocol checkboxes to disable them.
6. Click **Submit**.
7. Restart your Brother machine to activate the configuration.

## Related Information

- Before Using Network Security Features

# Network Security

# 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
- Configure a Certificate for SSL/TLS and Available Protocols
- Configure Certificates for Device Security

# 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(Port 443)** 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.<br>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. |
| **Disabled** | Disable version 3 of the SNMP protocol.<br>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 IPsec

# Introduction to IPsec

IPsec (Internet Protocol Security) is a security protocol that uses an optional Internet Protocol function to prevent data manipulation and ensure the confidentiality of data transmitted as IP packets. IPsec encrypts data carried over a network, such as print data sent from computers to a printer. Because the data is encrypted at the network layer, applications that employ a higher-level protocol use IPsec even if the user is not aware of its use.

IPsec supports the following functions:

- IPsec transmissions

  According to the IPsec setting conditions, a network-connected computer sends data to and receives data from a specified device using IPsec. When devices start communicating using IPsec, keys are exchanged using Internet Key Exchange (IKE) first, and then the encrypted data is transmitted using the keys.

  In addition, IPsec has two operation modes: the Transport mode and Tunnel mode. The Transport mode is used mainly for communication between devices and the Tunnel mode is used in environments such as a Virtual Private Network (VPN).

For IPsec transmissions, the following conditions are necessary:

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

- IPsec settings

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

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

## Related Information

- Use IPsec

# Configure IPsec Using Web Based Management

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

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** > **IPsec**.

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

| Option | Description |
|---|---|
| **Status** | Enable or disable IPsec. |
| **Negotiation Mode** | Select **Negotiation Mode** for IKE Phase 1. IKE is a protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec.<br>In the **Main** mode, the processing speed is slow, but the security is high. In the **Aggressive** mode, the processing speed is faster than in the **Main** mode, but the security is lower. |
| **All Non-IPsec Traffic** | Select the action to be taken for non-IPsec packets.<br>When using Web Services, you must select **Allow** for **All Non-IPsec Traffic**. If you select **Drop**, Web Services cannot be used. |
| **Broadcast/Multicast Bypass** | Select **Enabled** or **Disabled**. |
| **Protocol Bypass** | Select the checkboxes for the option or options you want. |
| **Rules** | Select the **Enabled** checkbox to activate the template. When you select multiple checkboxes, the lower numbered checkboxes have priority if the settings for the selected checkboxes conflict.<br>Click the corresponding drop-down list to select the **Address Template** that is used for the IPsec connection conditions. To add an **Address Template**, click **Add Template**.<br>Click the corresponding drop-down list to select the **IPsec Template** that is used for the IPsec connection conditions. To add an **IPsec Template**, click **Add Template**. |

6. Click **Submit**.

   If the machine must be restarted to activate the new settings, the restart confirmation screen will appear.

   If there is a blank item in the template you enabled in the **Rules** table, an error message appears. Confirm your choices and click **Submit** again.

## Related Information

- Use IPsec

**Related Topics:**

- Configure Certificates for Device Security

# Configure an IPsec Address Template Using Web Based Management

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** > **IPsec Address Template**.

   If the left navigation bar is not visible, start navigating from ☰.
5. Click the **Delete** button to delete an **Address Template**. When an **Address Template** is in use, it cannot be deleted.
6. Click the **Address Template** that you want to create. The **IPsec Address Template** appears.
7. Configure the settings.

| Option | Description |
|---|---|
| **Template Name** | Type a name for the template (up to 16 characters). |
| **Local IP Address** | • **IP Address**<br>Specify the IP address. Select **ALL IPv4 Address**, **ALL IPv6 Address**, **ALL Link Local IPv6**, or **Custom** from the drop-down list.<br>If you select **Custom** from the drop-down list, type the IP address (IPv4 or IPv6) in the text box.<br>• **IP Address Range**<br>Type the starting and ending IP addresses for the IP address range in the text boxes. If the starting and ending IP addresses are not standardized to IPv4 or IPv6, or the ending IP address is smaller than the starting address, an error will occur.<br>• **IP Address / Prefix**<br>Specify the IP address using CIDR notation.<br>For example: 192.168.1.1/24<br>Because the prefix is specified in the form of a 24-bit subnet mask (255.255.255.0) for 192.168.1.1, the addresses 192.168.1.### are valid. |
| **Remote IP Address** | • **Any**<br>If you select **Any**, all IP addresses are enabled.<br>• **IP Address**<br>Type the specified IP address (IPv4 or IPv6) in the text box.<br>• **IP Address Range**<br>Type the first and last IP addresses for the IP address range. If the first and last IP addresses are not standardized to IPv4 or IPv6, or the last IP address is smaller than the first address, an error will occur.<br>• **IP Address / Prefix**<br>Specify the IP address using CIDR notation. |

| Option | Description |
| --- | --- |
| | For example: 192.168.1.1/24<br>Because the prefix is specified in the form of a 24-bit subnet mask (255.255.255.0) for 192.168.1.1, the addresses 192.168.1.### are valid. |

8. Click **Submit**.

When you change the settings for the template currently in use, restart your machine to activate the configuration.

## Related Information

- Use IPsec

# Configure an IPsec Template Using Web Based Management

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** > **IPsec Template**.

   If the left navigation bar is not visible, start navigating from ☰.
5. Click the **Delete** button to delete an **IPsec Template**. When an **IPsec Template** is in use, it cannot be deleted.
6. Click the **IPsec Template** that you want to create. The **IPsec Template** screen appears. The configuration fields differ based on the **Use Prefixed Template** and **Internet Key Exchange (IKE)** settings you select.
7. In the **Template Name** field, type a name for the template (up to 16 characters).
8. If you selected **Custom** in the **Use Prefixed Template** drop-down list, select the **Internet Key Exchange (IKE)** options, and then change the settings if needed.
9. Click **Submit**.

## Related Information

- Use IPsec
  - IKEv1 Settings for an IPsec Template
  - IKEv2 Settings for an IPsec Template
  - Manual Settings for an IPsec Template

# IKEv1 Settings for an IPsec Template

| Option | Description |
|---|---|
| **Template Name** | Type a name for the template (up to 16 characters). |
| **Use Prefixed Template** | Select **Custom**, **IKEv1 High Security** or **IKEv1 Medium Security**. The setting items are different depending on the selected template. |
| **Internet Key Exchange (IKE)** | IKE is a communication protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec. To carry out encrypted communication for that time only, the encryption algorithm that is necessary for IPsec is determined and the encryption keys are shared. For IKE, the encryption keys are exchanged using the Diffie-Hellman key exchange method, and encrypted communication that is limited to IKE is carried out.<br>If you selected **Custom** in **Use Prefixed Template**, select **IKEv1**. |
| **Authentication Type** | • **Diffie-Hellman Group**<br>This key exchange method allows secret keys to be securely exchanged over an unprotected network. The Diffie-Hellman key exchange method uses a discrete logarithm problem, not the secret key, to send and receive open information that was generated using a random number and the secret key.<br>Select **Group1**, **Group2**, **Group5**, or **Group14**.<br>• **Encryption**<br>Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.<br>• **Hash**<br>Select **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.<br>• **SA Lifetime**<br>Specify the IKE SA lifetime.<br>Type the time (seconds) and number of kilobytes (KByte). |
| **Encapsulating Security** | • **Protocol**<br>Select **ESP**, **AH**, or **AH+ESP**.<br>- ESP is a protocol for carrying out encrypted communication using IPsec. ESP encrypts the payload (communicated contents) and adds additional information. The IP packet comprises the header and the encrypted payload, which follows the header. In addition to the encrypted data, the IP packet also includes information regarding the encryption method and encryption key, the authentication data, and so on.<br>- AH is part of the IPsec protocol that authenticates the sender and prevents manipulation (ensures the completeness) of the data. In the IP packet, the data is inserted immediately after the header. In addition, the packets include hash values, which are calculated using an equation from the communicated contents, secret key, and so on, in order to prevent the falsification of the sender and manipulation of the data. Unlike ESP, the communicated contents are not encrypted, and the data is sent and received as plain text.<br>• **Encryption (Not available for the AH option.)**<br>Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.<br>• **Hash**<br>Select **None**, **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.<br>**None** can be selected only when **ESP** is selected for **Protocol**. |

| Option | Description |
|---|---|
| | • **SA Lifetime**<br>Specify the IKE SA lifetime.<br>Type the time (seconds) and number of kilobytes (KByte).<br>• **Encapsulation Mode**<br>Select **Transport** or **Tunnel**.<br>• **Remote Router IP-Address**<br>Type the IP address (IPv4 or IPv6) of the remote router. Enter this information only when the **Tunnel** mode is selected.<br>SA (Security Association) is an encrypted communication method using IPsec or IPv6 that exchanges and shares information, such as the encryption method and encryption key, in order to establish a secure communication channel before communication begins. SA may also refer to a virtual encrypted communication channel that has been established. The SA used for IPsec establishes the encryption method, exchanges the keys, and carries out mutual authentication according to the IKE (Internet Key Exchange) standard procedure. In addition, the SA is updated periodically. |
| **Perfect Forward Secrecy (PFS)** | PFS does not derive keys from previous keys that were used to encrypt messages. In addition, if a key that is used to encrypt a message was derived from a parent key, that parent key is not used to derive other keys. Therefore, even if a key is compromised, the damage will be limited only to the messages that were encrypted using that key.<br>Select **Enabled** or **Disabled**. |
| **Authentication Method** | Select the authentication method. Select **Pre-Shared Key** or **Certificates**. |
| **Pre-Shared Key** | When encrypting communication, the encryption key is exchanged and shared beforehand using another channel.<br>If you selected **Pre-Shared Key** for the **Authentication Method**, type the **Pre-Shared Key** (up to 32 characters).<br>• **Local/ID Type/ID**<br>Select the sender's ID type, and then type the ID.<br>Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.<br>If you select **Certificate**, type the common name of the certificate in the **ID** field.<br>• **Remote/ID Type/ID**<br>Select the recipient's ID type, and then type the ID.<br>Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.<br>If you select **Certificate**, type the common name of the certificate in the **ID** field. |
| **Certificate** | If you selected **Certificates** for **Authentication Method**, select the certificate.<br>You can select only the certificates that were created using the **Certificate** page of Web Based Management's Security configuration screen. |

## Related Information

- Configure an IPsec Template Using Web Based Management

# IKEv2 Settings for an IPsec Template

| Option | Description |
|---|---|
| **Template Name** | Type a name for the template (up to 16 characters). |
| **Use Prefixed Template** | Select **Custom**, **IKEv2 High Security**, or **IKEv2 Medium Security**. The setting items are different depending on the selected template. |
| **Internet Key Exchange (IKE)** | IKE is a communication protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec. To carry out encrypted communication for that time only, the encryption algorithm that is necessary for IPsec is determined and the encryption keys are shared. For IKE, the encryption keys are exchanged using the Diffie-Hellman key exchange method, and encrypted communication that is limited to IKE is carried out.<br>If you selected **Custom** in **Use Prefixed Template**, select **IKEv2**. |
| **Authentication Type** | • **Diffie-Hellman Group**<br>This key exchange method allows secret keys to be securely exchanged over an unprotected network. The Diffie-Hellman key exchange method uses a discrete logarithm problem, not the secret key, to send and receive open information that was generated using a random number and the secret key.<br>Select **Group1**, **Group2**, **Group5**, or **Group14**.<br>• **Encryption**<br>Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.<br>• **Hash**<br>Select **MD5**, **SHA1**, **SHA256**, **SHA384** or **SHA512**.<br>• **SA Lifetime**<br>Specify the IKE SA lifetime.<br>Type the time (seconds) and number of kilobytes (KByte). |
| **Encapsulating Security** | • **Protocol**<br>Select **ESP**.<br>ESP is a protocol for carrying out encrypted communication using IPsec. ESP encrypts the payload (communicated contents) and adds additional information. The IP packet comprises the header and the encrypted payload, which follows the header. In addition to the encrypted data, the IP packet also includes information regarding the encryption method and encryption key, the authentication data, and so on.<br>• **Encryption**<br>Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.<br>• **Hash**<br>Select **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.<br>• **SA Lifetime**<br>Specify the IKE SA lifetime.<br>Type the time (seconds) and number of kilobytes (KByte).<br>• **Encapsulation Mode**<br>Select **Transport** or **Tunnel**.<br>• **Remote Router IP-Address**<br>Type the IP address (IPv4 or IPv6) of the remote router. Enter this information only when the **Tunnel** mode is selected. |

| Option | Description |
| --- | --- |
| | SA (Security Association) is an encrypted communication method using IPsec or IPv6 that exchanges and shares information, such as the encryption method and encryption key, in order to establish a secure communication channel before communication begins. SA may also refer to a virtual encrypted communication channel that has been established. The SA used for IPsec establishes the encryption method, exchanges the keys, and carries out mutual authentication according to the IKE (Internet Key Exchange) standard procedure. In addition, the SA is updated periodically. |
| **Perfect Forward Secrecy (PFS)** | PFS does not derive keys from previous keys that were used to encrypt messages. In addition, if a key that is used to encrypt a message was derived from a parent key, that parent key is not used to derive other keys. Therefore, even if a key is compromised, the damage will be limited only to the messages that were encrypted using that key.<br>Select **Enabled** or **Disabled**. |
| **Authentication Method** | Select the authentication method. Select **Pre-Shared Key**, **Certificates**, **EAP - MD5**, or **EAP - MS-CHAPv2**.<br>EAP is an authentication protocol that is an extension of PPP. By using EAP with IEEE802.1x, a different key is used for user authentication during each session.<br>The following settings are necessary only when **EAP - MD5** or **EAP - MS-CHAPv2** is selected in **Authentication Method**:<br>• **Mode**<br>Select **Server-Mode** or **Client-Mode**.<br>• **Certificate**<br>Select the certificate.<br>• **User Name**<br>Type the user name (up to 32 characters).<br>• **Password**<br>Type the password (up to 32 characters). The password must be entered two times for confirmation. |
| **Pre-Shared Key** | When encrypting communication, the encryption key is exchanged and shared beforehand using another channel.<br>If you selected **Pre-Shared Key** for the **Authentication Method**, type the **Pre-Shared Key** (up to 32 characters).<br>• **Local/ID Type/ID**<br>Select the sender's ID type, and then type the ID.<br>Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.<br>If you select **Certificate**, type the common name of the certificate in the **ID** field.<br>• **Remote/ID Type/ID**<br>Select the recipient's ID type, and then type the ID.<br>Select **IPv4 Address**, **IPv6 Address**, **FQDN**, **E-mail Address**, or **Certificate** for the type.<br>If you select **Certificate**, type the common name of the certificate in the **ID** field. |
| **Certificate** | If you selected **Certificates** for **Authentication Method**, select the certificate. |

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

## Related Information

- Configure an IPsec Template Using Web Based Management

# Manual Settings for an IPsec Template

| Option | Description |
|---|---|
| **Template Name** | Type a name for the template (up to 16 characters). |
| **Use Prefixed Template** | Select **Custom**. |
| **Internet Key Exchange (IKE)** | IKE is a communication protocol that is used to exchange encryption keys in order to carry out encrypted communication using IPsec. To carry out encrypted communication for that time only, the encryption algorithm that is necessary for IPsec is determined and the encryption keys are shared. For IKE, the encryption keys are exchanged using the Diffie-Hellman key exchange method, and encrypted communication that is limited to IKE is carried out.<br>Select **Manual**. |
| **Authentication Key (ESP, AH)** | Type the **In/Out** values.<br>These settings are necessary when **Custom** is selected for **Use Prefixed Template**, **Manual** is selected for **Internet Key Exchange (IKE)**, and a setting other than **None** is selected for **Hash** for **Encapsulating Security** section.<br>The number of characters you can set differs depending on the setting you chose for **Hash** in the **Encapsulating Security** section.<br>If the length of the specified authentication key is different than the selected hash algorithm, an error will occur.<br>• **MD5**: 128 bits (16 bytes)<br>• **SHA1**: 160 bits (20 bytes)<br>• **SHA256**: 256 bits (32 bytes)<br>• **SHA384**: 384 bits (48 bytes)<br>• **SHA512**: 512 bits (64 bytes)<br>When you specify the key in ASCII Code, enclose the characters in double quotation marks ("). |
| **Code key (ESP)** | Type the **In/Out** values.<br>These settings are necessary when **Custom** is selected for **Use Prefixed Template**, **Manual** is selected for **Internet Key Exchange (IKE)**, and **ESP** is selected for **Protocol** in **Encapsulating Security**.<br>The number of characters you can set differs depending on the setting you chose for **Encryption** in the **Encapsulating Security** section.<br>If the length of the specified code key is different than the selected encryption algorithm, an error will occur.<br>• **DES**: 64 bits (8 bytes)<br>• **3DES**: 192 bits (24 bytes)<br>• **AES-CBC 128**: 128 bits (16 bytes)<br>• **AES-CBC 256**: 256 bits (32 bytes)<br>When you specify the key in ASCII Code, enclose the characters in double quotation marks ("). |
| **SPI** | These parameters are used to identify security information. Generally, a host has multiple Security Associations (SAs) for several types of IPsec communication. Therefore, it is necessary to identify the applicable SA when an IPsec packet is received. The SPI parameter, which identifies the SA, is included in the Authentication Header (AH) and Encapsulating Security Payload (ESP) header. |

| Option | Description |
|---|---|
| | These settings are necessary when **Custom** is selected for **Use Prefixed Template**, and **Manual** is selected for **Internet Key Exchange (IKE)**.<br>Enter the **In/Out** values. (3-10 characters) |
| **Encapsulating Security** | • **Protocol**<br>Select **ESP** or **AH**.<br>- ESP is a protocol for carrying out encrypted communication using IPsec. ESP encrypts the payload (communicated contents) and adds additional information. The IP packet comprises the header and the encrypted payload, which follows the header. In addition to the encrypted data, the IP packet also includes information regarding the encryption method and encryption key, the authentication data, and so on.<br>- AH is part of the IPsec protocol that authenticates the sender and prevents manipulation of the data (ensures the completeness of the data). In the IP packet, the data is inserted immediately after the header. In addition, the packets include hash values, which are calculated using an equation from the communicated contents, secret key, and so on, in order to prevent the falsification of the sender and manipulation of the data. Unlike ESP, the communicated contents are not encrypted, and the data is sent and received as plain text.<br>• **Encryption (Not available for the AH option.)**<br>Select **DES**, **3DES**, **AES-CBC 128**, or **AES-CBC 256**.<br>• **Hash**<br>Select **None**, **MD5**, **SHA1**, **SHA256**, **SHA384**, or **SHA512**.<br>**None** can be selected only when **ESP** is selected for **Protocol**.<br>• **SA Lifetime**<br>Specify the IKE SA lifetime.<br>Type the time (seconds) and number of kilobytes (KByte).<br>• **Encapsulation Mode**<br>Select **Transport** or **Tunnel**.<br>• **Remote Router IP-Address**<br>Type the IP address (IPv4 or IPv6) of the remote router. Enter this information only when the **Tunnel** mode is selected.<br>SA (Security Association) is an encrypted communication method using IPsec or IPv6 that exchanges and shares information, such as the encryption method and encryption key, in order to establish a secure communication channel before communication begins. SA may also refer to a virtual encrypted communication channel that has been established. The SA used for IPsec establishes the encryption method, exchanges the keys, and carries out mutual authentication according to the IKE (Internet Key Exchange) standard procedure. In addition, the SA is updated periodically. |

## Related Information

- Configure an IPsec Template Using Web Based Management

# 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

# User Authentication

- Use Active Directory Authentication
- Use LDAP Authentication
- Use Secure Function Lock 3.0

# Use Active Directory Authentication

# Introduction to Active Directory Authentication

Active Directory Authentication restricts the use of your machine. If Active Directory Authentication is enabled, the machine's control panel will be locked. You cannot change the machine's settings until you enter a User ID and password.

Active Directory Authentication offers the following features:

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

- Stores incoming print data
- Stores incoming fax data
- Obtains the email address from the Active Directory server based on your User ID, when sending scanned data to an email server.

  To use this feature, select the **On** option for the **Get Mail Address** setting and **LDAP + kerberos** or **LDAP + NTLMv2** authentication method. Your email address will be set as the sender when the machine sends scanned data to an email server, or as the recipient if you want to send the scanned data to your email address.

When Active Directory Authentication is enabled, your machine stores all incoming fax data. After you log on, the machine prints the stored fax data.

You can change the Active Directory Authentication settings using Web Based Management.

## Related Information

- Use Active Directory Authentication

# Configure Active Directory Authentication Using Web Based Management

Active Directory authentication supports Kerberos authentication and NTLMv2 authentication. You must configure the SNTP protocol (network time server) and DNS server configuration for authentication.

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 **Administrator** > **User Restriction Function** or **Restriction Management**.

   If the left navigation bar is not visible, start navigating from ≡.
5. Select **Active Directory Authentication**.
6. Click **Submit**.
7. Click **Active Directory Authentication**.
8. Configure the following settings:

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

| Option | Description |
|---|---|
| **Storage Fax RX Data** | Select this option to store incoming fax data. You can print all incoming fax data after you log on to the machine. |
| **Remember User ID** | Select this option to save your User ID. |
| **Active Directory Server Address** | Type the IP address or the server name (for example: ad.example.com) of the Active Directory Server. |
| **Active Directory Domain Name** | Type the Active Directory domain name. |
| **Protocol & Authentication Method** | Select the protocol and authentication method. |
| **SSL/TLS** | Select the **SSL/TLS** option. |
| **LDAP Server Port** | Type the port number to connect the Active Directory server via LDAP (available only for **LDAP + kerberos** or **LDAP + NTLMv2** authentication method). |
| **LDAP Search Root** | Type the LDAP search root (available only for **LDAP + kerberos** or **LDAP + NTLMv2** authentication method). |

| Option | Description |
| --- | --- |
| **Get Mail Address** | Select this option to obtain logged on user's email address from the Active Directory server. (available only for **LDAP + kerberos** or **LDAP + NTLMv2** authentication method) |
| **Get User's Home Directory** | Select this option to obtain your home directory as the Scan to Network destination. (available only for **LDAP + kerberos** or **LDAP + NTLMv2** authentication method) |

9. Click **Submit**.

## Related Information

- Use Active Directory Authentication

# Log On to Change the Machine Settings Using the Machine's Control Panel (Active Directory Authentication)

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

1. On the machine's control panel, enter your User ID and Password to log on.
2. When authentication is successful, the machine's control panel is unlocked.

## Related Information

- Use Active Directory Authentication

# Use LDAP Authentication

- Introduction to LDAP Authentication
- Configure LDAP Authentication Using Web Based Management
- Log On to Change the Machine Settings Using the Machine's Control Panel (LDAP Authentication)

# Introduction to LDAP Authentication

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

LDAP Authentication offers the following features:

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

- Stores incoming print data
- Stores incoming fax data
- Obtains the email address from the LDAP server based on your User ID, when sending scanned data to an email server.

  To use this feature, select the **On** option for the **Get Mail Address** setting. Your email address will be set as the sender when the machine sends scanned data to an email server, or as the recipient if you want to send the scanned data to your email address.

When LDAP Authentication is enabled, your machine stores all incoming fax data. After you log on, the machine prints the stored fax data.

You can change the LDAP Authentication settings using Web Based Management.

## Related Information

- Use LDAP Authentication

# Configure LDAP Authentication Using Web Based Management

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 **Administrator** > **User Restriction Function** or **Restriction Management**.

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

5. Select **LDAP Authentication**.
6. Click **Submit**.
7. Click the **LDAP Authentication** menu.
8. Configure the following settings:

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

| Option | Description |
|---|---|
| **Storage Fax RX Data** | Select this option to store incoming fax data. You can print all incoming fax data after you log on to the machine. |
| **Remember User ID** | Select this option to save your User ID. |
| **LDAP Server Address** | Type the IP address or the server name (for example: ldap.example.com) of the LDAP server. |
| **SSL/TLS** | Select the **SSL/TLS** option to use LDAP over SSL/TLS. |
| **LDAP Server Port** | Type the LDAP server port number. |
| **LDAP Search Root** | Type the LDAP search root directory. |
| **Attribute of Name (Search Key)** | Type the attribute you want to use as a search key. |
| **Get Mail Address** | Select this option to obtain the logged user's email address from the LDAP server. |
| **Get User's Home Directory** | Select this option to obtain your home directory as the Scan to Network destination. |

9. Click **Submit**.

## Related Information

- Use LDAP Authentication

# Log On to Change the Machine Settings Using the Machine's Control Panel (LDAP Authentication)

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

1. On the machine's control panel, enter your User ID and Password to log on.
2. When authentication is successful, the machine's control panel is unlocked.

## Related Information

- Use LDAP Authentication

# Use Secure Function Lock 3.0

Secure Function Lock 3.0 increases security by restricting the functions available on your machine.

# Before Using Secure Function Lock 3.0

Use Secure Function Lock to configure passwords, set specific user page limits, and grant access to some or all of the functions listed here.

You can configure and change the following Secure Function Lock 3.0 settings using Web Based Management:

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

- **Print**
- **Copy**
- **Scan**
- **Fax**
- **Media**
- **Web Connect**
- **Apps**
- **Page Limits**
- **Page Counters**
- **Card ID (NFC ID)**

Touchscreen LCD models:

When Secure Function Lock is enabled, the machine automatically enters Public Mode and some of the machine's functions become restricted to authorized users only. To access the restricted machine functions, press  , select your user name, and enter your password.

## Related Information

- Use Secure Function Lock 3.0

# Configure Secure Function Lock 3.0 Using Web Based Management

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 **Administrator** > **User Restriction Function** or **Restriction Management**.

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

5. Select **Secure Function Lock**.
6. Click **Submit**.
7. Click the **Restricted Functions** menu.
8. Configure the settings to manage restrictions per user or per group.
9. Click **Submit**.
10. Click the **User List** menu.
11. Configure the User List.
12. Click **Submit**.

You can also change the user list lockout settings in the **Secure Function Lock** menu.

## Related Information

- Use Secure Function Lock 3.0

# Scan Using Secure Function Lock 3.0

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

## Setting Scan restrictions (for administrators)

Secure Function Lock 3.0 allows an 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 the **Scan** checkbox selected will be able to scan.

## Using the Scan feature (for restricted users)

- To scan using the machine's control panel:

  Restricted users must enter their passwords on the machine's control panel to access Scan mode.
- To scan from a computer:

  Restricted users must enter their passwords on the machine's control panel before scanning from their computers. If the password is not entered on the machine's control panel, an error message will appear on the user's computer.

If the machine supports IC card authentication, restricted users can also access Scan mode by touching the NFC symbol on the machine's control panel with their registered IC cards.

## Related Information

- Use Secure Function Lock 3.0

# Configure Public Mode for Secure Function Lock 3.0

Use the Secure Function Lock screen to set up Public Mode, which limits the functions available to public users. Public users will not need to enter a password to access the features made available through Public Mode settings.

Public Mode includes print jobs sent via Brother iPrint&Scan and Brother Mobile Connect.

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 **Administrator** > **User Restriction Function** or **Restriction Management**.

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

5. Select **Secure Function Lock**.
6. Click **Submit**.
7. Click the **Restricted Functions** menu.
8. In the **Public Mode** row, select a checkbox to allow, or clear a checkbox to restrict, the function listed.
9. Click **Submit**.

## Related Information

- Use Secure Function Lock 3.0

# Configure Personal Home Screen Settings Using Web Based Management

As an Administrator, you can specify which tabs users can view on their personal home screens. These tabs provide quick access to users' favorite shortcuts, which they can assign to their personal home screen tabs from the machine's control panel.

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

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 **Administrator** > **User Restriction Function** or **Restriction Management**.

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

5. Select **Secure Function Lock**.
6. In the **Tab Settings** field, select **Personal** for the tab names you want to use as your personal home screen.
7. Click **Submit**.
8. Click the **Restricted Functions** menu.
9. Configure the settings to manage the restrictions per user or group.
10. Click **Submit**.
11. Click the **User List** menu.
12. Configure the User List.
13. Select **User List / Restricted Functions** from the drop-down list for each user.
14. Select the tab name from the **Home Screen** drop-down list for each user.
15. Click **Submit**.

## Related Information

- Use Secure Function Lock 3.0

# Additional Secure Function Lock 3.0 Features

Configure the following features in the Secure Function Lock screen:

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

**All Counter Reset**

Click **All Counter Reset**, in the **Page Counters** column, to reset the page counter.

**Export to CSV file**

Click **Export to CSV file**, to export the current and last page counter including **User List / Restricted Functions** information as a CSV file.

**Card ID (NFC ID)**

Click the **User List** menu, and then type a user's Card ID in the **Card ID (NFC ID)** field. You can use your IC card for authentication.

**Output**

When the Mailbox unit is installed on your machine, select the output tray for each user from the drop-down list.

**Last Counter Record**

Click **Last Counter Record** if you want the machine to retain the page count after the counter has been reset.

**Counter Auto Reset**

Click **Counter Auto Reset** to configure the time interval you want between page counter reset. Choose a daily, weekly, or monthly interval.

## Related Information

- Use Secure Function Lock 3.0

# Register a new IC Card Using the Machine's Control Panel

You can register Integrated Circuit Cards (IC Cards) on your machine.

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

1. Touch the Near-Field Communication (NFC) symbol on the machine's control panel with a registered Integrated Circuit Card (IC Card).
2. Press your user ID on the LCD.
3. Press the Register Card button.
4. Touch a new IC Card to the NFC symbol.

   The new IC Card's number is then registered to the machine.
5. Press the OK button.

## Related Information

- Use Secure Function Lock 3.0

# Register an External IC Card Reader

When you connect an external IC (Integrated Circuit) card reader, use Web Based Management to register the card reader. Your machine supports HID class driver supported external IC card readers.

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 **Administrator** > **External Card Reader**.

   If the left navigation bar is not visible, start navigating from ≡.
5. Enter the necessary information, and then click **Submit**.
6. Restart your Brother machine to activate the configuration.
7. Connect the card reader to your machine.
8. Touch the card to the card reader when using card authentication.

## Related Information

- Use Secure Function Lock 3.0

# Send or Receive an Email Securely

# Configure Email Sending or Receiving Using Web Based Management

- Receiving Email is available only for certain models.
- We recommend using Web Based Management to configure secured email sending with user authentication, or email sending and receiving using SSL/TLS (supported models only).

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. In the **POP3/IMAP4/SMTP Client** field, click **Advanced Settings** and make sure the status of **POP3/IMAP4/SMTP Client** is **Enabled**.

- Available protocols may differ, depending on your machine.
- If the **Authentication Method** selection screen appears, select your authentication method, and then follow the on-screen instructions.

6. Configure the **POP3/IMAP4/SMTP Client** settings.
   - Confirm that the email settings are correct after configuration by sending a test email.
   - If you do not know the POP3/IMAP4/SMTP server settings, contact your network administrator or Internet Service Provider (ISP).
7. When finished, click **Submit**.

   The **Test Send/Receive E-mail Configuration** dialog box appears.
8. Follow the instructions in the dialog box to test the current settings.

## Related Information

- Send or Receive an Email Securely

**Related Topics:**

- Send or Receive an Email Securely Using SSL/TLS

# Send an Email with User Authentication

Your machine sends emails via an email server that requires user authentication. This method prevents unauthorized users from accessing the email server.

You can send email notification, email reports, and I-Fax (available only for certain models) using user authentication.

- Available protocols may differ, depending on your machine.
- We recommend using Web Based Management to configure the SMTP authentication.

## Email Server Settings

You must configure your machine's SMTP authentication method to match the method used by your email server. For details about your email server settings, contact your network administrator or Internet Service Provider (ISP).

To enable SMTP server authentication using Web Based Management, select your authentication method under **Server Authentication Method** on the **POP3/IMAP4/SMTP Client** screen.

## Related Information

- Send or Receive an Email Securely

# Send or Receive an Email Securely Using SSL/TLS

Your machine supports SSL/TLS communication methods. To use an email server that is using SSL/TLS communication, you must configure the following settings.

- Receiving Email is available only for certain models.
- We recommend using Web Based Management to configure SSL/TLS.

## Verify Server Certificate

Under **SSL/TLS**, if you choose **SSL** or **TLS**, the **Verify Server Certificate** checkbox will be selected automatically.

- 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 if importing a CA certificate is necessary.
- If you do not need to verify the server certificate, clear the **Verify Server Certificate** checkbox.

## Port Number

If you select **SSL**, or **TLS**, the **Port** value will be changed to match the protocol. To change the port number manually, type the port number after you select **SSL/TLS** settings.

You must configure your machine's communication method to match the method used by your email server. For details about your email server settings, contact your network administrator or your ISP.

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

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

| | | |
|---|---|---|
| SMTP | **Port** | 587 |
| | **Server Authentication Method** | **SMTP-AUTH** |
| | **SSL/TLS** | **TLS** |
| POP3 | **Port** | 995 |
| | **SSL/TLS** | **SSL** |
| IMAP4 | **Port** | 993 |
| | **SSL/TLS** | **SSL** |

## Related Information

- Send or Receive an Email Securely

**Related Topics:**

- Configure Email Sending or Receiving Using Web Based Management
- Configure Certificates for Device Security

# Store Print Log to Network

# Store Print Log to Network Overview

The Store Print Log to Network feature allows you to save the print log file from your machine to a network server using the Common Internet File System (CIFS) protocol. 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. CIFS is a 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:

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

- Print jobs from your computer
- USB Direct Print
- Copy
- Received Fax
- Web Connect Print

- 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.
- You can set the file type to TXT or CSV when storing a file to the server.

## Related Information

- Store Print Log to Network

# Configure the Store Print Log to Network Settings Using Web Based Management

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 **Administrator** > **Store Print Log to Network**.

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

5. In the **Print Log** field, click **On**.
6. Configure the following settings:

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

| Option | Description |
|---|---|
| **Network Folder Path** | Type the destination folder where your print log will be stored on the CIFS server (for example: \\ComputerName\SharedFolder). |
| **File Name** | Type the file name you want to use for the print log (up to 32 characters). |
| **File Type** | Select the **TXT** or **CSV** option for the print log file type. |
| **Time Source for Log** | Select the time source for the print log. |
| **Auth. Method** | Select the authentication method required for access to the CIFS server: **Auto**, **Kerberos**, or **NTLMv2**. Kerberos is an authentication protocol which allows devices or individuals to securely prove their identity to network servers using a single sign-on. NTLMv2 is the authentication method used by Windows to log into servers.<br>• **Auto**: If you select **Auto**, NTLMv2 will be used to the authentication method.<br>• **Kerberos**: Select the **Kerberos** option to use Kerberos authentication only.<br>• **NTLMv2**: Select the **NTLMv2** option to use NTLMv2 authentication only.<br>• For the **Kerberos** and **NTLMv2** authentication, you must also configure the **Date&Time** settings or the SNTP protocol (network time server) and DNS server.<br>• You can also configure the Date & Time settings from the machine's control panel. |
| **Username** | Type the user name for the authentication (up to 96 characters).<br>If the user name is part of a domain, enter the user name in one of the following styles: user@domain or domain\user. |

| Option | Description |
| --- | --- |
| **Password** | Type the password for the authentication (up to 32 characters). |
| **Kerberos Server Address** (if needed) | Type the Key Distribution Center (KDC) host address (for example: kerberos.example.com; up to 64 characters) or the IP address (for example: 192.168.56.189). |
| **Error Detection Setting** | Choose what action should be taken when the print log cannot be stored to the server due to a network error. |

7. In the **Connection Status** field, confirm the last log status.

You can also confirm the error status on the LCD of your machine.

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

## Related Information

- Store Print Log to Network

# Use the Store Print Log to Network's Error Detection Setting

Use Error Detection Settings to determine the action that is taken when the print log cannot be stored to the server due to a network error.

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 **Administrator** > **Store Print Log to Network**.

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

5. In the **Error Detection Setting** section, select the **Cancel Print** or **Ignore Log & Print** option.

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

| Option | Description |
|---|---|
| **Cancel Print** | If you select the **Cancel Print** option, the print jobs are canceled when the print log cannot be stored to the server.<br><br>Even if you select the **Cancel Print** option, your machine will print a received fax. |
| **Ignore Log & Print** | If you select the **Ignore Log & Print** option, the machine prints the documentation even if the print log cannot be stored to the server.<br>When the Store Print Log function has recovered, the print log is recorded as follows:<br><br>`Id, Type, Job Name, User Name, Date, Time, Print Pages`<br>`1, Print(xxxxxxx), "Document01.doc", "user01", 03/03/20xx, 14:01:32, 52`<br>`2, Print(xxxxxxx), "Document02.doc", "user01", 03/03/20xx, 14:45:30, ?` (a)<br>`3, <Error>, ?, ?, ?, ?, ?` (b)<br>`4, Print(xxxxxxx), "Report01.xls", "user02", 03/03/20xx, 19:30:40, 4`<br><br>a. If the print log cannot be stored at the end of printing, the number of printed pages will not be recorded.<br>b. 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 error is reflected in the print log. |

6. Click **Submit** to display the **Test Print Log to Network** page.

   To test your settings, click **Yes** and then go to the next step.

   To skip the test, click **No**. Your settings will be submitted automatically.
7. The machine will test your settings.
8. If your settings are accepted, **Test OK** appears on the screen.

   If **Test Error** appears, check all settings, and then click **Submit** to display the Test page again.

## Related Information

- Store Print Log to Network

# Use Store Print Log to Network with Secure Function Lock 3.0

When Secure Function Lock 3.0 is active, the names of the registered users for copy, Fax RX, Web Connect Print, and USB Direct Print are recorded in the Store Print Log to Network report. When the Active Directory Authentication is enabled, the user name is recorded in the Store Print Log to Network report:

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

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

## Related Information

- Store Print Log to Network

brother

Brother Earth

www.brotherearth.com

ENG
Version 0