安全功能说明书

目录

简介

提示定义

本使用说明书中使用以下符号和惯例：

重要事项	重要事项 图标表示可能导致财产损失或设备损坏的潜在危险。
提示	提示图标指定了操作环境、安装条件或特殊使用条件。
	“提示”图标指示有用的提示和补充信息。
粗体	粗体字表示设备的操作面板或计算机屏幕上的按键/按钮。
斜体	斜体字强调应当注意的要点或提示您参考相关主题。

相关信息

- 简介

商标

Adobe® 和 Reader® 是 Adobe Systems Incorporated 在美国和/或其他国家的注册商标或商标。

本手册中提及的软件名称都有一份软件许可协议，此协议指明了其相应的所有者。

Brother 产品、相关文档和任何其他资料中出现的任何公司的任何品牌名称和产品名称都是其相应公司的商标或注册商标。

相关信息

- 简介

版权

相关信息

- 简介

使用网络安全功能前

本设备采用了目前最新的网络安全与加密协议。这些网络功能可以应用于网络安全总计划中，有助于保护数据并防止未经授权用户访问该设备。

我们建议您禁用 FTP 和 TFTP 协议。使用这些协议访问本设备不安全。

相关信息

- 简介
  - 禁用非必要协议

禁用非必要协议

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **网络** > **协议**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 取消选中非必要协议的复选框进行禁用。
6. 点击**提交**。
7. 重新启动本 Brother 设备以激活配置。

相关信息

- 使用网络安全功能前

网络安全

- 配置设备安全性证书
- 使用 SSL/TLS
- 使用 SNMPv3
- 使用 IPsec
- 使用 IEEE 802.1x 身份验证保护您的网络

配置设备安全性证书

必须配置证书才可以使用 SSL/TLS 安全地管理网络设备。必须使用网络基本管理配置证书。

- 安全证书功能概述
- 如何创建和安装证书
- 创建自我认定证书
- 创建证书签订请求（CSR）并安装由证书授权中心（CA）颁发的证书
- 导入和导出证书和私人密钥
- 导入和导出 CA 证书

安全证书功能概述

本设备支持使用多个安全证书进行安全验证和设备通信。本设备允许使用以下安全证书功能：

支持的功能、选项和设置可能会因型号而有所不同。

- SSL/TLS 信息互通
- IEEE 802.1x 验证
- IPsec

本设备支持以下证书：

- 预安装证书

  本设备有预安装的自我认定证书。此证书让您可以使用 SSL/TLS 通信，而无需创建或安装其他证书。

预安装的自我认定证书可保护您的通信，保护程度达到特定级别。我们建议您使用由受信任的机构颁发的证书，以提高安全性。

- 自我认定证书

  本打印服务器可颁发自我认定证书。使用该证书时，您可以轻松使用 SSL/TLS 通信，而无需创建或安装其他 CA 证书。
- 证书授权中心（CA）颁发的证书

  有两种方法安装 CA 认证证书。若已经存在 CA 认证证书，或者希望使用外部 CA 认证证书：

  - 当使用打印服务器的证书签订请求（CSR）时。
  - 当导入证书和机密键时。
- 证书授权中心（CA）证书

  若要使用可识别 CA 机构并拥有其机密密钥的 CA 证书，则配置网络安全功能前必须先导入由 CA 颁发的 CA 证书。

- 如果您要使用 SSL/TLS 通信，我们建议您在使用之前先联系系统管理员。
- 当您将打印服务器重置为默认出厂设置时，已安装的证书和机密键将被删除。如果您希望重置打印服务器后仍然保留原有的证书和机密键，那么请在重置打印服务器之前先将其导出，然后重新安装。

相关信息

- 配置设备安全性证书

相关主题：

- 使用网络基本管理（Web 浏览器）为您的网络配置 IEEE 802.1x 身份验证

如何创建和安装证书

选择安全证书时有两个选项：使用自我认定证书或使用证书授权中心（CA）颁发的证书。

选项 1

自我认定证书

1. 使用网络基本管理创建自我认定证书。
2. 在计算机上安装自我认定证书。

选项 2

CA 证书

1. 使用网络基本管理创建证书签订请求（CSR）。
2. 使用网络基本管理在本 Brother 设备中安装由 CA 机构（证书授权中心）颁发的证书。
3. 在计算机上安装证书。

相关信息

- 配置设备安全性证书

创建自我认定证书

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击**创建自我认定证书**。
6. 输入**名称**和**有效日期**。
   - **名称**需少于 64 个字节。当通过 SSL/TLS 通信使用本设备时，请输入标识符，例如 IP 地址、节点名称或域名。在默认状态下显示节点名称。
   - 如果您使用 IPPS 或 HTTPS 协议并在 URL 中输入了与用于自我认定证书的**名称**不同的名称，将显示警告信息。
7. 从**公钥算法**下拉列表中选择设置。
8. 从**摘要算法**下拉列表中选择设置。
9. 点击**提交**。

相关信息

- 配置设备安全性证书

创建证书签订请求（CSR）并安装由证书授权中心（CA）颁发的证书

如果您已拥有外部证书授权中心（CA）认证证书，您可以通过导入和导出证书和机密键将它们保存在设备中并进行管理。如果您没有外部 CA 认证证书，创建证书签订请求（CSR），将其发送到 CA 进行验证，然后将返回证书安装到设备上。

- 创建证书签订请求（CSR）
- 将证书安装到本设备上

创建证书签订请求（CSR）

证书签订请求（CSR）是向证书授权中心（CA）发送的一个请求，用于验证证书中所包含的凭据。

我们建议您在创建 CSR 之前，在您的计算机中安装由 CA 认证的根证书。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 点击**创建 CSR**。
6. 输入**名称**(必填)，并添加有关**组织**（可选）的其他信息。

- 要求输入公司详细信息，以便 CA 能够确认您的身份，并向外部人员核实。
- **名称**必须少于 64 个字节。当通过 SSL/TLS 通信使用本设备时，请输入标识符，例如 IP 地址、节点名称或域名。在默认状态下显示节点名称。**名称**为必填项。
- 如果您在 URL 中输入的名称与证书使用的通用名称不同，将显示警告信息。
- **组织**、**组织单位**、**城市/位置**和**自治区/省份**的长度必须少于 64 个字节。
- **国家/区域**应是两个字符的 ISO 3166 国家代码。
- 如果您正在配置 X.509v3 证书扩展名，请选中**配置扩展分区**复选框，然后选择**自动（注册 IPv4）**或**手动**。

7. 从**公钥算法**下拉列表中选择设置。
8. 从**摘要算法**下拉列表中选择设置。
9. 点击**提交**。
   屏幕上显示 CSR。将 CSR 另存为文件，或将其复制和粘贴到证书授权中心提供的在线 CSR 表格中。
10. 点击**保存**。

- 关于将 CSR 发送到 CA 认证的方法，请遵循 CA 认证政策。
- 如果您正在使用 Windows Server 的企业根 CA，我们建议您使用网络服务器作为证书模板来安全创建客户端证书。如果您正在创建带 EAP-TLS 验证的 IEEE 802.1x 环境客户端证书，我们建议您使用用户作为证书模板。

相关信息

- 创建证书签订请求（CSR）并安装由证书授权中心（CA）颁发的证书

将证书安装到本设备上

当您接收到证书授权中心（CA）颁发的证书时，请遵循以下步骤将证书安装在打印服务器中。

本设备中只能安装因本设备的证书签订请求（CSR）授予的证书。需要创建新的 CSR 时，创建前请确保证书已安装。请先将证书安装在设备中，然后再创建其他 CSR。否则，在安装前创建的 CSR 将无效。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击**安装证书**。
6. 操作到包含 CA 授予的证书的文件，然后点击**提交**。
   证书创建成功，并保存在本设备的内存中。

若要使用 SSL/TLS 信息互通，必须在您的计算机中也装 CA 认证的根证书。联系您的网络管理员。

相关信息

- 创建证书签订请求（CSR）并安装由证书授权中心（CA）颁发的证书

导入和导出证书和私人密钥

通过导入和导出证书和机密键将它们存储到设备中并进行管理。

- 导入证书和机密键
- 导出证书和机密键

导入证书和机密键

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击**输入证书及机密键**。
6. 浏览并选择您想导入的目标文件。
7. 如果文件加密，请输入密码，然后点击**提交**。

证书和机密键已导入至您的设备。

相关信息

- 导入和导出证书和私人密钥

导出证书和机密键

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击随**证书列表**显示的**导出**。
6. 如果您想加密文件，请输入密码。
   如果使用空白密码，则输出不会加密。
7. 重新输入密码以进行确认，然后点击**提交**。
8. 点击**保存**。

证书和机密键已导出至您的计算机。

也可将证书导入计算机。

相关信息

- 导入和导出证书和私人密钥

导入和导出 CA 证书

您可以在本 Brother 设备上导入、导出并存储 CA 证书。

- 导入 CA 证书
- 导出 CA 证书

导入 CA 证书

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **CA 证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击**导入 CA 证书**。
6. 转到您想导入的文件。
7. 点击**提交**。

相关信息

- 导入和导出 CA 证书

导出 CA 证书

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **CA 证书**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 选择您想导出的证书，然后点击**导出**。
6. 点击**提交**。

相关信息

- 导入和导出 CA 证书

使用 SSL/TLS

- 使用 SSL/TLS 安全地管理网络设备
- 使用 SSL/TLS 安全打印文档
- 使用 SSL/TLS 安全发送或接收电子邮件

使用 SSL/TLS 安全地管理网络设备

配置 SSL/TLS 和可用协议证书

使用 SSL/TLS 通信之前，请先通过网络基本管理在本设备上配置一个证书。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**网络** > **网络** > **协议**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 点击 **HTTP 服务器设置**。
6. 从**选择证书**下拉列表中选择您想配置的证书。
7. 点击**提交**。
8. 点击**是**重启您的打印服务器。

相关信息

- 使用 SSL/TLS 安全地管理网络设备

相关主题：

- 使用 SSL/TLS 安全打印文档

使用 SSL/TLS 访问网络基本管理

若要安全管理网络设备，您必须通过安全协议来使用管理实用程序。

- 要使用 HTTPS 协议，必须在设备上启用 HTTPS。默认启用 HTTPS 协议。
- 可使用网络基本管理屏幕更改 HTTPS 协议设置。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 此时，您可以通过 HTTPS 协议使用本设备。

相关信息

- 使用 SSL/TLS 安全地管理网络设备

安装自我认定证书（适用于 Windows 管理员用户）

- 以下步骤适用于 Microsoft Edge。如果您使用其他网络浏览器，请参阅该网络浏览器的手册或在线帮助了解如何安装证书。
- 请确保您已使用网络基本管理创建您的自我认定证书。

1. 右击 **Microsoft Edge** 图标，然后点击**以管理员身份运行**。
   出现**用户帐户控制**屏幕时，点击**是**。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如果您所用连接不是专用连接，点击**高级**按钮，然后转到相应网页。
4. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

5. 在左侧导航栏中，点击**网络** > **安全** > **证书**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

6. 点击**导出**。
7. 若要加密输出文件，在**输入密码**字段中输入密码。如果**输入密码**字段为空白，将不加密输出文件。
8. 在**再次输入密码**字段中再次输入密码，然后点击**提交**。
9. 点击打开已下载的文件。
10. 显示**证书导入向导**时，点击**下一步**。
11. 点击**下一步**。
12. 如有需要，输入密码，然后点击**下一步**。
13. 选择**将所有的证书放入下列存储**，然后点击**浏览…**。
14. 选择**受信任的根证书颁发机构**，然后点击**确定**。
15. 点击**下一步**。
16. 点击**完成**。
17. 如果指纹（拇指纹）正确，点击**是**。
18. 点击**确定**。

相关信息

- 使用 SSL/TLS 安全地管理网络设备

使用 SSL/TLS 安全打印文档

- 使用 IPPS 打印文档
- 配置 SSL/TLS 和可用协议证书
- 配置设备安全性证书

使用 IPPS 打印文档

若要使用 IPP 协议安全打印文档，请使用 IPPS 协议。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **网络** > **协议**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 确认已选中 **IPP** 复选框。

   如果未选中 **IPP** 复选框，选中 **IPP** 复选框，然后点击**提交**。
   重启设备以激活配置。
   设备重新启动后，请返回到设备网页，输入密码，然后在左侧导航栏中点击**网络** > **网络** > **协议**。
6. 点击 **HTTP 服务器设置**。
7. 在 **IPP** 区域选中 **HTTPS(端口 443)** 复选框，然后点击**提交**。
8. 重启设备以激活配置。

使用 IPPS 通信时，不能阻止未经授权的用户访问打印服务器。

相关信息

- 使用 SSL/TLS 安全打印文档

使用 SNMPv3

- 使用 SNMPv3 安全管理网络设备

使用 SNMPv3 安全管理网络设备

简单网络管理协议版本 3（SNMPv3）提供了用户认证和数据加密，可安全地管理网络设备。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入 "https://Common Name"（其中，"Common Name" 为您签发证书的通用名称；可能是 IP 地址、节点名称或域名）。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**网络** > **网络** > **协议**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 确保已启用 **SNMP** 设置，然后点击**高级设置**。
6. 配置 SNMPv1/v2c 模式设置。

选项	说明
SNMP v1/v2c 读写访问	打印服务器使用 SNMP 协议版本 1 和版本 2c。您可以在此模式下使用本设备的所有应用程序。但是，由于未进行用户验证且数据也未加密，所以这种模式不安全。
SNMP v1/v2c 只读访问权限	打印服务器使用 SNMP 协议版本 1 和版本 2c 的只读访问权限。
已禁用	禁用 SNMP 协议版本 1 和版本 2c。 使用 SNMPv1/v2c 的所有应用程序都将受到限制。若要允许使用 SNMPv1/v2c 应用程序，请使用 **SNMP v1/v2c 只读访问权限**或 **SNMP v1/v2c 读写访问**模式。

7. 配置 SNMPv3 模式设置。

选项	说明
已启用	打印服务器使用 SNMP 协议版本 3。为了安全地管理打印服务器，请使用 SNMPv3 模式。
已禁用	禁用 SNMP 协议版本 3。 使用 SNMPv3 的所有应用程序都将受到限制。若要允许使用 SNMPv3 应用程序，请使用 SNMPv3 模式。

8. 点击**提交**。

如果本设备上显示协议设置选项，请选择所需的选项。

9. 重启设备以激活配置。

相关信息

- 使用 SNMPv3

使用 IPsec

IPsec 简介

IPsec（Internet Protocol Security，Inernet 协议安全性）是一种安全协议，它采用可选的 Internet 协议功能来防止数据处理，并在以 IP 数据包的形式传输数据时确保机密性。IPsec 对通过网络传输的数据进行加密，例如从计算机发送到打印机的打印数据。因为数据是在网络层上加密的，因此采用更高级别协议的应用程序也可使用 IPsec，虽然用户并没有意识到它的使用。

IPsec 支持下列功能：

- IPsec 传输

  根据 IPsec 设置条件，连接到网络的计算机会采用 IPsec 与指定的设备相互发送和接收数据。设备开始使用 IPsec 进行通信时，先使用因特网密钥交换（IKE）交换密钥，然后使用密钥传输加密的数据。

  另外，IPsec 有两种操作模式：透明模式和隧道模式。透明模式主要用于设备之间的通信，隧道模式则用在诸如虚拟专用网络（VPN）之类的环境中。

  要进行 IPsec 传输，必须满足下列条件：
  - 可以使用 IPsec 进行通信的计算机已连接到网络。
  - 本设备已完成 IPsec 通信的相关配置。
  - 连接到本设备的计算机已完成 IPsec 连接的相关配置。

- IPsec 设置

  采用 IPsec 的连接所必需的设置。这些设置可使用网络基本管理来配置。

  若要配置 IPsec 设置，您必须使用连接到网络的计算机上的浏览器。

相关信息

- 使用 IPsec

使用网络基本管理配置 IPsec

IPsec 连接条件有两种**模板**类型：**地址**和 **IPsec**。您最多可以配置 10 个连接条件。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。

   例如：

   https://192.168.1.2

   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **IPsec**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 配置设置。

选项	说明
状态	启用或禁用 IPsec。
协商模式	将 IKE 阶段 1 选择为**协商模式**。IKE 协议用于交换加密密钥以使用 IPsec 执行加密通信。 在**主**模式下，处理速度慢，但安全性高。在**积极**模式下，处理速度比**主**模式快，但安全性较低。
所有非 IPsec 流量	选择要对非 IPsec 数据包采取的操作。 使用网络服务时，必须将**所有非 IPsec 流量**选择为**允许**。如果您选择**阻止**，将无法使用网络服务。
广播/多播旁路	选择**已启用**或**已禁用**。
协议旁路	根据需要，选中单个或多个选项的复选框。
规则	选中**已启用**复选框以激活模板。选择多个复选框时，如果所选复选框的设置冲突，则编号较小的复选框具有优先权。 点击相应的下拉列表选择用于 IPsec 连接条件的**地址模板**。若要添加**地址模板**，点击**添加模板**。 点击相应的下拉列表选择用于 IPsec 连接条件的 **IPsec 模板**。若要添加 **IPsec 模板**，点击**添加模板**。

6. 点击**提交**。

   如果必须重新启动设备才能激活新设置，将显示重新启动确认屏幕。

   如果您在**规则**表格中启用的模板中有空白项，将显示错误信息。确认您的选择，然后再次点击**提交**。

相关信息

- 使用 IPsec

相关主题：

- 配置设备安全性证书

使用网络基本管理配置 IPsec 地址模板

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**网络** > **安全** > **IPsec 地址模板**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 点击**删除**按钮删除**地址模板**。如果**地址模板**正在使用中，则无法删除。
6. 点击要创建的**地址模板**。出现 **IPsec 地址模板**。
7. 配置设置。

选项	说明
模板名称	输入模板的名称（最多 16 个字符）。
本地 IP 地址	• **IP 地址** 指定 IP 地址。从下拉列表中选择**所有 IPv4 地址**、**所有 IPv6 地址**、**所有连接本地 IPv6** 或**自定义**。 如果您从下拉列表中选择**自定义**，请在文本框中输入 IP 地址（IPv4 或 IPv6）。 • **IP 地址范围** 在文本框中输入 IP 地址范围的开始和结束 IP 地址。如果开始和结束 IP 地址未标准化为 IPv4 或 IPv6，或者结束 IP 地址比开始地址小，将会发生错误。 • **IP 地址 / 前缀** 使用 CIDR 表示法指定 IP 地址。 例如：192.168.1.1/24 对于 192.168.1.1，因为前缀以 24 位子网掩码（255.255.255.0）的形式指定，所以地址 192.168.1.### 有效。
远程 IP 地址	• **任何** 如果选择**任何**，将启用所有 IP 地址。 • **IP 地址** 在文本框中输入指定的 IP 地址（IPv4 或 IPv6）。 • **IP 地址范围** 输入 IP 地址范围的第一个和最后一个 IP 地址。如果第一个和最后一个 IP 地址未标准化为 IPv4 或 IPv6，或者最后一个 IP 地址比第一个地址小，将会发生错误。 • **IP 地址 / 前缀** 使用 CIDR 表示法指定 IP 地址。 例如：192.168.1.1/24 对于 192.168.1.1，因为前缀以 24 位子网掩码（255.255.255.0）的形式指定，所以地址 192.168.1.### 有效。

8. 点击**提交**。

更改当前所用模板的设置时，重新启动设备以激活配置。

相关信息

- 使用 IPsec

使用网络基本管理配置 IPsec 模板

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **安全** > **IPsec 模板**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 点击**删除**按钮删除 **IPsec 模板**。如果 **IPsec 模板**正在使用中，则无法删除。
6. 点击要创建的 **IPsec 模板**。出现 **IPsec 模板**屏幕。配置字段根据您选择的**请使用已加前缀的模板**和**因特网密钥交换（IKE）**设置而有所不同。
7. 在**模板名称**字段中，输入模板名称（最多 16 个字符）。
8. 如果在**请使用已加前缀的模板**下拉列表中选择了**自定义**，选择**因特网密钥交换（IKE）**选项，然后更改设置（如有需要）。
9. 点击**提交**。

相关信息

- 使用 IPsec
  - IPsec 模板的 IKEv1 设置
  - IPsec 模板的 IKEv2 设置
  - IPsec 模板的手动设置

IPsec 模板的 IKEv1 设置

选项	说明
模板名称	输入模板名称（最多 16 个字符）。
请使用已加前缀的模板	选择**自定义**、**IKEv1 高安全性**或 **IKEv1 中安全性**。设置项目根据所选模板不同而有所不同。
因特网密钥交换（IKE）	IKE 通信协议用于交换加密密钥以使用 IPsec 执行加密通信。为了仅在特定的时间执行加密通信，将确定 IPsec 所需的加密算法并共享加密密钥。对于 IKE，将使用 Diffie-Hellman 密钥交换方法交换加密密钥，并执行限制为 IKE 的加密通信。 如果在**请使用已加前缀的模板**中选择了**自定义**，选择 **IKEv1**。
验证类型	• **Diffie-Hellman 组** 这种密钥交换方法可通过未受保护的网络安全地交换保密密钥。Diffie-Hellman 密钥交换方法使用离散对数问题，而不是保密密钥，来发送和接收使用随机数字和保密密钥生成的打开信息。 选择**组 1**、**组 2**、**组 5** 或**组 14**。 • **加密** 选择 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **哈希算法** 选择 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA 生存期** 指定 IKE SA 生存期。 输入时间（秒数）和千字节数（KB）
压缩安全设置	• **协议** 选择 **ESP**、**AH** 或 **AH+ESP**。 - ESP 是使用 IPsec 执行加密通信的协议。ESP 对负载（通信内容）进行加密并添加其他信息。IP 数据包由标题和加密的有效负载组成，其中有效负载跟在标题后面。除了加密数据，IP 数据包还包括与加密方法和加密密钥、验证数据等有关的信息。 - AH 是 IPsec 协议的一部分，用于验证发送方和防止操纵数据（确保数据的完整性）。在 IP 数据包中，数据紧接在标题后。数据包中还包含使用等式从通信内容、保密密钥等计算得出的哈希值，以防止篡改发送方和操纵数据。与 ESP 不同，通信内容不加密，数据以普通文本的方式发送和接收。 • **加密(不适用于 AH 选项。)** 选择 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **哈希算法** 选择**无**、**MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 仅当为**协议**选择 **ESP** 时，才能选择**无**。 • **SA 生存期** 指定 IKE SA 生存期。 输入时间（秒数）和千字节数（KB） • **压缩模式** 选择**传输**或**隧道**。 • **远程路由器 IP 地址** 输入远程路由器的 IP 地址（IPv4 或 IPv6）。仅当选择**隧道**模式时，输入此信息。

选项	说明
	SA（安全关联）是一种加密通信方法，它使用 IPsec 或 IPv6 交换和共享加密方法和加密密钥等信息，以便在开始通信前建立安全的通信信道。SA 还指已建立的虚拟加密通信信道. 用于 IPsec 的 SA 根据 IKE（因特网密钥交换）标准步骤建立加密方法、交换密钥和执行相互认证。SA 还会定期更新。
完美向前保密（PFS）	PFS 不会从用于加密信息的先前密钥派生密钥。另外，如果用于加密信息的密钥是从父密钥派生的，则该父密钥不用于派生其他密钥。因此，即使密钥泄露，损坏范围也仅限于使用该密钥加密的信息。 选择**已启用**或**已禁用**。
身份验证方式	选择验证方法。选择**预共享密钥**或**证书**。
预共享密钥	对通信加密时，将使用其他信道事先交换和共享加密密钥。 如果**身份验证方式**设置为**预共享密钥**，输入**预共享密钥**（最多 32 个字符）。 • **本地/ID 类型/ID** 选择发送方的 ID 类型，然后输入 ID。 将类型设置为 **IPv4 地址**、**IPv6 地址**、**FQDN**、**电子邮件地址**或**证书**。 如果选择**证书**，在 **ID** 字段中输入证书的通用名称。 • **远程/ID 类型/ID** 选择接收方的 ID 类型，然后输入 ID。 将类型设置为 **IPv4 地址**、**IPv6 地址**、**FQDN**、**电子邮件地址**或**证书**。 如果选择**证书**，在 **ID** 字段中输入证书的通用名称。
证书	如果**身份验证方式**设置为**证书**，选择证书。 仅可选择使用网络基本管理安全配置屏幕的**证书**页面创建的证书。

相关信息

- 使用网络基本管理配置 IPsec 模板

IPsec 模板的 IKEv2 设置

选项	说明
模板名称	输入模板名称（最多 16 个字符）。
请使用已加前缀的模板	选择**自定义**、**IKEv2 高安全性**或 **IKEv2 中安全性**。设置项目根据所选模板不同而有所不同。
因特网密钥交换（IKE）	IKE 通信协议用于交换加密密钥以使用 IPsec 执行加密通信。为了仅在特定的时间执行加密通信，将确定 IPsec 所需的加密算法并共享加密密钥。对于 IKE，将使用 Diffie-Hellman 密钥交换方法交换加密密钥，并执行限制为 IKE 的加密通信。 如果在**请使用已加前缀的模板**中选择了**自定义**，选择 **IKEv2**。
验证类型	• **Diffie-Hellman 组** 这种密钥交换方法可通过未受保护的网络安全地交换保密密钥。Diffie-Hellman 密钥交换方法使用离散对数问题，而不是保密密钥，来发送和接收使用随机数字和保密密钥生成的打开信息。 选择**组 1**、**组 2**、**组 5** 或**组 14**。 • **加密** 选择 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **哈希算法** 选择 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA 生存期** 指定 IKE SA 生存期。 输入时间（秒数）和千字节数（KB）
压缩安全设置	• **协议** 选择 **ESP**。 ESP 是使用 IPsec 执行加密通信的协议。ESP 对负载（通信内容）进行加密并添加其他信息。IP 数据包由标题和加密的有效负载组成，其中有效负载跟在标题后面。除了加密数据，IP 数据包还包括与加密方法和加密密钥、验证数据等有关的信息。 • **加密** 选择 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **哈希算法** 选择 **MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 • **SA 生存期** 指定 IKE SA 生存期。 输入时间（秒数）和千字节数（KB） • **压缩模式** 选择**传输**或**隧道**。 • **远程路由器 IP 地址** 输入远程路由器的 IP 地址（IPv4 或 IPv6）。仅当选择**隧道**模式时，输入此信息。 SA（安全关联）是一种加密通信方法，它使用 IPsec 或 IPv6 交换和共享加密方法和加密密钥等信息，以便在开始通信前建立安全的通信信道。SA 还指已建立的虚拟加密通信信道. 用于 IPsec 的 SA 根据 IKE（因特网密钥交换）标准步骤建立加密方法、交换密钥和执行相互认证。SA 还会定期更新。
完美向前保密（PFS）	PFS 不会从用于加密信息的先前密钥派生密钥。另外，如果用于加密信息的密钥是从父密钥派生的，则该父密钥不用于派生其他密钥。因此，即使密钥泄露，损坏范围也仅限于使用该密钥加密的信息。 选择**已启用**或**已禁用**。

选项	说明
身份验证方式	选择验证方法。选择**预共享密钥**、**证书**、**EAP - MD5** 或 **EAP - MS-CHAPv2**。 EAP 是一种验证协议，它是 PPP 的扩展。同时使用 EAP 和 IEEE802.1x 时，每次会话中将使用不同的密钥进行用户验证。 仅当将**身份验证方式**设置为 **EAP - MD5** 或 **EAP - MS-CHAPv2** 时，才有必要进行以下设置： • **模式** 选择**服务器模式**或**客户端模式**。 • **证书** 选择证书。 • **用户名** 输入用户名（最多 32 个字符）。 • **密码** 输入密码（最多 32 个字符）。密码必须输入两次以进行确认。
预共享密钥	对通信加密时，将使用其他信道事先交换和共享加密密钥。 如果**身份验证方式**设置为**预共享密钥**，输入**预共享密钥**（最多 32 个字符）。 • **本地/ID 类型/ID** 选择发送方的 ID 类型，然后输入 ID。 将类型设置为 **IPv4 地址**、**IPv6 地址**、**FQDN**、**电子邮件地址**或**证书**。 如果选择**证书**，在 **ID** 字段中输入证书的通用名称。 • **远程/ID 类型/ID** 选择接收方的 ID 类型，然后输入 ID。 将类型设置为 **IPv4 地址**、**IPv6 地址**、**FQDN**、**电子邮件地址**或**证书**。 如果选择**证书**，在 **ID** 字段中输入证书的通用名称。
证书	如果**身份验证方式**设置为**证书**，选择证书。 仅可选择使用网络基本管理安全配置屏幕的**证书**页面创建的证书。

相关信息

- 使用网络基本管理配置 IPsec 模板

IPsec 模板的手动设置

选项	说明
模板名称	输入模板名称（最多 16 个字符）。
请使用已加前缀的模板	选择**自定义**。
因特网密钥交换（IKE）	IKE 通信协议用于交换加密密钥以使用 IPsec 执行加密通信。为了仅在特定的时间执行加密通信，将确定 IPsec 所需的加密算法并共享加密密钥。对于 IKE，将使用 Diffie-Hellman 密钥交换方法交换加密密钥，并执行限制为 IKE 的加密通信。 选择**手动**。
验证密钥（ESP，AH）	输入**输入/输出**值。 当**请使用已加前缀的模板**设置为**自定义**、**因特网密钥交换（IKE）** 设置为**手动**且**压缩安全设置**部分的**哈希算法**设置为除**无**以外的其他设置时，必须进行这些设置。 根据您在**压缩安全设置**部分选择的**哈希算法**设置，可设置的字符数会有所不同。 如果所指定验证密钥的长度与所选哈希算法的长度不同，则会发生错误。 • **MD5**：128 位（16 字节） • **SHA1**：160 位（20 字节） • **SHA256**：256 位（32 字节） • **SHA384**：384 位（48 字节） • **SHA512**：512 位（64 字节） 当您用 ASCII 码指定密钥时，请将字符扩在双引号（"）中。
代码密钥（ESP）	输入**输入/输出**值。 当**请使用已加前缀的模板**设置为**自定义**、**因特网密钥交换（IKE）** 设置为**手动**且**压缩安全设置**中的**协议**设置为 **ESP** 时，必须进行这些设置。 根据您在**压缩安全设置**部分选择的**加密**设置，可设置的字符数会有所不同。 如果所指定代码密钥的长度与所选加密算法的长度不同，则会发生错误。 • **DES**：64 位（8 字节） • **3DES**：192 位（24 字节） • **AES-CBC 128**：128 位（16 字节） • **AES-CBC 256**：256 位（32 字节） 当您用 ASCII 码指定密钥时，请将字符扩在双引号（"）中。
SPI	这些参数用来标识安全信息。一般而言，主机会有多个安全关联（SA）用于多种类型的 IPsec 通信。因此，当接收到 IPsec 数据包时，必须标识适用的 SA。用于标识 SA 的 SPI 参数包括在验证标头（AH）和压缩安全设置负载（ESP）标头中。 当**请使用已加前缀的模板**设置为**自定义**且 **因特网密钥交换（IKE）** 设置为**手动**时，必须进行这些设置。 输入**输入/输出**值。（3 ～ 10 个字符）
压缩安全设置	• **协议** 选择 **ESP** 或 **AH**。

选项	说明
	- ESP 是使用 IPsec 执行加密通信的协议。ESP 对负载（通信内容）进行加密并添加其他信息。IP 数据包由标题和加密的有效负载组成，其中有效负载跟在标题后面。除了加密数据，IP 数据包还包括与加密方法和加密密钥、验证数据等有关的信息。 - AH 是 IPsec 协议的一部分，用于验证发送方和防止操纵数据（确保数据的完整性）。在 IP 数据包中，数据紧接在标题后。数据包中还包含使用等式从通信内容、保密密钥等计算得出的哈希值，以防止篡改发送方和操纵数据。与 ESP 不同，通信内容不加密，数据以普通文本的方式发送和接收。 • **加密(不适用于 AH 选项。)** 选择 **DES**、**3DES**、**AES-CBC 128** 或 **AES-CBC 256**。 • **哈希算法** 选择**无**、**MD5**、**SHA1**、**SHA256**、**SHA384** 或 **SHA512**。 仅当为**协议**选择 **ESP** 时，才能选择**无**。 • **SA 生存期** 指定 IKE SA 生存期。 输入时间（秒数）和千字节数（KB） • **压缩模式** 选择**传输**或**隧道**。 • **远程路由器 IP 地址** 输入远程路由器的 IP 地址（IPv4 或 IPv6）。仅当选择**隧道**模式时，输入此信息。 SA（安全关联）是一种加密通信方法，它使用 IPsec 或 IPv6 交换和共享加密方法和加密密钥等信息，以便在开始通信前建立安全的通信信道。SA 还指已建立的虚拟加密通信信道. 用于 IPsec 的 SA 根据 IKE（因特网密钥交换）标准步骤建立加密方法、交换密钥和执行相互认证。SA 还会定期更新。

相关信息

- 使用网络基本管理配置 IPsec 模板

使用 IEEE 802.1x 身份验证保护您的网络

什么是 IEEE 802.1x 验证?

IEEE 802.1x 是用于限制从未经授权的网络设备访问的 IEEE 标准。Brother 设备通过接入点或集线器向 RADIUS 服务器（验证服务器）发送验证请求。访问请求经 RADIUS 服务器验证通过后，本设备即可访问网络。

相关信息

- 使用 IEEE 802.1x 身份验证保护您的网络

使用网络基本管理（Web 浏览器）为您的网络配置 IEEE 802.1x 身份验证

- 如果使用 EAP-TLS 验证配置本设备，在开始配置之前，您必须先安装 CA 机构颁发的客户端证书。有关客户端证书的详细信息，请联系网络管理员。如果您安装了两个或更多证书，我们建议您记录您想使用的证书名称。
- 验证服务器证书前，必须导入由签署服务器证书的 CA 机构（证书授权中心）颁发的 CA 证书。请咨询您的网络管理员或因特网服务供应商（ISP）确认是否需要导入 CA 证书。

也可使用控制面板的无线设置向导（无线网络）配置 IEEE 802.1x 身份验证。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**网络**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 执行以下操作中的一项：
   - 对于有线网络
     点击**有线** > **有线 802.1x 身份验证**。
   - 对于无线网络
     点击**无线** > **无线（企业）**。
6. 配置 IEEE 802.1x 验证设置。

- 要启用有线网络 IEEE 802.1x 验证，请在**有线 802.1x 身份验证**页面上的**有线 802.1x 状态**中选中**已启用**。
- 如果您正在使用 **EAP-TLS** 验证，则必须从**客户端证书**下拉列表中选择已安装的客户端证书（同时显示证书名称）以进行验证。
- 如果选择 **EAP-FAST**、**PEAP**、**EAP-TTLS** 或 **EAP-TLS** 验证，从**服务器证书验证**下拉列表中选择验证方法。通过使用事先已经导入本设备的由签署服务器证书的 CA 机构（证书授权中心）颁发的 CA 证书，验证服务器证书。

从**服务器证书验证**下拉列表选择以下验证方式之一：

选项	说明
无验证	总是信任服务器证书，不执行验证。
CA 证书	通过使用由签署服务器证书的 CA 机构颁发的 CA 证书检查服务器证书的 CA 机构（证书授权中心）是否可靠的验证方法。

选项	说明
CA 证书+服务器 ID	此种验证方法还检查服务器证书的通用名称 [1]。

7. 配置完成后，点击**提交**。

   对于有线网络：配置完成后，将设备连接到支持 IEEE 802.1x 的网络。几分钟后，打印网络配置报告查看 <**Wired IEEE 802.1x**> 状态。

选项	说明
Success	有线 IEEE 802.1x 功能已启用，验证成功。
Failed	有线 IEEE 802.1x 功能已启用，但验证失败。
Off	有线 IEEE 802.1x 功能不可用。

相关信息

- 使用 IEEE 802.1x 身份验证保护您的网络

相关主题：

- 安全证书功能概述
- 配置设备安全性证书

1 通用名称验证是将服务器证书的通用名称与配置给**服务器 ID** 的字符串进行比对。使用此方式前，请先向系统管理员咨询服务器证书的通用名称，然后再配置**服务器 ID**。

IEEE 802.1x 验证方法

EAP-FAST

扩展验证协议-通过安全隧道的灵活验证（EAP-FAST）由思科系统公司研发，是使用用户 ID 和密码进行验证、通过对称密钥算法实现隧道验证的过程。

本 Brother 设备支持以下内部验证方法：

- EAP-FAST/无
- EAP-FAST/MS-CHAPv2
- EAP-FAST/GTC

EAP-MD5（有线网络）

扩展验证协议-消息摘要算法 5（EAP-MD5）使用用户 ID 和密码进行质询-响应验证。

PEAP

受保护的扩展验证协议（PEAP）是思科系统公司、Microsoft 公司和 RSA 安全公司联合研发的一版 EAP 方式。PEAP 在客户端和验证服务器之间创建加密安全套接字层（SSL）/传输层安全（TLS）隧道，用于发送用户 ID 和密码。PEAP 提供服务器和客户端之间的相互验证。

本 Brother 设备支持以下内部验证方法：

- PEAP/MS-CHAPv2
- PEAP/GTC

EAP-TTLS

扩展验证协议-隧道式传输层安全性（EAP-TTLS）由 Funk 软件公司和 Certicom 公司研发。EAP-TTLS 在客户端和验证服务器之间对 PEAP 创建了一个类似的加密 SSL 通道，用于发送用户 ID 和密码。EAP-TTLS 提供服务器和客户端之间的相互验证。

本 Brother 设备支持以下内部验证方法：

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

EAP-TLS

扩展验证协议-传输层安全性（EAP-TLS）在客户端和验证服务器上均要求数字证书验证。

相关信息

- 使用 IEEE 802.1x 身份验证保护您的网络

用户身份验证

- 使用 Active Directory 身份验证
- 使用 LDAP 身份验证
- 使用安全功能锁 3.0

使用 Active Directory 身份验证

- Active Directory 验证简介
- 使用网络基本管理配置 Active Directory 验证
- 使用设备操作面板登录以更改设备设置（Active Directory 验证）

Active Directory 验证简介

Active Directory 验证可限制对本设备的使用。如果启用 Active Directory 验证，设备的操作面板将被锁定。用户输入用户 ID 和密码前，您无法更改设备设置。

Active Directory 验证提供以下功能：

支持的功能、选项和设置可能会因型号而有所不同。

- 存储接收打印数据
- 存储接收传真数据
- 将扫描数据发送到邮件服务器时，根据用户 ID 从 Active Directory 服务器获取电子邮件地址。

  要使用此功能，在**获取邮件地址**设置中选择**开**选项，然后选择 **LDAP + kerberos** 或 **LDAP + NTLMv2** 验证方法。设备将扫描数据发送到邮件服务器时，您的电子邮件地址将被设置为发送方；如果您想将扫描数据发送到您的电子邮件地址，则您的电子邮件地址将被设置为接收方。

启用 Active Directory 验证时，设备将存储所有接收的传真数据。登录后，设备打印存储的传真数据。

您可以使用网络基本管理更改 Active Directory 验证设置。

相关信息

- 使用 Active Directory 身份验证

使用网络基本管理配置 Active Directory 验证

Active Directory 验证支持 Kerberos 验证和 NTLMv2 验证。必须配置用于认证的 SNTP 协议（网络时间服务器）和 DNS 服务器配置。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**管理员** > **用户限制功能**或**限制管理**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 选择 **Active Directory 身份验证**。
6. 点击**提交**。
7. 点击 **Active Directory 身份验证**。
8. 配置以下设置：

支持的功能、选项和设置可能会因型号而有所不同。

选项	说明
存储传真 RX 数据	选择此选项可存储接收传真数据。登录设备后，您可以打印所有接收传真数据。
记住用户 ID	选择此选项可保存您的 ID。
Active Directory 服务器地址	输入 Active Directory 服务器的 IP 地址或服务器名称（例如：ad.example.com）。
Active Directory 域名称	输入 Active Directory 域名。
协议和身份验证方法	选择协议和身份验证方法。
SSL/TLS	选择 **SSL/TLS** 选项。
LDAP 服务器端口	输入端口号以通过 LDAP（仅适用于 **LDAP + kerberos** 或 **LDAP + NTLMv2** 验证方法）连接 Active Directory 服务器。
LDAP 搜索根目录	输入 LDAP 搜索根（仅适用于 **LDAP + kerberos** 或 **LDAP + NTLMv2** 验证方法）。
获取邮件地址	选择此选项可从 Active Directory 服务器获取已登录用户的电子邮件地址。（仅适用于 **LDAP + kerberos** 或 **LDAP + NTLMv2** 验证方法）
获取用户的主目录	选择此选项可获取作为扫描到网络目的地的主目录。（仅适用于 **LDAP + kerberos** 或 **LDAP + NTLMv2** 验证方法）

9. 点击**提交**。

相关信息

- 使用 Active Directory 身份验证

使用设备操作面板登录以更改设备设置（Active Directory 验证）

启用 Active Directory 验证时，设备的操作面板将被锁定，直到您在设备的操作面板上输入用户 ID 和密码。

1. 在设备操作面板上，输入您的用户 ID 和密码进行登录。
2. 验证成功后，设备操作面板将解锁。

相关信息

- 使用 Active Directory 身份验证

使用 LDAP 身份验证

- LDAP 验证简介
- 使用网络基本管理配置 LDAP 验证
- 使用设备操作面板登录以更改设备设置（LDAP 验证）

LDAP 验证简介

LDAP 验证可限制对本设备的使用。如果启用 LDAP 验证，设备的操作面板将被锁定。用户输入用户 ID 和密码前，您无法更改设备设置。

LDAP 验证提供以下功能：

支持的功能、选项和设置可能会因型号而有所不同。

- 存储接收打印数据
- 存储接收传真数据
- 将扫描数据发送到邮件服务器时，根据用户 ID 从 LDAP 服务器获取电子邮件地址。

  要使用此功能，将**获取邮件地址**设置选择为**开**。设备将扫描数据发送到邮件服务器时，您的电子邮件地址将被设置为发送方；如果您想将扫描数据发送到您的电子邮件地址，则您的电子邮件地址将被设置为接收方。

启用 LDAP 验证时，设备将存储所有接收的传真数据。登录后，设备打印存储的传真数据。

您可以使用网络基本管理更改 LDAP 验证设置。

相关信息

- 使用 LDAP 身份验证

使用网络基本管理配置 LDAP 验证

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**管理员** > **用户限制功能**或**限制管理**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 选择 **LDAP 验证**。
6. 点击**提交**。
7. 点击 **LDAP 验证**菜单。
8. 配置以下设置：

   支持的功能、选项和设置可能会因型号而有所不同。

选项	说明
存储传真 RX 数据	选择此选项可存储接收传真数据。登录设备后，您可以打印所有接收传真数据。
记住用户 ID	选择此选项可保存您的 ID。
LDAP 服务器地址	输入 LDAP 服务器的 IP 地址或服务器名称（例如：ldap.example.com）。
SSL/TLS	选择 **SSL/TLS** 选项使用 LDAP over SSL/TLS。
LDAP 服务器端口	输入 LDAP 服务器端口号。
LDAP 搜索根目录	输入 LDAP 搜索根目录。
名字属性（搜索关键）	输入要用作搜索关键字的属性。
获取邮件地址	选择此选项可从 LDAP 服务器获取已登录用户的电子邮件地址。
获取用户的主目录	选择此选项可获取作为扫描到网络目的地的主目录。

9. 点击**提交**。

相关信息

- 使用 LDAP 身份验证

使用设备操作面板登录以更改设备设置（LDAP 验证）

启用 LDAP 验证时，设备操作面板将被锁定，直到您在设备操作面板上输入用户 ID 和密码。

1. 在设备操作面板上，输入您的用户 ID 和密码进行登录。
2. 验证成功后，设备操作面板将解锁。

相关信息

- 使用 LDAP 身份验证

使用安全功能锁 3.0

安全功能锁 3.0 可通过限制设备上的可用功能来增强安全性。

使用安全功能锁 3.0 前

使用安全功能锁配置密码、设置特定用户页数限制及允许使用以下列出的某些或全部功能。
您可以使用网络基本管理配置和更改以下安全功能锁 3.0 设置：

支持的功能、选项和设置可能会因型号而有所不同。

- **打印**
- **复印**
- **扫描**
- **传真**
- **介质**
- **网络连接**
- **应用**
- **页数限制**
- **页面计数器**
- **卡 ID (NFC ID)**

触摸式液晶显示屏型号：
启用安全功能锁后，设备会自动进入公共模式并且部分功能仅限授权用户使用。要访问设备的限制功能，按 ，选择用户名并输入密码。

相关信息

- 使用安全功能锁 3.0

使用网络基本管理配置安全功能锁 3.0

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**管理员** > **用户限制功能**或**限制管理**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 选择**安全功能锁定**。
6. 点击**提交**。
7. 点击**受限功能** 菜单。
8. 配置相关设置，以管理每个用户或每个群组的权限。
9. 点击**提交**。
10. 点击**用户列表**菜单。
11. 配置用户列表。
12. 点击**提交**。

   也可更改在**安全功能锁定**菜单中设置的用户列表锁定设置。

相关信息

- 使用安全功能锁 3.0

使用安全功能锁 3.0 进行扫描

支持的功能、选项和设置可能会因型号而有所不同。

设置扫描限制（适用于管理员）

安全功能锁 3.0 允许管理员指定用户扫描的权限。当扫描功能设置为对公共用户关闭时，仅已选中**扫描**复选框的用户具有扫描权限。

使用扫描功能（适用于受限用户）

- 若要使用设备的操作面板进行扫描：

  受限用户必须在设备操作面板上输入自己的密码才能访问扫描模式。
- 若要从计算机进行扫描：

  从计算机进行扫描前，受限用户必须在设备操作面板上输入自己的密码。如果没有在设备操作面板上输入密码，用户的计算机上将显示一条错误信息。

如果本设备支持 IC 卡验证，则受限用户也可通过用其注册 IC 卡触碰设备操作面板上的 NFC 符号，来访问扫描模式。

相关信息

- 使用安全功能锁 3.0

配置安全功能锁 3.0 的公共模式

使用“安全功能锁”屏幕设置“公共模式”，以限制公共用户可使用的功能。公共用户不需要输入密码就可以访问通过“公共模式”设置设为可用的功能。

公共模式包括通过 Brother iPrint&Scan 和 Brother Mobile Connect 发送的打印作业。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。

   例如：

   https://192.168.1.2

   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**管理员** > **用户限制功能**或**限制管理**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 选择**安全功能锁定**。
6. 点击**提交**。
7. 点击**受限功能** 菜单。
8. 在**公共模式**行中，选中相应的复选框允许使用所列出的功能，或取消选中相应的复选框限制使用所列出的功能。
9. 点击**提交**。

相关信息

- 使用安全功能锁 3.0

使用网络基本管理配置个人主页屏幕

作为管理员，您可以指定用户可在其个人主页屏幕上查看的选项卡。这些选项卡允许快速访问用户的常用快捷方式；用户可以从设备的操作面板中将这些快捷方式指定给他们的个人主页屏幕选项卡。

支持的功能、选项和设置可能会因型号而有所不同。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**管理员** > **用户限制功能**或**限制管理**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 选择**安全功能锁定**。
6. 在**选项卡设置**字段中，选择**个人**作为要用作个人主页屏幕的选项卡名称。
7. 点击**提交**。
8. 点击**受限功能** 菜单。
9. 配置相关设置，以管理每个用户或群组的权限。
10. 点击**提交**。
11. 点击**用户列表**菜单。
12. 配置用户列表。
13. 从下拉列表中选择各用户的**用户列表/受限功能**。
14. 从**主屏幕**下拉列表中选择各用户的选项卡名称。
15. 点击**提交**。

相关信息

- 使用安全功能锁 3.0

安全功能锁 3.0 的其他安全功能

在安全功能锁屏幕中配置以下功能：

支持的功能、选项和设置可能会因型号而有所不同。

所有计数器重置

点击**页面计数器**列中的**所有计数器重置**重置页面计数器。

导出到 CSV 文件

点击**导出到 CSV 文件**，将包含**用户列表/受限功能**信息的当前页面和尾页计数器记录导出为 CSV 文件。

卡 ID (NFC ID)

点击**用户列表**菜单，然后在**卡 ID (NFC ID)**字段中输入用户的卡 ID。您可以使用 IC 卡进行验证。

输出

设备上已安装出纸分页器单元时，从下拉列表中选择各用户的出纸托板。

最后计数器记录

如果您想让设备在重置计数器后仍保留页面计数，点击**最后计数器记录**。

计数器自动重设

点击**计数器自动重设**配置所需的重置页面计数器的时间间隔。可选择每天、每周或每月。

相关信息

- 使用安全功能锁 3.0

使用设备的操作面板注册新 IC 卡

可在设备上注册集成电路卡（IC 卡）。

支持的功能、选项和设置可能会因型号而有所不同。

1. 让已注册的集成电路卡（IC 卡）触碰本设备操作面板上的近场通信（NFC）标记。
2. 按液晶显示屏上您的用户 ID。
3. 按注册卡按钮。
4. 将新 IC 卡触碰到 NFC 标记。
   新 IC 卡的号码即被注册到本设备中。
5. 按 OK 按钮。

相关信息

- 使用安全功能锁 3.0

注册外接 IC 卡读卡器

连接外接 IC（集成电路）卡读卡器时，使用网络基本管理注册读卡器。您的设备可连接支持 HID 级别驱动程序的外接 IC 卡读卡器。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。

   例如：

   https://192.168.1.2

   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**管理员** > **外部读卡器**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 输入必要信息，然后点击 **提交**。
6. 重新启动本 Brother 设备以激活配置。
7. 将读卡器连接到设备。
8. 使用卡验证时，让卡触碰读卡器。

相关信息

- 使用安全功能锁 3.0

安全发送或接收电子邮件

- 使用网络基本管理配置电子邮件发送或接收
- 发送带用户身份验证的电子邮件
- 使用 SSL/TLS 安全发送或接收电子邮件

使用网络基本管理配置电子邮件发送或接收

- 电子邮件接收功能仅适用于特定型号。
- 我们建议您使用网络基本管理配置带用户身份验证的加密电子邮件发送或使用 SSL/TLS 的电子邮件发送和接收功能（仅限支持型号）。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**网络** > **网络** > **协议**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 在 **POP3/IMAP4/SMTP 客户端**字段中，点击**高级设置**，确保 **POP3/IMAP4/SMTP 客户端**的状态为**已启用**。

   - 适用协议可能会因设备不同而有所差异。
   - 如果出现**身份验证方式**选项屏幕，选择您的验证方法，然后遵循屏幕提示。
6. 配置 **POP3/IMAP4/SMTP 客户端**设置。
   - 通过发送测试电子邮件来确认配置后的电子邮件设置是否正确。
   - 如果您不知道 POP3/IMAP4/SMTP 服务器设置，请联系您的网络管理员或因特网服务供应商 （ISP）。
7. 完成后，点击**提交**。
   将显示**测试发送和接收电子邮件配置**对话框。
8. 遵循对话框中的提示测试当前的设置。

相关信息

- 安全发送或接收电子邮件

相关主题：

- 使用 SSL/TLS 安全发送或接收电子邮件

发送带用户身份验证的电子邮件

本设备通过要求进行用户身份验证的邮件服务器发送电子邮件。此方法可防止未经授权用户访问电子邮件服务器。可以使用用户身份验证发送电子邮件通知、电子邮件报告和 I-Fax（仅适用于特定型号）。

- 适用协议可能会因设备不同而有所差异。
- 我们建议您使用网络基本管理配置 SMTP 验证。

电子邮件服务器设置

您必须配置本设备的 SMTP 验证方法，以匹配邮件服务器所使用的方法。关于邮件服务器设置的详细信息，请联系您的网络管理员或因特网服务供应商（ISP）。

若要使用网络基本管理启用 SMTP 服务器验证，在 **POP3/IMAP4/SMTP 客户端** 屏幕上的**服务器验证方法**下选择您的验证方法。

相关信息

- 安全发送或接收电子邮件

使用 SSL/TLS 安全发送或接收电子邮件

本设备支持 SSL/TLS 通信方法。若要使用采用 SSL/TLS 通信的邮件服务器，必须配置以下设置。

- 电子邮件接收功能仅适用于特定型号。
- 我们建议您使用网络基本管理配置 SSL/TLS。

验证服务器证书

如果您选择 **SSL/TLS** 中的 **SSL** 或 **TLS**，**验证服务器证书**复选框将被自动选中。

- 验证服务器证书前，必须导入由签署服务器证书的 CA 机构（证书授权中心）颁发的 CA 证书。请咨询您的网络管理员或因特网服务供应商（ISP）确认是否需要导入 CA 证书。
- 如果不需要验证服务器证书，请取消勾选**验证服务器证书**复选框。

端口号码

如果您选择 **SSL** 或 **TLS**，**端口**值将根据协议自动更改。若要手动更改端口号，请在选择 **SSL/TLS** 设置后输入端口号。

必须根据邮件服务器所使用的方法配置本设备的通信方法。有关邮件服务器设置的详细信息，请联系您的网络管理员或 ISP。

在大多数情况下，加密网页邮件服务要求以下设置：

支持的功能、选项和设置可能会因型号而有所不同。

SMTP	**端口**	587
	服务器验证方法	**SMTP 身份验证**
	SSL/TLS	**TLS**
POP3	**端口**	995
	SSL/TLS	**SSL**
IMAP4	**端口**	993
	SSL/TLS	**SSL**

相关信息

- 安全发送或接收电子邮件

相关主题：

- 使用网络基本管理配置电子邮件发送或接收
- 配置设备安全性证书

存储打印日志到网络

将打印日志存储到网络的功能概述

通过存储打印日志到网络功能，您可以使用公共因特网文件系统（CIFS）协议将本设备的打印日志文件保存到网络服务器中。您可以记录各个打印作业的 ID、打印作业类型、作业名称、用户名、日期、时间和打印页数。CIFS 是通过 TCP/IP 运行的协议，允许网络计算机在内部网或因特网上共享文件。

打印日志中记录以下打印功能：

支持的功能、选项和设置可能会因型号而有所不同。

- 从计算机打印作业
- USB 直接打印
- 复印
- 接收到的传真
- 网络连接打印

- 存储打印日志到网络功能支持 Kerberos 验证和 NTLMv2 验证。必须在操作面板上正确配置用于身份验证的 SNTP 协议（网络时间服务器）或日期、时间和时区。
- 将文件保存到服务器中时，文件类型可以设置为 TXT 或 CSV。

相关信息

- 存储打印日志到网络

使用网络基本管理配置“存储打印日志到网络”设置

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。
   例如：
   https://192.168.1.2
   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。

4. 在左侧导航栏中，点击**管理员** > **存储打印日志到网络**。

如果左侧导航栏不可见，请点击 ☰ 启动导航。

5. 在**打印日志**字段中，点击**开**。
6. 配置以下设置：

支持的功能、选项和设置可能会因型号而有所不同。

选项	说明
网络文件夹路径	输入 CIFS 服务器上用于存储打印日志的目标文件夹（例如：\\ComputerName\SharedFolder）。
文件名	输入您想为打印日志指定的文件名称（最多 32 个字符）。
文件类型	选择 **TXT** 或 **CSV** 选项作为打印日志文件类型。
日志时间源	选择打印日志的时间源。
验证方法	选择访问 CIFS 服务器所需的验证方法：**自动**、**Kerberos** 或 **NTLMv2**。通过 Kerberos 验证协议，设备或个人可使用单点登录向网络服务器安全地证明其身份。NTLMv2 是 Windows 用于登录服务器的验证方法。 • **自动**：如果选择**自动**，将使用 NTLMv2 作为验证方法。 • **Kerberos**：选择 **Kerberos** 选项，则只可使用 Kerberos 验证。 • **NTLMv2**：选择 **NTLMv2** 选项，则只可使用 NTLMv2 验证。 • 对于 **Kerberos** 和 **NTLMv2** 验证，还必须配置**日期和时间**设置或 SNTP 协议（网络时间服务器）和 DNS 服务器。 • 您也可以使用设备的操作面板配置日期和时间设置。
用户名	输入用于验证的用户名（最多 96 个字符）。 如果用户名是域的一部分，请以下列任一格式输入用户名：user@domain 或 domain\user。
密码	输入用于验证的密码（最多 32 个字符）。
Kerberos 服务器地址(如有需要)	输入密钥分发中心（KDC）主机地址（例如：kerberos.example.com；最多 64 个字符）或 IP 地址（例如：192.168.56.189）。
错误检测设置	选择由于网络错误而无法将打印日志存储到服务器时将进行的操作。

7. 在**连接状态**字段中，确认最新的日志状态。

   也可在设备的液晶显示屏上确认错误状态。

8. 点击**提交**显示**网络日志打印测试**页面。
   要测试设置，点击**是**，然后转到下一步。
   要跳过测试，点击**否**。系统将自动提交设置。
9. 设备将测试您的设置。
10. 如果您的设置被接受，屏幕上将显示**测试正常**。
    如果显示**测试错误**，请检查所有设置，然后点击**提交**再次显示测试页面。

相关信息

- 存储打印日志到网络

使用存储打印日志到网络功能的错误检测设置

使用错误检测设置可决定由于网络错误而无法将打印日志存储到服务器时将进行的操作。

1. 打开您的网络浏览器。
2. 在您的浏览器地址栏中输入“https://设备的 IP 地址”（其中，“设备的 IP 地址”为本设备的 IP 地址）。

   例如：

   https://192.168.1.2

   本设备的 IP 地址可在网络配置报告中找到。
3. 如有需要，在**登录**字段中输入密码，然后点击**登录**。

   用于管理本设备设置的默认密码位于设备背面或底座并标有 “**Pwd**” 字样。首次登录时，请遵循屏幕提示更改默认密码。
4. 在左侧导航栏中，点击**管理员** > **存储打印日志到网络**。

   如果左侧导航栏不可见，请点击 ☰ 启动导航。
5. 在**错误检测设置**部分，选择**取消打印**或**忽略日志并打印**选项。

   支持的功能、选项和设置可能会因型号而有所不同。

选项	说明
取消打印	如果您选择**取消打印**选项，当无法将打印日志保存到服务器时，将取消打印作业。 即使选择**取消打印**选项，设备仍会打印接收到的传真。
忽略日志并打印	如果您选择**忽略日志并打印**选项，即使无法将打印日志存储到服务器，设备仍会打印文档。 存储打印日志功能恢复后，打印日志记录如下： Id, Type, Job Name, User Name, Date, Time, Print Pages 1, Print(xxxxxxx), “Document01.doc”, “user01”, 03/03/20xx, 14:01:32, 52 2, Print(xxxxxxx), “Document02.doc”, “user01”, 03/03/20xx, 14:45:30, ? (a) 3, <Error>, ?, ?, ?, ?, ? (b) 4, Print(xxxxxxx), “Report01.xls”, “user02”, 03/03/20xx, 19:30:40, 4 a. 如果打印结束时无法存储打印日志，将不会记录打印页数。 b. 如果打印开始和结束时均无法存储打印日志，将不记录当前作业的打印日志。此功能恢复后，此错误将反映在打印日志中。

6. 点击**提交**显示**网络日志打印测试**页面。

   要测试设置，点击**是**，然后转到下一步。

   要跳过测试，点击**否**。系统将自动提交设置。
7. 设备将测试您的设置。
8. 如果您的设置被接受，屏幕上将显示**测试正常**。

   如果显示**测试错误**，请检查所有设置，然后点击**提交**再次显示测试页面。

相关信息

- 存储打印日志到网络

使用带安全功能锁 3.0 的存储打印日志到网络功能

安全功能锁 3.0 激活时，复印、传真接收、Web Connect Print 和 USB Direct Print 的注册用户名称将被记录在保存打印日志至网络的报告中。Active Directory Authentication 启用时，用户名将被记录在存储打印日志至网络的报告中：

支持的功能、选项和设置可能会因型号而有所不同。

```
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
```

相关信息

- 存储打印日志到网络

brother

Brother Earth

www.brotherearth.com

SCHN

版本 0