安全功能说明书

重要安全信息

- 管理本机设置的默认密码位于本机底部并标有 **“Pwd:”**。我们建议立即更改默认密码，以保护本机免受未授权访问。
- 当将本机连接到外部网络（如互联网）时，请确保您的网络环境受独立防火墙或其他手段保护，以防止因设置不当导致信息泄露或恶意第三方未授权访问。
- 若周围存在无线信号，无线局域网允许您自由建立局域网连接。但是，如果安全设置配置不正确，信号可能会被恶意第三方拦截，可能导致：
  - 个人或机密信息被盗
  - 信息被误传给冒充特定身份的人员
  - 泄露被截获的通信内容记录

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）

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

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** 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。若要安全地管理打印服务器，请使用 SNMPv3 模式，然后配置设置。
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 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