



智能卡验证

管理员指南

目录

修改历史.....	4
概述.....	5
部署准备查对表.....	6
配置打印机设置.....	7
访问“嵌入式 Web 服务器”	7
设置屏幕超时.....	7
手动安装证书.....	7
自动安装证书.....	7
配置 TCP/IP 码设置.....	8
设置日期和时间.....	8
配置 LDAP 网络帐户设置.....	8
保护对打印机的访问.....	9
配置打印机电子邮件设置.....	10
配置应用程序.....	12
配置“智能卡验证客户端”	12
配置安全电子邮件.....	14
配置安全挂起打印作业.....	15
导入或导出配置文件.....	15
使用应用程序.....	16
安全电子邮件.....	16
安全挂起打印作业.....	16
疑难解答.....	18
应用程序错误.....	18
登录问题.....	18
验证问题.....	20
安全电子邮件问题.....	24
安全挂起打印作业问题.....	28
LDAP 问题.....	29
许可证错误.....	30

注意事项..... 31

索引..... 32

修改历史

2017 年 8 月

- 添加有关更改登录方法的说明。
- 添加有关禁用设备配额应用程序的说明。
- 添加对巴西葡萄牙语、芬兰语、法语、德语、意大利语、简体中文和西班牙语的支持。

2016 年 7 月

- 添加有关如何配置“发送电子邮件到私人信箱”应用程序的说明。

2016 年 1 月

- 带有类似平板触摸显示屏的多功能产品的初始文档发布。

概述

*智能卡验证*是一个应用程序集合，用于保护对打印机及其功能访问。应用程序让您手动或使用智能卡登录到打印机，然后安全地发送电子邮件和释放打印作业。您还可以在应用程序中配置其他安全设置，如电子邮件签名和加密。

“智能卡验证”包包括以下应用程序：

- **智能卡验证客户端**—让您通过要求用户使用智能卡或用户名和密码登录来保护对打印机的访问。您可以保护对打印机主屏幕或单独的应用程序和功能的访问。应用程序还提供 **Kerberos 验证选项**和 **Kerberos 票证**，可用于保护其他应用程序。
- **智能卡驱动程序**—让打印机与支持的智能卡通信。
- **显示定制**—让您上载图像到打印机。您可以使用图像来创建自定义的幻灯片或者设置打印机的壁纸和屏幕保护程序。使用“智能卡验证”客户端来要求用户在访问打印机主屏幕之前进行身份验证以保护此应用程序。
- **安全电子邮件**—让您数字签名和加密从打印机发送的电子邮件。该应用程序会覆盖标准的打印机电子邮件功能。
- **安全挂起打印作业**—让经过验证的用户查看或释放他们的挂起打印作业。

本文档提供有关如何配置、使用和解决应用程序问题的信息。

部署准备查对表

确认：

- 您已经在打印机中安装以下项目：
 - 至少 512MB RAM
 - 智能卡读卡器及其驱动程序
- 您已经禁用设备配额应用程序：
 - 1 获取打印机 IP 地址。请执行下面的任一操作：
 - 在打印机主屏幕上找到 IP 地址。
 - 从打印机主屏幕，触摸 **设置** > **网络/端口** > **网络概述**。
 - 2 打开 Web 浏览器，然后键入打印机 IP 地址。
 - 3 单击 **应用程序** > **设备配额** > **停止**。

您有下列信息用于配置智能卡验证客户端：

- 证书颁发机构证书（.cer 文件）
 - 轻量级目录访问协议 (LDAP) 和 Active Directory® 帐户
-

- Kerberos 领域、域和域控制器
-

- Kerberos 文件（对于多个域）

配置打印机设置

您可能需要管理权限才能配置打印机设置。

访问“嵌入式 Web 服务器”

- 1 获取打印机 IP 地址。请执行下面的任一操作：
 - 在打印机主屏幕上找到 IP 地址。
 - 从打印机主屏幕，触摸**设置** > **网络/端口** > **网络概述**。
- 2 打开 Web 浏览器，然后键入打印机 IP 地址。

设置屏幕超时

为了防止未经授权的访问，您可以限制用户登录到打印机而没有活动的时间。

- 1 从“嵌入式 Web 服务器”，单击**设置** > **设备** > **首选项**。
- 2 在“屏幕超时”字段中，指定在显示屏变为待机并且用户注销之前的时间。建议将值设置为 30 秒。
- 3 单击**保存**。

手动安装证书

注意：要自动下载 CA 证书，请参阅[第 7 页上的“自动安装证书”](#)。

在配置 Kerberos 或域控制器设置之前，请安装用于域控制器验证的 CA 证书。如果您要将链验证用于域控制器证书，请安装整个证书链。每个证书必须是一个单独的 PEM (.cer) 文件。

- 1 从“嵌入式 Web 服务器”，单击**设置** > **安全** > **证书管理**。
- 2 从“管理 CA 证书”部分，单击**上载 CA**，然后浏览 PEM (.cer) 文件。

示例证书：

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQY6sV0KL3tIhBtlr4gHG85zANBgkqhkiG9w0BAQUFADBz
...
I3DTbPe0mnIbTq0iWqKEaVne1vvaDt52iSpEQyevwgUcHD16rFy+sOnCaQ==
-----END CERTIFICATE-----
```

- 3 单击**保存**。

自动安装证书

- 1 从“嵌入式 Web 服务器”，单击**设置** > **安全** > **证书管理** > **配置证书自动更新**。
- 2 如果提示您加入 Active Directory 域，请单击**加入域**，然后键入域信息。

注意：确认 Active Directory 域与智能卡设置中使用的 Kerberos 领域或域相匹配。如需更多信息，请参阅[第 12 页上的“配置智能卡设置”](#)。

3 选择启用自动更新。

注意：如果您要安装 CA 证书而不等待预定的运行时间，请选择立即取回。

4 单击保存。

配置 TCP/IP 码设置

1 从“嵌入式 Web 服务器”，单击设置 > 网络/端口 > TCP/IP。

2 执行下面的任何操作：

- 如果您使用静态 IP 地址，请键入 DNS 服务器地址。如果备份 DNS 服务器可用，请键入备份 DNS 服务器地址。
- 如果打印机位于不同的域中，请在“域搜索顺序”字段中键入其他域。使用逗号来分隔多个域。

注意：使用分配给用户工作站的域名。

3 单击保存。

设置日期和时间

当使用 Kerberos 验证时，请确保打印机和域控制器之间的时差不超过 5 分钟。您可以手动更新日期和时间设置，或者使用“网络时间协议 (NTP)”来自动同步域控制器的时间。

1 从“嵌入式 Web 服务器”，单击设置 > 设备 > 首选项 > 日期和时间。

手动配置

注意：手动配置日期和时间会禁用 NTP。

- a 从“配置”部分，在“手动设置日期和时间”字段中，输入适当的日期和时间。
- b 选择日期格式、时间格式和时区。

注意：如果您选择（UTC+用户）自定义，请指定 UTC (GMT) 和 DST 的时差值。

配置 NTP

- a 从“网络时间协议”部分，选择启用 NTP，然后键入 NTP 服务器的 IP 地址或主机名。
- b 如果 NTP 服务器要求验证，请在“启用验证”菜单中，选择 MD5 密钥。
- c 根据您的打印机型号，输入密钥 ID 和密码，或者浏览包含 NTP 验证凭证的文件。

2 单击保存。

配置 LDAP 网络帐户设置

需要 LDAP 网络帐户才能发送加密电子邮件。从 LDAP 服务器添加和配置收件人的加密证书。如需更多信息，请与您的系统管理员联系。

注意：需要 Kerberos 网络帐户才能创建 LDAP + GSSAPI 网络帐户。

1 从“嵌入式 Web 服务器”，单击设置 > 安全 > 登录方法。

2 从“网络帐户”部分，单击添加登录方法 > LDAP。

3 选择 LDAP 或 LDAP + GSSAPI。

4 从“常规信息”部分，配置下列设置：

- **设置名**—LDAP 网络帐户的唯一名称。
- **服务器地址**

注意：确认地址与“智能卡验证客户端”域控制器地址，或 Kerberos 配置文件中的 KDC 地址相同。

- **服务器端口**—如果您使用 SSL，请使用端口 **636**。否则，使用端口 **389**。

5 从“设备凭证”部分，清除**匿名 LDAP 绑定**，然后键入用于连接到 LDAP 服务器的验证凭证。

6 如果 LDAP 服务器需要 SSL，请从“高级选项”部分，将“使用 SSL/TLS”设置为 **SSL/TLS**。

7 从“地址簿设置”部分，选择**使用用户凭证**。

8 单击**保存并校验**。

保护对打印机的访问

保护对主屏幕的访问

要求用户在访问打印机主屏幕之前进行验证。

注意：在您开始之前，请确认已在您的打印机中启用“显示定制”应用程序。如需更多信息，请参阅 [显示定制管理员指南](#)。

1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录方法**。

2 从“公共”部分，单击**管理权限**。

3 展开**应用程序**，清除**幻灯片、更换壁纸和屏幕保护程序**，然后单击**保存**。

4 从“其他登录方法”部分，单击“智能卡”旁边的**管理权限**。

5 选择您要管理其权限的组。

注意：“所有用户”组是默认创建的。当您在“组授权列表”字段中指定现有的 Active Directory 组时，会出现更多的组名。如需更多信息，请参阅 [第 13 页上的“配置高级设置”](#)。

6 展开**应用程序**，然后选择**幻灯片、更换壁纸和屏幕保护程序**。

7 单击**保存**。

保护对单独应用程序和功能的访问

要求用户在访问应用程序或内置的打印机功能之前进行验证。

1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录方法**。

2 从“公共”部分，单击**管理权限**。

3 限制对您要保护的应用程序或功能的公共访问。执行下面的任何操作：

- 对于“安全电子邮件”，请展开**功能访问**，清除**电子邮件功能**复选框，然后单击**保存**。
- 对于“安全挂起打印作业”，请展开**应用程序**，清除**安全挂起打印作业**复选框，然后单击**保存**。
- 对于其他应用程序或功能，展开一个或多个类别，清除应用程序或功能复选框，然后单击**保存**。

4 从“其他登录方法”部分，单击“智能卡”旁边的**管理权限**。

5 选择您要管理其权限的组。

注意：“所有用户”组是默认创建的。当您在“组授权列表”字段中指定现有的 Active Directory 组时，会出现更多的组名。如需更多信息，请参阅[第 13 页上的“配置高级设置”](#)。

6 选择您希望经验证用户访问的应用程序或功能。执行下面的任何操作：

- 对于“安全电子邮件”，请展开**功能访问**，然后选择**电子邮件功能**。
- 对于“安全挂起打印作业”，请展开**应用程序**，然后选择**安全挂起打印作业**。
- 对于其他应用程序或功能，请展开一个或多个类别，然后选择应用程序或功能。

7 单击**保存**。

在主屏幕上显示安全的应用程序或功能

默认情况下，安全的应用程序或功能从打印机主屏幕隐藏。

1 从嵌入式网页服务器，单击**设置 > 安全 > 杂项**。

2 在“受保护特性”菜单中，选择**显示**。

3 单击**保存**。

配置打印机电子邮件设置

该应用程序会覆盖打印机电子邮件功能。

配置 SMTP 设置

1 从“嵌入式 Web 服务器”，单击**设置 > 电子邮件 > 电子邮件设置**。

2 配置下面的设置：

- **主要 SMTP 网关**—用于发送电子邮件的服务器的 IP 地址或主机名。
注意：对于 Kerberos 验证，请使用主机名。
- **主要 SMTP 网关端口**
- **次要 SMTP 网关**—次要或备份 SMTP 服务器的服务器 IP 地址或主机名。
- **次要 SMTP 网关端口**
- **SMTP 超时**
- **使用 SSL/TLS**
- **答复地址**
- **SMTP 服务器验证**

注意：

- 如果选择 **Kerberos 5**，请键入 Kerberos 领域。
- 如果选择 **NTLM**，请键入 NTLM 域。
- 如果 SMTP 服务器要求验证但不支持 Kerberos，请在“答复地址”字段中，键入打印机 IP 地址或主机名。

- **设备启动的电子邮件**—对于设备启动的电子邮件，设备凭证是必需的。

注意： 如果选择使用设备 **SMTP 凭证**，请键入验证凭证。

- **用户启动的电子邮件**—对于用户启动的电子邮件，用户凭证是必需的。

注意： 如果您使用 **Kerberos 验证**，请选择使用会话用户 **ID 和密码**。

3 单击**保存**。

配置默认的电子邮件和扫描设置

1 从“嵌入式 Web 服务器”，单击**设置 > 电子邮件 > 电子邮件默认设置**。

2 配置设置。

3 如果需要，请调整高级成像和管理控制设置。

4 单击**保存**。

配置发送电子邮件到私人信箱

“发送电子邮件到私人信箱”允许用户将一个电子邮件副本发送到他们的电子邮件地址。如需更多信息，请参阅*发送电子邮件到私人信箱管理员指南*。

根据您的打印机型号，请执行下面的任一操作：

对于应用程序的内置版本

1 从“嵌入式 Web 服务器”，单击**设置 > 电子邮件 > 电子邮件默认设置 > 管理控制**。

2 选择**限制电子邮件收件人**。

3 单击**保存**。

对于“嵌入式解决方案框架 (eSF)”应用程序

1 从“嵌入式 Web 服务器”，导航至应用程序的配置页：

应用程序 > 发送电子邮件到私人信箱 > 配置

2 选择**启用**。

3 单击**应用**。

配置应用程序

配置“智能卡验证客户端”

您可能需要管理权限才能配置应用程序。

配置登录屏幕设置

使用登录屏幕设置来设置您希望用户登录到打印机的方式。

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“登录屏幕”部分，选择登录类型。
- 3 在“用户验证模式”菜单中，选择验证用户证书的方法。
 - **Active Directory**—智能卡上的用户证书使用 Kerberos 验证进行验证。此设置可能需要 LDAP 查询。
 - **具有来宾访问的 Active Directory**—拥有智能卡但不在 Active Directory 中的用户可以访问部分打印机功能。需要正确配置的“在线证书状态协议 (OCSP)”服务器。如果 Active Directory 验证失败，那么应用程序会查询 OCSP 服务器。
 - **仅 PIN 码**—用户只能访问不要求 Kerberos 验证的应用程序或功能。
- 4 在“验证智能卡”菜单中，选择在触碰智能卡之后验证用户的方法。
- 5 如果需要，请允许用户更改登录方法。
- 6 单击应用。

配置手动登录设置

对于手动登录，打印机使用在 Kerberos 配置文件中指定的默认域。如果您使用不同的域，请在手动登录设置中指定域名。

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“手动登录设置”部分，在“手动登录域”字段中键入一个或多个域。
- 3 单击应用。

配置智能卡设置

注意：确认打印机和验证服务器之间的网络连接配置正确。如需更多信息，请与您的系统管理员联系。

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“智能卡设置”部分，在“Kerberos 信息”菜单中，选择下面的任一项：
 - **使用设备 Kerberos 设置文件**—必须在打印机上手动安装 Kerberos 配置文件。执行下面的操作：
 - a 从“嵌入式 Web 服务器”，单击设置 > 安全 > 登录方法。
 - b 从“网络帐户”部分，单击添加登录方法 > Kerberos。

- c 从“导入 Kerberos 文件”部分，浏览适当的 krb5.conf 文件。
- d 如果您的网络不使用反向 DNS 查询，请从“杂项设置”部分选择**禁用反向 IP 查询**。
- e 单击**保存并校验**。

- **使用简单 Kerberos 设置**—在打印机上自动创建 Kerberos 文件。指定以下项目：
 - **领域**—领域必须以大写字母键入。
 - **域控制器**—使用逗号来分隔多个值。域控制器按列出的顺序进行验证。
 - **域**—在“领域”字段中指定必须映射到 Kerberos 领域的域。使用逗号来分隔多个域。
注意：域是区分大小写的。
 - **超时**—输入从 3 至 30 秒的值。

3 在“域控制器验证”菜单中，选择验证域控制器证书的方法。

注意：在配置此设置之前，请确认在打印机上安装适当的证书。如需更多信息，请参阅[第 7 页上的“手动安装证书”](#)。

- **使用设备证书验证**—使用安装在打印机上的 CA 证书。
- **使用设备链验证**—使用安装在打印机上的整个证书链。
- **使用 OCSP 验证**—使用 OCSP 服务器。必须在打印机上安装整个证书链。从“在线证书状态协议 (OCSP)”部分，配置以下设置：
 - **响应者 URL**—OCSP 响应者或中继器的 IP 地址或主机名，以及使用的端口号。使用逗号来分隔多个值。
例如：`http://x:y`，其中 **x** 是 IP 地址或主机名，而 **y** 是端口号。
 - **响应者证书**—使用 X.509 证书。
 - **响应者超时**—输入从 5 至 30 秒的值。
 - **允许未知状态**—即使一个或多个证书的状态未知，用户也可以登录。

4 单击**应用**。

配置高级设置

1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：

应用程序 > 智能卡验证客户端 > 配置

2 从“高级设置”部分，选择一个会话用户 ID。

注意：一些应用程序，如“安全挂起打印作业”和“安全电子邮件”需要会话用户 ID 的值。

3 在“电子邮件发件人地址”菜单中，选择打印机检索用户电子邮件地址的位置。

4 如果需要，请选择**等待用户信息**来在允许用户访问主屏幕或安全应用程序之前检索所有的用户信息。

如果以下设置设定为“LDAP 查询”，请选择此选项。

- 会话用户 ID
- 电子邮件发件人地址

如果以下设置不为空，请选择此选项。

- 其他用户属性
- 组授权列表

注意：如果您使用“安全电子邮件”的手动登录，请选择此选项来将用户的电子邮件地址存储在登录会话中。要允许手动登录用户发送打印机给他们自己，请在打印机电子邮件设置中启用“发送一份副本给我”。

5 如果需要，请选择将 **SSL 用于用户信息** 来使用 SSL 连接从域控制器检索用户信息。

6 如果需要，在“其他用户属性”字段中，键入必须添加到会话的其他 LDAP 属性。使用逗号来分隔多个值。

7 在“组授权列表”中，键入可以访问应用程序或功能的 Active Directory 组。使用逗号来分隔多个值。

注意：组必须在 LDAP 服务器中。

8 如果在您的网络中没有启用 DNS，请上载主机文件。

以下面的格式在文本文件中键入映射：**xy**，其中 **x** 是 IP 地址，而 **y** 是主机名。您可以分配多个主机名到一个 IP 地址。例如：**255.255.255.255 HostName1 HostName2 HostName3**。

您不能分配多个 IP 地址到一个主机名。要分配 IP 地址到主机名组，请在文本文件的每个单独行上键入每一个 IP 地址及其关联的主机名。

例如：

```
123.123.123.123 HostName1 HostName2
456.456.456.456 HostName3
```

9 单击**应用**。

配置安全电子邮件

您可能需要管理权限才能配置应用程序。

配置安全电子邮件设置

1 从“嵌入式 Web 服务器”，浏览至应用程序的配置页：

应用程序 > 安全电子邮件 > 配置

2 配置设置。

注意：

- 要数字签名电子邮件，您必须持有有效的数字签名证书，并使用智能卡登录。签名证书只能从智能卡使用。如需更多信息，请与您的系统管理员联系。
- 要接收加密的电子邮件，收件人必须在 LDAP 服务器地址簿中，并且必须持有有效的加密证书。如需更多信息，请参阅[第 8 页上的“配置 LDAP 网络帐户设置”](#)。
- 要将安全标记应用于电子邮件，请启用该设置，然后键入您要使用的文本。
- 如需有关每一个设置的更多信息，请参阅鼠标悬停的帮助。

3 单击**应用**。

配置安全挂起打印作业

限制未经验证的用户查看挂起作业

可以使用内置的挂起作业应用程序来查看打印机中的所有挂起作业。设置安全挂起打印作业之后，从打印机主屏幕移除挂起作业图标。

- 1 从嵌入式网页服务器，单击**设置 > 设备 > 可见的主屏幕图标**。
- 2 清除**挂起作业**。
- 3 单击**保存**。

配置安全挂起打印作业设置

- 1 从嵌入式网页服务器，导览至应用程序的配置页：
应用程序 > 安全挂起打印作业 > 配置
- 2 从“释放选项”部分，配置这些设置。
 - **释放方法**—指定用户如何打印他们的挂起作业。
 - **按排序显示打印作业**—指定打印作业如何在显示屏上列出。
- 3 单击**应用**。

将打印作业转换为安全挂起打印作业

- 1 从嵌入式网页服务器，单击**设置 > 安全 > 保密打印设置**。
- 2 选择**要求挂起所有作业**。
- 3 单击**保存**。

导入或导出配置文件

注意：导入配置文件会覆盖现有的应用程序配置。

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页。执行以下操作之一：
 - 单击**应用程序 > 智能卡验证客户端 > 配置**
 - 单击**应用程序 > 安全电子邮件 > 配置**
 - 单击**应用程序 > 安全挂起打印作业 > 配置**
- 2 单击**导入或导出**。

使用应用程序

安全电子邮件

发送数字签名和加密的电子邮件

注意：

- 当使用手动登录时，请配置“智能卡验证客户端”验证设置以检索所有的用户信息。如需更多信息，请参阅 [智能卡验证客户端管理员指南](#)。
- 要发送电子邮件，请确认您已经将有效的电子邮件地址分配给帐户。

1 登录到打印机。

2 从打印机主屏幕，触摸应用程序图标。

3 将文档放入 ADF 进纸匣中，或放在扫描仪玻璃上。

4 键入收件人的电子邮件地址。使用逗号来分隔多个电子邮件地址。

5 如果需要，请配置其他电子邮件和扫描设置。

6 触摸**发送**。

7 数字签名或加密电子邮件。

注意：要数字签名电子邮件，您必须持有有效的数字签名证书，并使用智能卡登录。签名证书只能从智能卡使用。如需更多信息，请与您的系统管理员联系。

8 如果需要，请选择安全选项。

9 触摸**发送**。

10 如果出现加密错误，请执行下面的任一操作：

- 要将加密的电子邮件只发送给拥有加密证书的收件人，请选择**发送加密**。
- 要将未加密的电子邮件发送给所有收件人，请选择**发送未加密**。

11 触摸**发送**。

安全挂起打印作业

打印挂起作业

注意：

- 确认将标准打印作业转换为安全挂起打印作业。如需更多信息，请参阅[第 15 页上的“将打印作业转换为安全挂起打印作业”](#)。

- 当使用打印并挂起特性时，确认打印驱动程序支持它。如需更多信息，请参阅 *打印驱动程序帮助*。您可以从网站上下载用于 Windows 的 Lexmark 通用打印驱动程序和用于 Macintosh 的打印驱动程序：www.lexmark.com。

1 打开文档后，单击**文件 > 打印**。

2 选择打印机。

注意：如果需要，请配置打印设置。

3 如果需要，请打印并挂起特性。

a 选择打印并挂起特性。

- 对于 Windows 用户，单击**属性、首选项、选项或设置**，然后单击**打印并挂起**。
- 对于 Macintosh 用户，从选项菜单选择**打印并挂起**。

b 选择打印作业类型。

- **保留**—发送打印作业，并将它们保存在打印机内存中用于以后打印。
- **校验**—打印多副本打印作业的第一份副本以作检验。在打印或取消剩余的副本之前，将它们一直挂起。
- **重复**—立即打印作业并将一份副本保存在打印机内存中，以便以后打印更多的副本。

注意：安全挂起打印作业应用程序不支持保密打印作业。

c 从关联到打印作业的 LDAP 目标键入用户名。

4 单击**确定或打印**。

5 从打印机主屏幕，登录到您的帐户，然后触摸应用程序图标。

注意：

- 确认在登录到打印机和发送打印作业时都使用同一个帐户。
- 根据应用程序的配置，打印释放队列中的所有作业可能在您触摸应用程序图标时自动打印。如需更多信息，请参阅第 15 页上的 [“配置安全挂起打印作业设置”](#)。

6 如果出现提示，请输入您的验证凭证。

7 选择您要打印的一个或多个作业，然后指定要打印的份数。

8 触摸**打印**。

疑难解答

应用程序错误

请尝试下列办法中的一个或多个：

检查诊断日志

- 1 打开 Web 浏览器，然后键入 **IP/se**，其中 **IP** 是打印机 IP 地址。
- 2 单击**嵌入式解决方案**，然后执行下列操作：
 - a 清除日志文件。
 - b 将日志级别设置为**是**。
 - c 生成日志文件。
- 3 分析日志，然后解决问题。

注意：解决问题之后，将日志级别设置为**否**。

联系 Lexmark 代表

登录问题

无法检测到读卡器或智能卡

请尝试下列办法中的一个或多个：

确认读卡器已正确连接到打印机

确认读卡器和智能卡兼容

确认读卡器被支持

如需支持的读卡器列表，请参阅 *自述文件*。

确认读卡器驱动程序已经安装在打印机上

联系 Lexmark 代表

用户被锁定

请尝试下列办法中的一个或多个：

增加允许登录失败的次数和锁定时间

注意：此解决方案仅在某些打印机型号中适用。

- 1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录限制**。
- 2 增加允许登录失败的次数和锁定时间。
- 3 单击**保存**。

注意：在锁定时间过去之后，新设置生效。

重置或更换智能卡

无法验证 PIN 码

请尝试下列办法中的一个或多个：

确认您输入的 **PIN** 码是正确的

联系系统管理员

无法手动登录

请尝试下列办法中的一个或多个：

确认在 **Kerberos** 配置中指定的域是正确的

在手动登录设置中指定域

如需更多信息，请参阅[第 12 页上的“配置手动登录设置”](#)。

联系系统管理员

打印机主屏幕不锁定

请尝试下列办法中的一个或多个：

确认“显示定制”已启用

如需更多信息，请参阅[显示定制管理员指南](#)。

保护对主屏幕的访问

如需更多信息，请参阅[第 9 页上的“保护对主屏幕的访问”](#)。

验证问题

Kerberos 验证失败

请尝试下列办法中的一个或多个：

检查诊断日志

- 1 打开 Web 浏览器，然后键入 **IP/se**，其中 **IP** 是打印机 IP 地址。
- 2 单击**嵌入式解决方案**，然后执行下列操作：
 - a 清除日志文件。
 - b 将日志级别设置为**是**。
 - c 生成日志文件。
- 3 分析日志，然后解决问题。

注意：分析日志之后，将日志级别设置为**否**。

确认配置文件已经安装在打印机上

- 如果您使用简单 Kerberos 设置来创建 Kerberos 配置文件，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，确认领域、域控制器、域和超时值是**正确**的。
- 如果您使用设备 Kerberos 设置文件，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录方法**。
 - 2 从“网络帐户”部分，单击**Kerberos > 查看文件**。
 - 3 如果没有安装 Kerberos 配置文件，请在“导入 Kerberos 文件”部分中，浏览适当的 krb5.conf 文件。
 - 4 单击**保存并校验**。

确认配置文件内容和格式是正确的

- 如果您使用简单 Kerberos 设置，请修改简单 Kerberos 设置的**设定**。
- 如果您使用设备 Kerberos 设置文件，请修改并重新安装文件。

确认 Kerberos 领域使用大写字母

- 如果您使用简单 Kerberos 设置，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，确认领域是**正确**的，并以**大写字母**键入。
 - 3 单击**应用**。
- 如果您使用设备 Kerberos 设置文件，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录方法**。
 - 2 从“网络帐户”部分，单击**Kerberos > 查看文件**。
 - 3 确认配置文件中的领域以**大写字母**键入。

指定 Microsoft® Windows® 操作系统域

- 如果您使用简单 Kerberos 设置，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，在“域”字段中，添加 Windows 域。
例如，如果“域”字段的值是 **DomainName, .DomainName**，而 Windows 域是 **x.y.z**，请将“域”字段值更改为 **DomainName, .DomainName, x.y.z**。
注意：域是区分大小写的。
 - 3 单击**应用**。
- 如果您使用设备 Kerberos 设置文件，请将输入项添加到文件的 **domain_realm** 部分中。以大写键入 Windows 域的领域，然后在打印机上重新安装文件。

联系 Lexmark 代表

无法从智能卡生成或读取证书信息

请尝试下列办法中的一个或多个：

确认智能卡上的证书信息是正确的

联系 Lexmark 代表

无法验证域控制器

请尝试下列办法中的一个或多个：

确认 Kerberos 配置文件中的领域、域控制器和域是正确的

- 如果您使用简单 Kerberos 设置，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，确认领域、域控制器和域是正确的。
- 如果您使用设备 Kerberos 设置文件，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 登录方法**。
 - 2 从“网络帐户”部分，单击**Kerberos > 查看文件**。
 - 3 确认领域、域控制器和域是正确的。

增加域控制器的超时值

- 如果您使用简单 Kerberos 设置，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，在“超时”字段中，输入从 3 至 30 秒的值。
 - 3 单击**应用**。

- 如果您使用设备 Kerberos 设置文件，请输入从 3 至 30 秒的值。当您完成后，请在打印机上重新安装文件。如需有关配置智能卡设置的更多信息，请参阅[第 12 页上的“配置智能卡设置”](#)。

确认域控制器可用

使用逗号来分隔多个值。域控制器按列出的顺序进行验证。

确认打印机和域控制器之间的端口 88 未被阻止

无法验证域控制器证书

请尝试下列办法中的一个或多个：

确认安装在打印机上的证书是正确的

如需更多信息，请参阅[第 7 页上的“手动安装证书”](#)。

确认域控制器验证方法配置正确

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“智能卡设置”部分，在“域控制器验证”菜单中，选择适当的验证方法。
- 3 单击应用。

在 Kerberos 配置文件中找不到领域

添加或更改领域

- 如果您使用简单 Kerberos 设置，请执行下列操作：
 - 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
 - 2 从“简单 Kerberos 设置”部分，在“领域”字段中，添加或更改领域。领域必须以大写字母键入。
注意：简单 Kerberos 设置不支持多个 Kerberos 领域输入项。如果需要多个领域，请安装包含所需领域的 Kerberos 配置文件。
 - 3 单击应用。
- 如果您使用设备 Kerberos 设置文件，请在文件中添加或更改领域。领域必须以大写字母键入。当您完成后，请在打印机上重新安装文件。

域控制器和设备时钟不同步

确认打印机和域控制器之间的时差不超过 5 分钟

如需更多信息，请参阅[第 8 页上的“设置日期和时间”](#)。

无法验证域控制器证书链

请尝试下列办法中的一个或多个：

确认链验证所需的所有证书已经安装在打印机上并且信息是正确的

如需更多信息，请参阅[第 7 页上的“手动安装证书”](#)。

确认证书链是从域控制器到根 CA

确认所有证书都没有过期

- 1 从“嵌入式 Web 服务器”，单击**设置 > 安全 > 证书管理**。
- 2 确认“有效期自”和“有效期至”日期没有过期。

即使一个或多个证书的状态未知，也允许用户登录

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“在线证书状态协议 (OCSP)”部分，选择**允许未知状态**。
- 3 单击**应用**。

联系 Lexmark 代表

无法连接到 OCSP 响应者

请尝试下列办法中的一个或多个：

确认 OCSP 响应者 URL 是正确的

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“在线证书状态协议 (OCSP)”部分，确认响应者 URL 是正确的。
- 3 单击**应用**。

增加响应者超时值

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“在线证书状态协议 (OCSP)”部分，在“响应者超时”字段中，输入从 5 至 30 的值。
- 3 单击**应用**。

无法对 OCSP 响应者验证域控制器证书

请尝试下列办法中的一个或多个：

确认 OCSP 响应者 URL 和响应者证书配置正确

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“在线证书状态协议 (OCSP)”部分，在“响应者 URL”字段中，指定以下设置：
 - OCSP 响应者或中继器的 IP 地址或主机名
 - 使用的端口号例如：`http://x:y`，其中 `x` 是 IP 地址，而 `y` 是端口号。
- 3 在“响应者证书”字段中，浏览适当的证书。
- 4 单击应用。

确认域控制器返回正确的证书

确认 OCSP 响应者验证正确的域控制器证书

无法访问打印机上的单独应用程序和功能

请尝试下列办法中的一个或多个：

允许对应用程序或功能的安全访问

如需更多信息，请参阅第 9 页上的 [“保护对单独应用程序和功能的访问”](#)。

如果用户属于一个 Active Directory 组，请确认该组被授权访问应用程序和功能

安全电子邮件问题

无法使用应用程序发送电子邮件

确认“设备配额”应用程序已被禁用

从“嵌入式 Web 服务器”，单击应用程序 > 设备配额 > 停止。

无法检索用户电子邮件地址

请尝试下列办法中的一个或多个：

确认打印机电子邮件功能受到保护

如需更多信息，请参阅第 9 页上的 [“保护对打印机的访问”](#)。

确认用户电子邮件地址被正确检索

- 1 从“嵌入式 Web 服务器”，导览至“智能卡验证客户端”的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“高级设置”部分，在“电子邮件发件人地址”菜单中，选择打印机检索用户电子邮件地址的位置。
- 3 选择等待用户信息。
- 4 单击应用。

联系 Lexmark 代表

无法检索用户签名证书

请尝试下列办法中的一个或多个：

确认签名证书可供用户使用

在用户的智能卡上安装适当的签名证书。

确认证书被正确检索

- 1 从“嵌入式 Web 服务器”，导览至“智能卡验证客户端”的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“高级设置”部分，选择等待用户信息。
- 3 单击应用。

联系 Lexmark 代表

签名证书对用户不可用

请尝试下列操作之一：

发送没有数字签名的电子邮件

确认签名证书可供用户使用

在用户的智能卡上安装适当的签名证书。

联系系统管理员

无法从 LDAP 服务器检索证书

请尝试下列办法中的一个或多个：

确认网络电缆是否连接牢固并且打印机的网络设置是否配置正确

如需更多信息，请参阅打印机用户指南。

确认服务器和防火墙设置配置为允许打印机和 LDAP 服务器之间通过端口 389 或端口 636 通信
如果您使用 SSL，请使用端口 636。否则，使用端口 389。

确认 LDAP 服务器地址包含主机名，而不是 IP 地址

如需更多信息，请参阅第 8 页上的 [“配置 LDAP 网络帐户设置”](#)。

如果 LDAP 服务器需要 SSL，请确认 SSL 设置是正确的

如需更多信息，请参阅第 8 页上的 [“配置 LDAP 网络帐户设置”](#)。

将 LDAP 搜索库缩小到包含所有必需用户的最低可能范围

确认所有 LDAP 属性是正确的

联系系统管理员

无法为一个或多个收件人加密电子邮件

请尝试下列办法中的一个或多个：

将未加密的电子邮件发送给没有加密证书的收件人，而将加密的电子邮件发送给拥有加密证书的收件人
选择**发送到全部**。如需更多信息，请参阅第 16 页上的 [“发送数字签名和加密的电子邮件”](#)。

将加密的电子邮件只发送给拥有加密证书的收件人

选择**发送加密**。如需更多信息，请参阅第 16 页上的 [“发送数字签名和加密的电子邮件”](#)。

将未加密的电子邮件发送给所有收件人

选择**发送未加密**。如需更多信息，请参阅第 16 页上的 [“发送数字签名和加密的电子邮件”](#)。

联系 Lexmark 代表

无法连接到电子邮件服务器

请尝试下列办法中的一个或多个：

确认打印机已连接到域

如需更多信息，请参阅第 8 页上的 [“配置 TCP/IP 码设置”](#)。

确认“SMTP 服务器验证”设置是正确的

- 1 从“嵌入式 Web 服务器”，单击**设置 > 电子邮件 > 电子邮件设置**。
- 2 在“SMTP 服务器验证”菜单中，执行下列操作之一：
 - 如果 SMTP 服务器需要用户凭证，请选择 **Kerberos 5**。
 - 如果不支持 Kerberos，请选择**不要求验证**。

- 如果 SMTP 服务器要求验证但不支持 Kerberos，请在“答复地址”字段中，键入打印机 IP 地址或主机名。

3 单击保存。

注意：如需更多信息，请参阅[第 10 页上的“配置 SMTP 设置”](#)。

如果 SMTP 服务器使用 Kerberos，请确认主要和次要 SMTP 网关的主机名是正确的

- 1** 从“嵌入式 Web 服务器”，单击**设置 > 电子邮件 > 电子邮件设置**。
- 2** 在“主要 SMTP 网关”和“次要 SMTP 网关”字段中，键入网关的主机名而不是 IP 地址。
- 3** 单击**保存**。

确认服务器和防火墙设置配置为允许打印机和 SMTP 服务器之间通过端口 25 通信

确认网络电缆是否连接牢固并且打印机的网络设置是否配置正确

如需更多信息，请参阅[打印机用户指南](#)。

联系系统管理员

无法发送副本给自己

请尝试下列办法中的一个或多个：

确认在登录会话中输入所有用户信息

确认打印机被配置为检索所有用户信息

- 1** 从“嵌入式 Web 服务器”，浏览至“智能卡验证客户端”的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2** 从“高级设置”部分，选择**等待用户信息**。
- 3** 单击**应用**。

确认“发送电子邮件到私人信箱”配置正确

如需更多信息，请参阅[第 11 页上的“配置发送电子邮件到私人信箱”](#)。

联系 Lexmark 代表

安全挂起打印作业问题

无法确定用户 ID

此错误指出本地帐户、网络帐户或验证模块登录方法没有为会话设置用户 ID。请尝试下列办法中的一个或多个：

确认应用程序是安全的

如需更多信息，请参阅[第 15 页上的“配置安全挂起打印作业设置”](#)。

确认会话用户 ID 设置正确

从嵌入式网页服务器，执行下列操作之一：

使用本地帐户登录方法

- 1 单击**设置 > 安全 > 登录方法**。
- 2 从“本地帐户”部分，单击本地帐户类型，然后确认帐户有用户名。
- 3 单击**保存**。

使用网络帐户登录方法

- 1 单击**设置 > 安全 > 登录方法**。
- 2 从“网络帐户”部分，单击网络帐户，然后确认帐户有正确的用户 ID。如需更多信息，请与您的系统管理员联系。
- 3 单击**保存**。

使用验证模块

- 1 单击**应用程序**。
- 2 选择验证模块，然后单击**配置**。
- 3 为会话用户 ID 指定适当的设置。
- 4 单击**保存或应用**。

请联系您的解决方案提供商

如果您仍然不能解决问题，请联系您的解决方案提供商。

没有用户可用的打印作业

请尝试下列办法中的一个或多个：

确认作业发送到正确的打印机并且没有过期

用户可能将作业发送到不同的打印机，或者作业可能由于没有及时打印已被自动删除。

确认会话用户 ID 设置正确

从嵌入式网页服务器，执行下列操作之一：

使用本地帐户登录方法

- 1 单击**设置 > 安全 > 登录方法**。
- 2 从“本地帐户”部分，单击本地帐户类型，然后确认帐户有用户名。
- 3 单击**保存**。

使用网络帐户登录方法

- 1 单击**设置 > 安全 > 登录方法**。
- 2 从“网络帐户”部分，单击网络帐户，然后确认帐户有正确的用户 ID。如需更多信息，请与您的系统管理员联系。
- 3 单击**保存**。

使用验证模块

- 1 单击**应用程序**。
- 2 选择验证模块，然后单击**配置**。
- 3 为会话用户 ID 指定适当的设置。
- 4 单击**保存或应用**。

请联系您的解决方案提供商

如果您仍然不能解决问题，请联系您的解决方案提供商。

LDAP 问题

LDAP 查询失败

请尝试下列办法中的一个或多个：

确认服务器和防火墙设置配置为允许打印机和 LDAP 服务器之间通过端口 389 和端口 636 通信

如果在您的网络中不使用反向 DNS 查询，请在 Kerberos 设置中禁用它

- 1 从“嵌入式 Web 服务器”，单击**设置 > 安全**。
- 2 从“网络帐户”部分，单击**Kerberos**。
- 3 从“杂项设置”部分，选择**禁用反向 IP 查询**。
- 4 单击**保存并校验**。

如果 LDAP 服务器需要 SSL，请为 LDAP 查询启用 SSL

- 1 从“嵌入式 Web 服务器”，导览至应用程序的配置页：
应用程序 > 智能卡验证客户端 > 配置
- 2 从“高级设置”部分，选择将**SSL 用于用户信息**。
- 3 单击**应用**。

将 **LDAP** 搜索库缩小到包含所有必需用户的最低可能范围

确认所有 **LDAP** 属性是正确的

许可证错误

联系 **Lexmark** 代表

注意事项

版本注意事项

2017 年 8 月

以下文字如果与当地法律法规有所冲突，可能并不适用于那些地区：LEXMARK INTERNATIONAL, INC.以其现状提供此手册，并没有任何保证（不论明示的或暗示的），包括，但不限于以其特定目的进行销售及适用的暗示保证。某些司法管辖区并不准许在某些交易中排除明示的或暗示的保证；因此，这份声明可能并不适用于你方。

本手册中可能会有技术上的不准确或印刷错误。鉴于此，本手册中的内容会阶段性地更新；这些改动将会体现在以后的版本中。产品或程序有可能会随时改动，如有改动，恕不另行通知。

本手册中提到的有关产品、程序或服务并不意味着生产厂商打算将这些产品、程序或服务向所有的国家提供，也不意味着只能使用此产品、程序或服务。任何功能一样的产品、程序或服务，只要不侵犯现有的知识产权，都可以用来替换使用。与其他的产品、程序或服务（除厂商明确标明外）共同操作并进行评估与验证是用户的责任。

如需 Lexmark 技术支持，请访问 <http://support.lexmark.com>。

如需有关耗材和下载的信息，请访问 www.lexmark.com。

© 2016 Lexmark International, Inc.

保留所有权利。

商标

Lexmark 和 Lexmark 徽标是 Lexmark International, Inc. 在美国和/或其他国家的商标或注册商标。

Microsoft、Windows 和 Active Directory 是微软集团公司在美国和其他国家的注册商标或商标。

所有其他商标的所有权属于它们各自的所有者。

索引

A

- 安全标记
 - 配置 14
- 安全的应用程序或功能
 - 在主屏幕上显示 10
- 安全电子邮件
 - 配置 14
- 安全挂起打印作业
 - 从打印机使用 16
- 安全证书
 - 手动安装 7
 - 自动安装 7

B

- 保护
 - 打印机功能 9
 - 电子邮件功能 9
 - 挂起作业 9
 - 应用程序 9
 - 主屏幕 9
- 保留打印作业 16
- 部署准备查对表 6

C

- 查对表
 - 部署准备 6
- 查看 Kerberos 配置文件 20
- 超时
 - 自动 7
- 重复打印作业 16

D

- DNS 设置
 - 配置 8
- 打印并挂起
 - 启用 16
- 打印挂起作业 16
- 打印机电子邮件设置
 - 配置 10
- 打印机主屏幕不锁定 19
- 打印作业
 - 转换为安全挂起打印作业 15
- 导出配置文件 15
- 导入配置文件 15
- 登录屏幕设置
 - 配置 12

- 电子邮件
 - 发送 10
 - 发送数字签名的 16
- 电子邮件功能
 - 保护 9
- 电子邮件和扫描设置
 - 配置 11
- 电子邮件加密
 - 配置 14

F

- 发送电子邮件到私人信箱 11
 - 配置 11
- 发送电子邮件时出现错误
 - 无法从 LDAP 服务器检索证书 25
- 发送加密的电子邮件 16
- 发送数字签名的电子邮件 16
- 访问控制 9
- 访问“嵌入式 Web 服务器” 7

G

- 概述 5
- 高级设置
 - 配置 13
- 功能
 - 保护 9
- 挂起打印作业
 - 类型 16
 - 删除 16
 - 释放 16
- 挂起打印作业的类型 16
- 挂起作业
 - 保护 9
 - 打印 16
 - 限制用户查看 15
- 挂起作业图标
 - 移除 15

J

- 加密
 - 配置 14
- 加密电子邮件
 - 发送 16
- 简单 Kerberos 设置 12
- 将打印作业转换为安全挂起打印作业 15

K

- Kerberos 设置 12
- Kerberos 验证失败 20

L

- LDAP 查询失败 29
- LDAP 网络帐户
 - 配置 8
 - 添加 8
- 链验证 12

M

- 没有发现加密证书 26
- 没有发现领域 22
- 没有发现签名证书 25
- 没有检测到读卡器 18
- 没有为一个或多个收件人发现加密证书 26
- 没有用户可用的打印作业 28

O

- OCSP 响应者连接错误 23
- OCSP 验证 12

P

- PIN 码验证错误 19
- 配置发送电子邮件到私人信箱 11
- 配置手动登录 12
- 配置文件
 - 导入或导出 15
- 配置应用程序 15
- 配置智能卡设置 12
- 屏幕超时
 - 设置 7

Q

- 签名证书对用户不可用 25
- 嵌入式 Web 服务器
 - 访问 7
- 缺少 Kerberos 领域 22

R

- 日期和时间设置
 - 配置 NTP 8
 - 手动配置 8

