



# Markvision Enterprise

版本 4.2

---

## 管理员指南

2022 年 9 月

[www.lexmark.com](http://www.lexmark.com)

---

# 目录

|                               |    |
|-------------------------------|----|
| 修改记录.....                     | 7  |
| 概述.....                       | 11 |
| 理解 MarkVision Enterprise..... | 11 |
| 开始.....                       | 12 |
| 最佳实践.....                     | 12 |
| 系统要求.....                     | 14 |
| 支持的语言.....                    | 15 |
| 支持的打印机型号.....                 | 15 |
| 设置数据库.....                    | 18 |
| 设置 run-as 用户.....             | 18 |
| 安装 MVE.....                   | 19 |
| 无提示安装 MVE.....                | 19 |
| 访问 MVE.....                   | 22 |
| 更改语言.....                     | 22 |
| 更改密码.....                     | 22 |
| 维护应用程序.....                   | 23 |
| 升级到 MVE 4.2.....              | 23 |
| 备份和还原数据库.....                 | 23 |
| 安装后更新安装程序设置.....              | 26 |
| 设置用户访问.....                   | 27 |
| 概述.....                       | 27 |
| 理解用户角色.....                   | 27 |
| 管理用户.....                     | 28 |
| 启用 LDAP 服务器验证.....            | 28 |
| 安装 LDAP 服务器证书.....            | 30 |
| 发现打印机.....                    | 31 |
| 创建发现配置文件.....                 | 31 |
| 管理发现配置文件.....                 | 33 |
| 示例场景：发现打印机.....               | 33 |

|                         |           |
|-------------------------|-----------|
| <b>管理安全仪表板.....</b>     | <b>35</b> |
| 概述.....                 | 35        |
| 访问安全仪表板.....            | 35        |
| 管理设备安全信息.....           | 35        |
| 管理设备一致性检查.....          | 35        |
| <b>查看打印机.....</b>       | <b>37</b> |
| 查看打印机列表.....            | 37        |
| 查看打印机信息.....            | 40        |
| 导出打印机数据.....            | 40        |
| 管理视图.....               | 41        |
| 更改打印机列表视图.....          | 43        |
| 使用搜索栏筛选打印机.....         | 43        |
| 管理关键字.....              | 43        |
| 使用保存搜索.....             | 43        |
| 理解打印机生命周期状态.....        | 43        |
| 运行保存搜索.....             | 45        |
| 创建保存搜索.....             | 45        |
| 理解搜索规则设置.....           | 46        |
| 管理保存搜索.....             | 49        |
| 示例场景：监控设备群的碳粉水平.....    | 49        |
| <b>保护打印机通信.....</b>     | <b>51</b> |
| 理解打印机安全状态.....          | 51        |
| 使用默认配置保护打印机.....        | 51        |
| 理解权限和功能访问控制.....        | 53        |
| 配置打印机安全性.....           | 54        |
| 保护设备群中的打印机通信.....       | 55        |
| 保护打印机的其他方法.....         | 55        |
| <b>管理打印机.....</b>       | <b>56</b> |
| 重新启动打印机.....            | 56        |
| 查看打印机“嵌入式 Web 服务器”..... | 56        |
| 审核打印机.....              | 56        |
| 更新打印机状态.....            | 56        |
| 设置打印机状态.....            | 56        |
| 分配配置到打印机.....           | 57        |

|                                      |           |
|--------------------------------------|-----------|
| 取消配置分配.....                          | 57        |
| 执行配置.....                            | 57        |
| 检查打印机与配置的一致性.....                    | 58        |
| 部署文件到打印机.....                        | 58        |
| 更新打印机固件.....                         | 59        |
| 从打印机卸载应用程序.....                      | 59        |
| 分配事件到打印机.....                        | 59        |
| 分配关键字到打印机.....                       | 60        |
| 将凭证输入到安全打印机.....                     | 60        |
| 手动配置默认的打印机证书.....                    | 60        |
| 移除打印机.....                           | 61        |
| <b>管理配置.....</b>                     | <b>62</b> |
| 概述.....                              | 62        |
| 创建配置.....                            | 62        |
| 从打印机创建配置.....                        | 64        |
| 示例场景：克隆配置.....                       | 65        |
| 从打印机创建高级安全组件.....                    | 65        |
| 生成配置设置的可打印版本.....                    | 66        |
| 理解动态设置.....                          | 66        |
| 理解变量设置.....                          | 66        |
| 配置彩色打印权限.....                        | 66        |
| 创建应用程序软件包.....                       | 67        |
| 导入或导出配置.....                         | 68        |
| 将文件导入资源库.....                        | 68        |
| <b>管理证书.....</b>                     | <b>69</b> |
| 设置 MVE 来自动管理证书.....                  | 69        |
| 理解自动证书管理特性 .....                     | 69        |
| 为自动证书管理配置 MVE .....                  | 71        |
| 使用 NDES 配置 Microsoft 企业 CA .....     | 72        |
| 通过 SCEP 使用 Microsoft 证书颁发机构管理证书..... | 73        |
| 概述 .....                             | 73        |
| 安装根 CA 服务器.....                      | 73        |
| 使用 NDES 配置 Microsoft 企业 CA .....     | 74        |
| 配置从属 CA 服务器 .....                    | 75        |
| 配置证书分发点和颁发机构信息访问设置.....              | 76        |
| 配置 CRL 可访问性.....                     | 77        |
| 配置 NDES 服务器 .....                    | 77        |

|                                        |            |
|----------------------------------------|------------|
| 为 MVE 配置 NDES.....                     | 78         |
| 通过 MSCEWS 使用 Microsoft 证书颁发机构管理证书..... | 80         |
| 系统要求.....                              | 80         |
| 网络连接性要求.....                           | 80         |
| 为 CEP 和 CES 服务器创建 SSL 证书.....          | 81         |
| 创建证书模板.....                            | 81         |
| 理解验证方法.....                            | 82         |
| 委派要求.....                              | 83         |
| 配置 Windows 集成身份验证.....                 | 84         |
| 配置客户端证书身份验证.....                       | 85         |
| 配置用户名密码身份验证.....                       | 88         |
| 通过 SCEP 使用 OpenXPKI 证书颁发机构管理证书.....    | 90         |
| 配置 OpenXPKI CA.....                    | 90         |
| 手动配置 OpenXPKI CA.....                  | 93         |
| 生成 CRL 信息.....                         | 97         |
| 配置 CRL 可访问性.....                       | 98         |
| 启用 SCEP 服务.....                        | 98         |
| 启用签名者代表（注册代理）证书.....                   | 99         |
| 在 OpenXPKI CA 中启用证书请求的自动批准.....        | 99         |
| 创建第二个领域.....                           | 100        |
| 允许同时存在具有相同主题的多个活动证书.....               | 102        |
| 为 OpenXPKI CA 设置默认端口号.....             | 103        |
| 在 OpenXPKI CA 中拒绝不带质询密码的证书请求.....      | 103        |
| 在证书中添加客户端身份验证 EKU.....                 | 103        |
| 当通过 SCEP 请求时获得完整的证书科目.....             | 103        |
| 吊销证书并发布 CRL.....                       | 104        |
| 通过 EST 使用 OpenXPKI 证书颁发机构管理证书.....     | 105        |
| 配置 OpenXPKI CA.....                    | 105        |
| 手动配置 OpenXPKI CA.....                  | 108        |
| 创建第二个领域.....                           | 114        |
| <b>管理打印机警报.....</b>                    | <b>119</b> |
| 概述.....                                | 119        |
| 创建操作.....                              | 119        |
| 理解操作占位符.....                           | 120        |
| 管理操作.....                              | 121        |
| 创建事件.....                              | 121        |
| 理解打印机警报.....                           | 122        |
| 管理事件.....                              | 126        |
| <b>查看任务状态和记录.....</b>                  | <b>127</b> |
| 概述.....                                | 127        |

|                                      |            |
|--------------------------------------|------------|
| 查看任务状态.....                          | 127        |
| 停止任务.....                            | 127        |
| 查看日志.....                            | 127        |
| 清除日志.....                            | 127        |
| 导出日志.....                            | 127        |
| <b>调度任务.....</b>                     | <b>128</b> |
| 创建时间表.....                           | 128        |
| 管理预定任务.....                          | 129        |
| <b>执行其他管理任务.....</b>                 | <b>130</b> |
| 配置常规设置.....                          | 130        |
| 配置电子邮件设置.....                        | 130        |
| 添加登录免责声明.....                        | 130        |
| 签署 MVE 证书.....                       | 131        |
| 移除用户信息和引用.....                       | 131        |
| <b>常见问题解答.....</b>                   | <b>133</b> |
| Markvision Enterprise 常见问题解答.....    | 133        |
| <b>疑难解答.....</b>                     | <b>136</b> |
| 用户已经忘记密码.....                        | 136        |
| 管理员用户已经忘记密码.....                     | 136        |
| 页面未加载.....                           | 137        |
| 不能发现网络打印机.....                       | 137        |
| 不正确的打印机信息.....                       | 137        |
| MVE 没有将打印机识别为安全打印机.....              | 137        |
| 对多个应用程序执行配置在第一次尝试中失败，但在随后的尝试中成功..... | 138        |
| 使用打印机证书执行配置失败.....                   | 138        |
| OpenXPKI 证书颁发机构.....                 | 139        |
| <b>附录.....</b>                       | <b>141</b> |
| <b>注意事项.....</b>                     | <b>144</b> |
| <b>术语表.....</b>                      | <b>146</b> |
| <b>索引.....</b>                       | <b>147</b> |

## 修改记录

### 2022 年 8 月

- 添加有关以下项目的信息：
  - Enrollment over Secure Transport (EST) 协议（如 RFC 7030 中所定义）
  - 安全仪表板
  - 发现过程中的关键字自动分配
  - 基于 SSL/TLS 的电子邮件支持
  - Windows Server 2022 支持
- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 通过“Microsoft 证书注册 Web 服务 (MSCEWS)”使用 Microsoft CA 管理证书
  - 配置 OpenXPki CA 服务器
  - 管理 MVE 配置

### 2022 年 3 月

- 更新有关支持的打印机型号的信息。
- 添加有关创建客户端证书的信息。

### 2021 年 5 月

- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 管理 Microsoft 证书颁发机构 (CA)
  - 为自动证书管理配置 Markvision™ Enterprise (MVE)
  - 使用“网络设备注册服务 (NDES)”配置 Microsoft 企业 CA
- 添加有关以下项目的信息：
  - 通过“Microsoft 证书注册 Web 服务 (MSCEWS)”使用 Microsoft CA 管理证书
  - 为“证书注册策略 Web 服务 (CEP)”和“证书注册 Web 服务 (CES)”服务器创建 SSL 证书
  - CEP 和 CES 的身份验证方法
  - 命名设备证书

### 2020 年 11 月

- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 支持的数据库
- 添加有关以下项目的信息：
  - 管理和部署配置
  - 备份和还原数据库
  - 使用 OpenXPki 和 Microsoft 证书颁发机构管理证书

- 添加对以下内容的支持：
  - 管理和部署配置到一组打印机型号
  - 创建自定义数据库名称

## 2020 年 2 月

- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 支持的服务器
  - 支持的数据库
  - 有效的 **MVE** 升级路径
- 添加有关以下项目的信息：
  - 最佳实践的说明
  - 管理自动证书的说明
  - 默认的高级安全组件及其设置
  - 保护打印机的其他方法
  - 示例场景

## 2019 年 6 月

- 更新有关以下项目的信息：
  - 为需要证书的打印机型号添加脚注
  - 在设置数据库时分配 **dbo** 权限
  - 升级到 **3.4** 版本时的有效升级路径
  - 备份和还原数据库时需要的文件
  - **LDAP** 服务器验证设置
  - 将证书有效性状态、日期和时区参数添加到搜索规则设置中
  - 在打印机安全设置中配置权限和功能访问控制
  - 更新打印机固件时，从资源库选择固件文件
  - 更新打印机固件时，选择开始日期、开始和暂停时间，以及每周的天数
  - 管理配置
- 添加有关以下项目的信息：
  - 理解打印机安全状态
  - 配置高级安全组件
  - 从打印机创建高级安全组件
  - 生成配置设置的可打印版本
  - 上载打印机设备群证书颁发机构
  - 移除用户信息和引用
  - 理解权限和功能访问控制
  - 对多个应用程序执行配置失败时的故障排除步骤
  - 管理员用户忘记密码时的故障排除步骤



## 2018 年 8 月

- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 设置数据库
  - 升级到 MVE 3.3
  - 常见问题解答
  - 创建操作
  - 创建时间表
- 添加有关以下项目的信息：
  - 设置 run-as 域用户帐户
  - 导出日志
  - 当 MVE 不能识别安全打印机时的故障排除步骤

## 2018 年 7 月

- 更新有关升级到 MVE 3.2 的信息。

## 2018 年 4 月

- 更新有关以下项目的信息：
  - 支持的打印机型号
  - 设置数据库
  - 备份和还原数据库文件
  - 用于访问 MVE 的 URL
  - 理解变量设置
- 添加有关以下项目的信息：
  - 配置打印机证书
  - 停止任务
  - 更新打印机固件

## 2017 年 9 月

- 更新有关以下项目的信息：
  - 系统要求
  - MVE 与 Lexmark™ 表单打印机 2580、2581、2590 和 2591 型号之间的通信
  - Microsoft SQL Server 数据库的手动删除
  - 备份和还原数据库文件
  - 当部署固件和解决方案文件到打印机时，功能访问控制的必需安全设置
  - 当部署应用程序时对许可证的支持
  - 打印机警报及其相关操作
  - 打印机状态自动恢复
  - 事件和关键字分配

## 2017 年 6 月

- MVE 3.0 的初始文档发布。

## 概述

### 理解 MarkVision Enterprise

MarkVision™ Enterprise (MVE) 是为 IT 专业人员设计，基于 Web 的打印机管理实用程序软件。

使用 MVE，您可以通过执行以下操作在企业环境中有效地管理大型打印机设备群：

- 查找、组织和跟踪打印机设备群。您可以审核打印机以收集打印机数据，如状态、设置和耗材。
- 创建配置并将它们分配给打印机。
- 将固件、打印机证书、证书颁发机构 (CA) 和应用程序部署到打印机。
- 监视打印机事件和警报。

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。

本文档供管理员使用。

# 开始

## 最佳实践

本主题概述使用 MVE 有效管理设备群的建议步骤。

### 1 在您的环境中安装 MVE。

#### a 使用最新的 Windows Server 环境创建服务器。

相关内容：

[Web 服务器要求](#)

#### b 创建不具有管理员访问权限的域用户帐户。

相关内容：

[设置 run-as 用户](#)

#### c 创建 Microsoft SQL Server 数据库，设置加密，然后为新的用户帐户提供数据库访问权限。

相关内容：

- [数据库要求](#)
- [设置数据库](#)

#### d 使用域用户帐户和带 Windows 身份验证的 SQL 服务器安装 MVE。

相关内容：

[安装 MVE](#)

### 2 设置 MVE，然后发现和组织设备群。

#### a 签署服务器证书。

相关内容：

- [签署 MVE 证书](#)
- [设置 MVE 来自动管理证书](#)

#### b 设置 LDAP 设置。

相关内容：

- [启用 LDAP 服务器验证](#)
- [安装 LDAP 证书](#)

#### c 连接到电子邮件服务器。

相关内容：

[配置电子邮件设置](#)

#### d 发现设备群。

相关内容：

[发现打印机](#)

#### e 预定审核和状态更新。

相关内容：

- [审核打印机](#)
- [更新打印机状态](#)

**f** 设置基本设置，如联系人名称、位置、资产标签和时区。

**g** 组织设备群。使用关键字（如位置）对打印机进行分类。

相关内容：

- [分配关键字到打印机](#)
- [创建保存搜索](#)

### 3 保护设备群。

**a** 使用默认的高级安全组件保护打印机访问。

相关内容：

- [使用默认配置保护打印机](#)
- [理解权限和功能访问控制](#)
- [保护打印机的其他方法](#)

**b** 创建一个包含证书的安全配置。

相关内容：

- [创建配置](#)
- [将文件导入资源库](#)

**c** 在当前设备群上执行配置。

相关内容：

- [分配配置到打印机](#)
- [执行配置](#)

**d** 预定执行和一致性检查。

相关内容：

[创建时间表](#)

**e** 将配置添加到发现配置文件以保护新打印机。

相关内容：

[创建发现配置文件](#)

**f** 签署打印机证书。

相关内容：

[签署 MVE 证书](#)

### 4 保持固件为最新。

相关内容：

[更新打印机固件](#)

### 5 安装和配置应用程序。

相关内容：

- [创建配置](#)
- [将文件导入资源库](#)

### 6 监控设备群。

相关内容：

[创建保存搜索](#)

## 系统要求

MVE 作为 Web 服务器安装，可以通过网络中任何计算机上的 Web 浏览器进行访问。MVE 还使用数据库来存储有关打印机设备群的信息。以下列表是对 Web 服务器、数据库和用户系统的要求：

### Web 服务器要求

|       |                              |
|-------|------------------------------|
| 处理器   | 至少 2GHz 使用超线程技术 (HTT) 的双核处理器 |
| RAM   | 至少 4GB                       |
| 硬盘驱动器 | 至少 60GB                      |

注意：MVE、“Lexmark 文档流程解决方案 (LDD)” 和 “设备部署实用程序 (DDU)” 不能在同一个服务器上运行。

### 支持的服务器

- Windows Server 2022 标准版
- Windows Server 2019
- Windows Server 2016 标准版
- Windows Server 2012 标准版
- Windows Server 2012 R2

注意：MVE 支持在本地环境中对受支持的服务器进行虚拟化。

### 数据库要求

#### 支持的数据库

- Firebird® 数据库（内置）
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

注意：建议的最小数据库大小是 60GB，以便为 FRAMEWORK 分配 20MB，为 MONITOR 和 QUARTZ 分配 4.5MB。如需更多信息，请参阅[第 18 页上的“设置数据库”](#)。

### 用户系统要求

#### 支持的 Web 浏览器

- Microsoft Edge
- Mozilla Firefox（最新版本）
- Google Chrome™（最新版本）
- Apple Safari（最新版本）

#### 屏幕分辨率

至少 1280 x 768 像素

## 支持的语言

- 巴西葡萄牙语
- 英语
- 法语
- 德语
- 意大利语
- 简体中文
- 西班牙语

## 支持的打印机型号

- Lexmark 6500
- Lexmark B2236<sup>2</sup>
- Lexmark B2338<sup>2</sup>、B2442<sup>2</sup>、B2546<sup>2</sup>、B2650<sup>2</sup>、B2865<sup>1</sup>
- Lexmark B3440<sup>2</sup>、B3442<sup>2</sup>
- Lexmark C2132
- Lexmark C2240<sup>2</sup>、C2325<sup>2</sup>、C2425<sup>2</sup>、C2535<sup>2</sup>
- Lexmark C2335<sup>2</sup>
- Lexmark C3224<sup>2</sup>
- Lexmark C3326<sup>2</sup>
- Lexmark C3426<sup>2</sup>
- Lexmark C4150<sup>2</sup>、C6160<sup>2</sup>、C9235<sup>2</sup>
- Lexmark C4342<sup>2</sup>、C4352<sup>2</sup>
- Lexmark C746、C748
- Lexmark C792
- Lexmark C925<sup>1</sup>、C950
- Lexmark CS310、CS410、CS510
- Lexmark CS317、CS417、CS517
- Lexmark CS331<sup>2</sup>
- Lexmark CS421<sup>2</sup>、CS521<sup>2</sup>、CS622<sup>2</sup>
- Lexmark CS431<sup>2</sup>
- Lexmark CS531<sup>2</sup>、CS632<sup>2</sup>
- Lexmark CS720<sup>2</sup>、CS725<sup>2</sup>
- Lexmark CS727<sup>2</sup>、CS728<sup>2</sup>
- Lexmark CS730<sup>2</sup>
- Lexmark CS735<sup>2</sup>
- Lexmark CS820<sup>2</sup>、CS827<sup>2</sup>
- Lexmark CS921<sup>2</sup>、CS923<sup>2</sup>、CS927<sup>2</sup>
- Lexmark CS943<sup>2</sup>
- Lexmark CX310、CX410、CX510

- Lexmark CX317、CX417、CX517
- Lexmark CX331<sup>2</sup>
- Lexmark CX421<sup>2</sup>、CX522<sup>2</sup>、CX622<sup>2</sup>、CX625<sup>2</sup>
- Lexmark CX431<sup>2</sup>
- Lexmark CX532<sup>2</sup>
- Lexmark CX625<sup>2</sup>
- Lexmark CX635<sup>2</sup>
- Lexmark CX725<sup>2</sup>
- Lexmark CX728<sup>2</sup>
- Lexmark CX730<sup>2</sup>
- Lexmark CX735<sup>2</sup>
- Lexmark CX820<sup>2</sup>、CX825<sup>2</sup>、CX827<sup>2</sup>、CX860<sup>2</sup>
- Lexmark CX920<sup>2</sup>、CX921<sup>2</sup>、CX922<sup>2</sup>、CX923<sup>2</sup>、CX924<sup>2</sup>、CX927<sup>2</sup>
- Lexmark CX930<sup>2</sup>、CX931<sup>2</sup>
- Lexmark CX942<sup>2</sup>、CX943<sup>2</sup>、CX944<sup>2</sup>
- Lexmark Forms Printer 2580<sup>4</sup>、2581<sup>4</sup>、2590<sup>4</sup>、2591<sup>4</sup>
- Lexmark M1140、M1145、M3150
- Lexmark M1242<sup>2</sup>、M1246<sup>2</sup>、M3250<sup>2</sup>、M5255<sup>2</sup>、M5265<sup>2</sup>、M5270<sup>2</sup>
- Lexmark M3350<sup>2</sup>
- Lexmark M5155、M5163、M5170
- Lexmark M5255<sup>2</sup>、M5265<sup>2</sup>、M5270<sup>2</sup>
- Lexmark MB2236<sup>2</sup>
- Lexmark MB2338<sup>2</sup>、MB2442<sup>2</sup>、MB2546<sup>2</sup>、MB2650<sup>2</sup>、MB2770<sup>2</sup>
- Lexmark MB3442<sup>2</sup>
- Lexmark MC2325<sup>2</sup>、MC2425<sup>2</sup>、MC2535<sup>2</sup>、MC2640<sup>2</sup>
- Lexmark MC3224<sup>2</sup>
- Lexmark MC3326<sup>2</sup>
- Lexmark MC3426<sup>2</sup>
- Lexmark MS310、MS312、MS315、MS410、MS415、MS510、MS610
- Lexmark MS317、MS417、MS517
- Lexmark MS321<sup>2</sup>、MS421<sup>2</sup>、MS521<sup>2</sup>、MS621<sup>2</sup>、MS622<sup>2</sup>
- Lexmark MS331<sup>2</sup>、MS431<sup>2</sup>
- Lexmark MS531<sup>2</sup>、MS631<sup>2</sup>、MS632<sup>2</sup>
- Lexmark MS617、MS817、MS818
- Lexmark MS710、MS711、MS810、MS811、MS812
- Lexmark MS725<sup>2</sup>、MS821<sup>2</sup>、MS822<sup>2</sup>、MS823<sup>2</sup>、MS824<sup>2</sup>、MS825<sup>2</sup>、MS826<sup>2</sup>
- Lexmark MS911
- Lexmark MX310、MX410、MX510、MX511、MX610、MX611
- Lexmark MX317、MX417、MX517
- Lexmark MX321<sup>2</sup>、MX421<sup>2</sup>、MX521<sup>2</sup>、MX522<sup>2</sup>、MX622<sup>2</sup>



- Lexmark MX331<sup>2</sup>、MX431<sup>2</sup>
- Lexmark MX432<sup>2</sup>
- Lexmark MX532<sup>2</sup>、MX632<sup>2</sup>
- Lexmark MX617、MX717、MX718
- Lexmark MX6500
- Lexmark MX710、MX711、MX810、MX811、MX812
- Lexmark MX721<sup>2</sup>、MX722<sup>2</sup>、MX725<sup>2</sup>、MX822<sup>2</sup>、MX824<sup>2</sup>、MX826<sup>2</sup>
- Lexmark MX910、MX911、MX912
- Lexmark MX931<sup>2</sup>
- Lexmark T650<sup>1</sup>、T652<sup>1</sup>、T654<sup>1</sup>、T656<sup>1</sup>
- Lexmark X651<sup>1</sup>、X652<sup>1</sup>、X654<sup>1</sup>、X656<sup>1</sup>、X658<sup>1</sup>、XS651<sup>1</sup>、XS652<sup>1</sup>、XS654<sup>1</sup>、XS658<sup>1</sup>
- Lexmark X746、X748、X792
- Lexmark X850<sup>1</sup>、X852<sup>1</sup>、X854<sup>1</sup>、X860<sup>1</sup>、X862<sup>1</sup>、X864<sup>1</sup>、XS864<sup>1</sup>
- Lexmark X925、X950、X952、X954
- Lexmark XC2130、XC2132
- Lexmark XC2235<sup>2</sup>、XC2240<sup>2</sup>、XC4240<sup>2</sup>
- Lexmark XC2335<sup>2</sup>
- Lexmark XC4140<sup>2</sup>、XC4150<sup>2</sup>、XC6152<sup>2</sup>、XC8155<sup>2</sup>、XC8160<sup>2</sup>
- Lexmark XC9225<sup>2</sup>、XC9235<sup>2</sup>、XC9245<sup>2</sup>、XC9255<sup>2</sup>、XC9265<sup>2</sup>
- Lexmark XC9325<sup>2</sup>、XC9335<sup>2</sup>
- Lexmark XC9445<sup>2</sup>、XC9455<sup>2</sup>、XC9465<sup>2</sup>
- Lexmark XM1135、XM1140、XM1145、XM3150
- Lexmark XM1242<sup>2</sup>、XM1246<sup>2</sup>、XM3250<sup>2</sup>
- Lexmark XM3142<sup>2</sup>
- Lexmark XM3350<sup>2</sup>
- Lexmark XM5163、XM5170、XM5263、XM5270
- Lexmark XM5365<sup>2</sup>、XM5370<sup>2</sup>
- Lexmark XM7155、XM7163、XM7170、XM7263、XM7270
- Lexmark XM7355<sup>2</sup>、MX7365<sup>2</sup>、MX7370<sup>2</sup>
- Lexmark XM9145、XM9155、XM9165
- Lexmark XM9335<sup>2</sup>
- Lexmark XC2326
- Lexmark XC2326
- Lexmark XC4342<sup>2</sup>、XC4352<sup>2</sup>

<sup>1</sup> 打印机证书更新是必需的。在此版本中，Java 平台安全性和性能更新会消除对某些证书签名算法（如 MD5 和 SHA1）的支持。此更改可防止 MVE 使用某些打印机。如需更多信息，请参阅[帮助信息文档](#)。

<sup>2</sup> 必须在打印机上启用 SNMPv3 支持。

<sup>3</sup> 如果在打印机上设置了高级安全密码，那么 MVE 无法支持该打印机。

<sup>4</sup> MVE 无法与处于“未就绪”状态的 Lexmark 表单打印机 2580、2581、2590 和 2591 型号通信。只有当 MVE 先前已经与处于“就绪”状态的打印机通信时，通信才起作用。当出现错误或警告（如空的耗材）时，打印机可能处于“未就绪”状态。要更改状态，请解决错误或警告，然后按**就绪**。

## 设置数据库

您可以使用 Firebird 或 Microsoft SQL Server 作为后台数据库。下表可以帮助您决定要使用的数据库。

|       | Firebird                                                                             | Microsoft SQL Server                                                                    |
|-------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 服务器安装 | 必须安装在与 MVE 相同的服务器上。                                                                  | 能够从任何服务器运行。                                                                             |
| 通信    | 只锁定到 localhost。                                                                      | 通过静态端口或动态命名实例进行通信。<br>支持 SSL/TLS 与受保护的 Microsoft SQL 服务器通信。                             |
| 性能    | 显示大型设备群的性能问题。                                                                        | 显示大型设备群的最佳性能。                                                                           |
| 数据库大小 | 对于 FRAMEWORK，默认的数据库大小是 6MB，对于 MONITOR 和 QUARTZ 是 1MB。每添加一条打印机记录，FRAMEWORK 表格会增加 1KB。 | 对于 FRAMEWORK，默认的数据库大小是 20MB，对于 MONITOR 和 QUARTZ 是 4.5MB。每添加一条打印机记录，FRAMEWORK 表格会增加 1KB。 |
| 配置    | 在安装期间自动配置。                                                                           | 需要预安装设置。                                                                                |

如果您使用 Firebird，那么 MVE 安装程序会安装和配置 Firebird，不需要其他配置。

如果您使用 Microsoft SQL Server，请在安装 MVE 之前，执行以下操作：

- 允许应用程序自动运行。
- 设置网络库来使用 TCP/IP 套接字。
- 创建下列数据库：

**注意：**以下是默认的数据库名称。您还可以提供自定义的数据库名称。

- FRAMEWORK
- MONITOR
- QUARTZ

- 如果您使用命名实例，请将 Microsoft SQL Server Browser 服务设置为自动启动。否则，在 TCP/IP 套接字上设置一个静态端口。
- 创建一个拥有所有三个数据库的 dbowner 权限的用户帐户，MVE 用它来连接和设置数据库。如果用户是 Microsoft SQL Server 帐户，请在 Microsoft SQL Server 上启用 Microsoft SQL Server 和“Windows 身份验证”模式。

**注意：**卸载配置为使用 Microsoft SQL Server 的 MVE 不会删除已创建的表格或数据库。卸载之后，必须手动删除 FRAMEWORK、MONITOR 和 QUARTZ 数据库。

- 将 dbo 权限分配给数据库用户，然后将 dbo 架构设置为默认架构。

## 设置 run-as 用户

在安装期间，可以指定 MVE 作为本地系统帐户或者域用户帐户执行。作为 run-as 域用户帐户执行 MVE 可以提供更安全的安装。与本地系统帐户相比，域用户帐户拥有有限的权限。

|           | run-as 域用户帐户                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | run-as 本地系统 |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 本地系统权限    | <ul style="list-style-type: none"> <li>归档对以下内容的所有访问权限： <ul style="list-style-type: none"> <li><code>\$MVE_INSTALL/tomcat/logs</code></li> <li><code>\$MVE_INSTALL/tomcat/temp</code></li> <li><code>\$MVE_INSTALL/tomcat/work</code></li> <li><code>\$MVE_INSTALL/apps/library</code></li> <li><code>\$MVE_INSTALL/apps/dm-mve/picture</code></li> <li><code>\$MVE_INSTALL/./mve_truststore*</code></li> <li><code>\$MVE_INSTALL/jre/lib/security/cacerts</code></li> <li><code>\$MVE_INSTALL/apps/dm-mve/WEB-INF/ldap</code></li> <li><code>\$MVE_INSTALL/apps/dm-mve/download</code></li> </ul> </li> <li>其中 <code>\$MVE_INSTALL</code> 是 安装目录。</li> <li>Windows 特权: <code>LOGON_AS_A_SERVICE</code></li> </ul> | 管理员权限       |
| 数据库连接身份验证 | <ul style="list-style-type: none"> <li>使用 Microsoft SQL Server 的 Windows 身份验证</li> <li>SQL 身份验证</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | SQL 身份验证    |
| 配置        | 在安装之前必须配置域用户。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 在安装期间自动配置   |

如果将 MVE 设置为 run-as 域用户帐户，则在与 MVE 服务器相同的域中创建用户。

# 安装 MVE

- 1 将可执行文件下载到不包含任何空格的路径。
- 2 以管理员身份运行文件，然后按照计算机屏幕上的说明进行操作。

注意：

- 密码被散列并安全地存储。由于密码一旦存储就不能解密，因此请确认您记得密码，或者将它们存储在一个安全的位置。
- 如果您使用“Windows 身份验证”连接到 Microsoft SQL Server，那么在安装期间不会进行连接验证。确保指定执行 MVE windows 服务的用户在 Microsoft SQL Server 实例中具有相应的帐户。指定的用户必须拥有 FRAMEWORK、MONITOR 和 QUARTZ 数据库的 dbowner 权限。

# 无提示安装 MVE

无提示安装的数据库设置

| 设置                                                                       | 描述           | 值                                                                                                                                                     |
|--------------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--help</code>                                                      | 显示有效选项列表。    |                                                                                                                                                       |
| <code>--version</code>                                                   | 显示产品信息。      |                                                                                                                                                       |
| <code>--unattendedmodeui</code><br><code>&lt;unattendedmodeui&gt;</code> | 无人值守模式的用户界面。 | 默认: <b>none</b><br>允许: <ul style="list-style-type: none"> <li>• <b>none</b></li> <li>• <b>minimal</b></li> <li>• <b>minimalWithDialogs</b></li> </ul> |

| 设置                                                               | 描述               | 值                                                                                                                                                                                                                         |
|------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--optionfile &lt;optionfile&gt;</code>                     | 安装选项文件。          | 默认:                                                                                                                                                                                                                       |
| <code>--debuglevel &lt;debuglevel&gt;</code>                     | 调试信息的详细级别。       | 默认: <b>2</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>0</b></li> <li>• <b>1</b></li> <li>• <b>2</b></li> <li>• <b>3</b></li> <li>• <b>4</b></li> </ul>                                                       |
| <code>--mode &lt;mode&gt;</code>                                 | 安装模式。            | 默认: <b>win32</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>win32</b></li> <li>• <b>unattended</b></li> </ul>                                                                                                  |
| <code>--debugtrace &lt;debugtrace&gt;</code>                     | 调试文件名。           | 默认:                                                                                                                                                                                                                       |
| <code>--installer-language &lt;installer-language&gt;</code>     | 语言选择。            | 默认: <b>en</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>en</b></li> <li>• <b>es</b></li> <li>• <b>de</b></li> <li>• <b>fr</b></li> <li>• <b>it</b></li> <li>• <b>pt_BR</b></li> <li>• <b>zh_CN</b></li> </ul> |
| <code>--encryptionKey &lt;encryptionKey&gt;</code>               | 加密密钥。            | 加密密钥:<br>默认:                                                                                                                                                                                                              |
| <code>--prefix &lt;prefix&gt;</code>                             | 安装目录。            | 默认: <b>C:\Program Files</b>                                                                                                                                                                                               |
| <code>--mveLexmark_runas &lt;mveLexmark_runas&gt;</code>         | run-as 用户选项。     | 默认: <b>LOCAL_SYSTEM</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>LOCAL_SYSTEM</b></li> <li>• <b>SPECIFIC_USER</b></li> </ul>                                                                                 |
| <code>--serviceRunAsUsername &lt;serviceRunAsUsername&gt;</code> | run-as 用户名。      | 用户名:<br>默认:                                                                                                                                                                                                               |
| <code>--serviceRunAsPassword &lt;serviceRunAsPassword&gt;</code> | run-as 用户密码。     | 密码:<br>默认:                                                                                                                                                                                                                |
| <code>--mveLexmark_database &lt;mveLexmark_database&gt;</code>   | 数据库类型。           | 默认:<br>允许:<br><ul style="list-style-type: none"> <li>• <b>FIREBIRD</b></li> <li>• <b>SQL_SERVER</b></li> </ul>                                                                                                            |
| <code>--firebirdUsername &lt;firebirdUsername&gt;</code>         | Firebird 数据库用户名。 | 用户名:<br>默认:                                                                                                                                                                                                               |
| <code>--firebirdPassword &lt;firebirdPassword&gt;</code>         | Firebird 数据库密码。  | 密码:<br>默认:                                                                                                                                                                                                                |

| 设置                                                                                                 | 描述                          | 值                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--firebirdFWDbName</code><br><code>&lt;firebirdFWDbName&gt;</code>                           | FRAMEWORK 的 Firebird 数据库名称。 | 数据库名称:<br>默认: <b>FRAMEWORK</b>                                                                                                                                                          |
| <code>--firebirdMNDbName</code><br><code>&lt;firebirdMNDbName&gt;</code>                           | MONITOR 的 Firebird 数据库名称。   | 默认: <b>MONITOR</b>                                                                                                                                                                      |
| <code>--firebirdQZDbName</code><br><code>&lt;firebirdQZDbName&gt;</code>                           | QUARTZ 的 Firebird 数据库名称。    | 默认: <b>QUARTZ</b>                                                                                                                                                                       |
| <code>--databaseIPAddress</code><br><code>&lt;databaseIPAddress&gt;</code>                         | 数据库 IP 地址或主机名。              | IP 地址或主机名:<br>默认:                                                                                                                                                                       |
| <code>--databasePort</code><br><code>&lt;databasePort&gt;</code>                                   | 数据库端口号。                     | 端口号:<br>默认:                                                                                                                                                                             |
| <code>--instanceName</code><br><code>&lt;instanceName&gt;</code>                                   | 实例名称。                       | 实例名称:<br>默认:                                                                                                                                                                            |
| <code>--instanceIdentifier</code><br><code>&lt;instanceIdentifier&gt;</code>                       | 实例。                         | 默认: <b>databasePort</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>databasePort</b></li> <li>• <b>instanceName</b></li> </ul>                                                |
| <code>--databaseUsername</code><br><code>&lt;databaseUsername&gt;</code>                           | 数据库用户名。                     | 用户名:<br>默认:                                                                                                                                                                             |
| <code>--databasePassword</code><br><code>&lt;databasePassword&gt;</code>                           | 数据库密码。                      | 密码:<br>默认:                                                                                                                                                                              |
| <code>--sqlServerAuthenticationMethod</code><br><code>&lt;sqlServerAuthenticationMethod&gt;</code> | Microsoft SQL Server 验证方法。  | 默认:<br><b>sqlServerDbAuthentication</b><br>允许:<br><ul style="list-style-type: none"> <li>• <b>sqlServerDbAuthentication</b></li> <li>• <b>sqlServerWindowsAuthentication</b></li> </ul> |
| <code>--fWDbName &lt;fWDbName&gt;</code>                                                           | FRAMEWORK 的数据库名称。           | 数据库名称:<br>默认: <b>FRAMEWORK</b>                                                                                                                                                          |
| <code>--mNDbName &lt;mNDbName&gt;</code>                                                           | MONITOR 的数据库名称。             | 默认: <b>MONITOR</b>                                                                                                                                                                      |
| <code>--qZDbName &lt;qZDbName&gt;</code>                                                           | QUARTZ 的数据库名称。              | 默认: <b>QUARTZ</b>                                                                                                                                                                       |
| <code>--mveAdminUsername</code><br><code>&lt;mveAdminUsername&gt;</code>                           | 管理员用户名。                     | 用户名:<br>默认: <b>admin</b>                                                                                                                                                                |
| <code>--mveAdminPassword</code><br><code>&lt;mveAdminPassword&gt;</code>                           | 管理员密码。                      | 密码:<br>默认:                                                                                                                                                                              |

## 访问 MVE

要访问 MVE，请使用您在安装期间创建的登录凭证。您还可以设置其他登录方法，如 LDAP、Kerberos 或其他本地帐户。如需更多信息，请参阅[第 27 页上的“设置用户访问”](#)。

- 1 打开 Web 浏览器，然后键入 **https://MVE\_SERVER/mve/**，其中 **MVE\_SERVER** 是托管 MVE 的主机名或 IP 地址。
- 2 如果需要，请接受免责声明。
- 3 输入您的凭证。
- 4 单击**登录**。

### 注意：

- 登录后，确保更改在安全期间使用的默认管理员密码。如需更多信息，请参阅[第 22 页上的“更改密码”](#)。
- 如果 MVE 空闲超过 30 分钟，用户会被自动注销。

## 更改语言

- 1 打开 Web 浏览器，然后键入 **https://MVE\_SERVER/mve/**，其中 **MVE\_SERVER** 是托管 MVE 的主机名或 IP 地址。
- 2 如果需要，请接受免责声明。
- 3 在页面的右上角，选择语言。

## 更改密码

- 1 打开 Web 浏览器，然后键入 **https://MVE\_SERVER/mve/**，其中 **MVE\_SERVER** 是托管 MVE 的主机名或 IP 地址。
- 2 如果需要，请接受免责声明。
- 3 输入您的凭证。
- 4 单击**登录**。
- 5 在页面的右上角，单击您的用户名，然后单击**更改密码**。
- 6 更改密码。

# 维护应用程序

## 升级到 MVE 4.2

在开始升级之前，请执行以下操作：

- 备份数据库、应用程序和属性文件。如需更多信息，请参阅[第 23 页上的“备份和还原数据库”](#)。
- 如果需要，请提供自定义数据库名称。

如果要从 1.x 版本进行升级，请先升级到 2.0 版本，再分别升级到 3.3 和 4.0 版本，然后升级到 4.2 版本。策略迁移过程仅在升级到 MVE 2.0 时执行。

|         |                          |
|---------|--------------------------|
| 有效的升级路径 | 3.3 到 4.0 到 4.2          |
| 无效的升级路径 | 1.6.X 到 4.2<br>2.0 到 4.2 |

- 1 备份数据库和应用程序文件。任何升级或卸载都会造成不可恢复的数据丢失风险。如果升级失败，则可以使用备份文件将应用程序还原为以前的状态。

**警告—可能的损坏：**当升级 MVE 时，数据库会发生改变。不要还原从先前版本创建的数据库备份。

**注意：**如需更多信息，请参阅[第 23 页上的“备份和还原数据库”](#)。

- 2 将可执行文件下载到临时位置。

- 3 以管理员身份运行安装程序，然后按照计算机屏幕上的说明进行操作。

**注意：**

- 当您升级到 MVE 2.0 时，分配给打印机的策略被迁移到每一个打印机型号的单一配置中。例如，如果传真、复印、纸张和打印策略被分配给 X792 打印机，那么这些策略会被合并到 X792 配置中。此过程不可应用于未被分配给打印机的策略。MVE 生成日志文件，确认策略已成功迁移到配置。如需更多信息，请参阅[第 133 页上的“我可以在哪里找到日志文件？”](#)。
- 升级之后，请确认在再次访问应用程序之前清除浏览器缓存。
- 当 MVE 升级到 3.5 或更高版本时，高级安全组件将从它们所在的配置中分离出来。如果一个或多个高级安全组件相同，则会将它们组合到一个组件中。创建的高级安全组件将自动添加到高级安全组件库中。

## 备份和还原数据库

**注意：**执行备份和还原过程时可能会丢失数据。请确保正确地执行这些步骤。

### 备份数据库和应用程序文件

我们建议定期备份您的数据库。

- 1 停止 Firebird 服务和 Markvision Enterprise 服务。
- a 打开运行对话框，然后键入 **services.msc**。
  - b 用鼠标右键单击 **Firebird Guardian - DefaultInstance**，然后单击**停止**。
  - c 用鼠标右键单击 **Markvision Enterprise**，然后单击**停止**。

## 2 浏览安装 Markvision Enterprise 的文件夹。

例如: **C:\Program Files\**

## 3 备份应用程序和数据库文件。

### 备份应用程序文件

将以下文件复制到一个安全的存储库:

- Lexmark\mve\_encryption.jceks
- Lexmark\mve\_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

**注意:** 确保这些文件被正确存储。没有 mve\_encryption.jceks 文件中的加密密钥, 则无法恢复以加密格式存储在数据库和文件系统中的数据。

### 备份数据库文件

执行下面的任一操作:

**注意:** 以下文件使用默认的数据库名称。这些说明还适用于定制的数据库名称。

- 如果您使用 Firebird 数据库, 请将以下文件复制到一个安全的存储库。必须定期备份这些文件以避免数据丢失。

- Lexmark\Markvision Enterprise\firebird\security2.fdb

如果您使用自定义数据库名称, 请更新以下文件:

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf

- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB

- 如果您使用 Microsoft SQL Server, 请创建 FRAMEWORK、MONITOR 和 QUARTZ 的备份。  
如需更多信息, 请与您的 Microsoft SQL Server 管理员联系。

## 4 重新启动 Firebird 服务和 Markvision Enterprise 服务。

**a** 打开运行对话框, 然后键入 **services.msc**。

**b** 用鼠标右键单击 **Firebird Guardian - DefaultInstance**, 然后单击**重新启动**。

**c** 用鼠标右键单击 **Markvision Enterprise**, 然后单击**重新启动**。



## 还原数据库和应用程序文件

**警告—可能的损坏：**当您升级 MVE 时，数据库可能会改变。不要还原从先前版本创建的数据库备份。

### 1 停止 Markvision Enterprise 服务。

如需更多信息，请参阅[第 23 页上的“备份数据库和应用程序文件”](#)的[第 1 步](#)。

### 2 浏览安装 Markvision Enterprise 的文件夹。

例如：**C:\Program Files\**

### 3 还原应用程序文件。

使用您在备份过程中保存的文件替换下列文件：

- Lexmark\mve\_encryption.jceks
- Lexmark\mve\_truststore.p12
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\platform.properties
- Lexmark\Markvision Enterprise\apps\library
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\encryption.properties
- Lexmark\Markvision Enterprise\jre\lib\security\cacerts
- Lexmark\Markvision Enterprise\tomcat\conf\server.xml

**注意：**只有当新的 MVE 安装是相同的版本时，您才能将数据库备份还原为新的 MVE 安装。

### 4 还原数据库文件。

执行下面的任一操作：

- 如果您使用 Firebird 数据库，请替换您在备份过程中保存的以下文件：

**注意：**以下文件使用默认的数据库名称。此说明还适用于定制的数据数据库名称。

- Lexmark\Markvision Enterprise\firebird\security2.fdb

如果您使用自定义数据库名称，则以下文件也被还原：

- Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\database.properties
- Lexmark\Markvision Enterprise\apps\mve-data-service\WEB-INF\classes\application.yml
- Lexmark\Markvision Enterprise\firebird\aliases.conf
- Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB
- Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB
- Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB
- 如果您使用 Microsoft SQL Server，请联系您的 Microsoft SQL Server 管理员。

### 5 重新启动 Markvision Enterprise 服务。

如需更多信息，请参阅[第 23 页上的“备份数据库和应用程序文件”](#)的[第 4 步](#)。

## 安装后更新安装程序设置

“Markvision Enterprise 密码实用程序”允许您更新已在安装期间配置的 **Microsoft SQL Server** 设置，而无需重新安装 MVE。该实用程序还允许您更新 **run-as** 用户域帐户凭证，如用户名和密码。如果忘记了以前的管理员用户凭证，您还可以使用该实用程序创建另一个管理员用户。

- 1 浏览安装 Markvision Enterprise 的文件夹。

例如：**C:\Program Files\**

- 2 启动 Lexmark\Markvision Enterprise\ 目录中的 **mvepwdutility-windows.exe** 文件。

- 3 选择语言，然后单击**确定** > 下一步。

- 4 按照计算机屏幕上的说明进行操作。

# 设置用户访问

## 概述

MVE 让您将内部用户直接添加到 MVE 服务器或者 使用在 LDAP 服务器中注册的用户帐户。如需有关添加内部用户的更多信息，请参阅[第 28 页上的“管理用户”](#)。如需有关使用 LDAP 用户帐户的更多信息，请参阅[第 28 页上的“启用 LDAP 服务器验证”](#)。

当添加用户时，必须分配角色。如需更多信息，请参阅[第 27 页上的“理解用户角色”](#)。

在验证过程中，系统会检查 MVE 服务器中存在的内部用户的用户凭证。如果 MVE 无法验证用户身份，那么它会尝试验证 LDAP 服务器中的用户。如果在 MVE 服务器和 LDAP 服务器中同时存在用户名，则使用 MVE 服务器中的密码。

## 理解用户角色

MVE 用户可以分配到一个或多个角色。根据角色，用户可以执行以下任务：

- **管理员**—访问并执行所有菜单中的任务。他们还有管理权限，如添加用户到系统或配置系统设置。只有具有“管理员”角色的用户才能停止任何正在运行的任务，而不管启动任务的用户类型是什么。
- **打印机**
  - 管理发现配置文件。
  - 设置打印机状态。
  - 执行审核。
  - 管理类别和关键字。
  - 预定审核、数据导出以及打印机发现。
- **配置**
  - 管理配置，包括导入和导出配置文件。
  - 将文件上载到资源库。
  - 分配并执行配置到打印机。
  - 预定一致性检查和配置执行。
  - 部署文件到打印机。
  - 更新打印机固件。
  - 生成打印机证书签名请求。
  - 下载打印机证书签名请求。
- **事件管理器**
  - 管理操作和事件。
  - 分配事件到打印机。
  - 测试操作。
- **服务台**
  - 更新打印机状态。
  - 重新启动打印机。
  - 运行一致性检查。
  - 执行配置到打印机。

**注意：**

- MVE 中的所有用户可以查看打印机信息页，并管理保存搜索和视图。
- 如需有关分配用户角色的更多信息，请参阅[第 28 页上的“管理用户”](#)。

## 管理用户

- 1 在页面的右上角，单击 。
- 2 单击**用户**，然后执行下面的任何操作：

### 添加用户

- a 单击**创建**。
- b 键入用户名、用户 ID 和密码。
- c 选择角色。

**注意：**如需更多信息，请参阅[第 27 页上的“理解用户角色”](#)。

- d 单击**创建用户**。

### 编辑用户

- a 选择一个用户 ID。
- b 配置设置。
- c 单击**保存更改**。

### 删除用户

- a 选择一个或多个用户。
- b 单击**删除**，然后确认删除。

**注意：**在连续三次登录尝试失败后，用户帐户会被锁定。只有“管理员”用户能够重新激活用户帐户。如果“管理员”用户被锁定，系统会在 5 分钟后自动重新激活它。

## 启用 LDAP 服务器验证

LDAP 是一种基于标准的、跨平台的可扩展协议，它直接在 TCP/IP 上运行。它用于访问称为目录的专用数据库。

为避免维护多个用户凭证，您可以使用公司 LDAP 服务器来验证用户 ID 和密码。

作为先决条件，LDAP 服务器必须包含与所需用户角色相对应的用户组。如需更多信息，请参阅[第 27 页上的“理解用户角色”](#)。

- 1 单击页面右上角的 。
- 2 单击 **LDAP**，然后选择**启用用于验证的 LDAP**。
- 3 在 LDAP 服务器主机名字段中，键入执行验证的 LDAP 服务器的 IP 地址或主机名。

**注意：**如果要在 MVE 服务器和 LDAP 服务器之间使用加密通信，请使用完全合格域名 (FQDN)。

- 4 根据选择的加密协议，指定服务器端口号。

## 5 选择加密协议。

- 无
- **TLS** - 一种使用数据加密和证书验证来保护服务器和客户端之间通信的安全协议。如果选择了此选项，则在建立连接后会向 LDAP 服务器发送 **START\_TLS** 命令。如果希望通过端口 **389** 进行安全通信，请使用此设置。
- **SSL/TLS** - 一种使用公钥加密来验证服务器和客户端之间通信的安全协议。如果希望从 LDAP 绑定一开始就进行安全通信，请使用此选项。此选项通常用于端口 **636** 或其他安全 LDAP 端口。

## 6 选择绑定类型。

- **简单** - MVE 服务器为 LDAP 服务器生成指定的凭证，以便使用 LDAP 服务器查找工具。
  - a 键入绑定用户名。
  - b 键入绑定密码，然后确认密码。
- **Kerberos** - 要配置设置，请执行以下操作：
  - a 键入绑定用户名。
  - b 键入绑定密码，然后确认密码。
  - c 单击**选择文件**，然后浏览至 **krb5.conf** 文件。
- **SPNEGO** - 要配置设置，请执行以下操作：
  - a 键入服务主体名称。
  - b 单击**选择文件**，然后浏览至 **krb5.conf** 文件。
  - c 单击**选择文件**，然后浏览至 Kerberos 密钥表文件。

此选项仅用于配置“简单”和“受保护的 GSSAPI 协商机制 (SPNEGO)”以支持“单点登录”功能。

## 7 在高级选项部分中，配置以下内容：

- **搜索库** - 根节点的基本专有名称 (DN)。在 LDAP 社区服务器层次结构中，此节点必须是用户节点和组节点的祖先节点。例如，**dc=mvetest,dc=com**。
- 注意：**指定根 DN 时，请确保根 DN 仅包含 **dc** 和 **o**。如果 **ou** 或 **cn** 是用户节点和组节点的祖先节点，则在用户和组搜索库中使用 **ou** 或 **cn**。
- **用户搜索库** - LDAP 社区服务器中用户对象所在的节点。此节点位于用于列出所有用户节点的根 DN 下。例如，**ou=people**。
  - **用户搜索筛选器** - 用于在 LDAP 社区服务器中查找用户对象的参数。例如，**(uid={0})**。

### 允许有多个条件和复杂表达式的示例

| 登录凭证    | 在用户搜索筛选器字段中，键入                         |
|---------|----------------------------------------|
| 常用名     | <b>(CN={0})</b>                        |
| 登录名     | <b>(sAMAccountName={0})</b>            |
| 用户主体名称  | <b>(userPrincipalName={0})</b>         |
| 电话号码    | <b>(telephoneNumber={0})</b>           |
| 登录名或常用名 | <b>( (sAMAccountName={0})(CN={0}))</b> |

**注意：**唯一有效的模式是 **{0}**，这意味着 MVE 将搜索 MVE 用户登录名。

- **搜索用户库对象和整个子树** - 系统搜索用户搜索库下的所有节点。
- **组搜索库** - LDAP 社区服务器中包含与 MVE 角色对应的用户组的节点。此节点位于用于列出所有组节点的根 DN 下。例如，**ou=group**。

- **组搜索筛选器** - 用于在与 MVE 中的角色对应的组中查找用户的参数。

**注意：**只能使用 **{0}** 和 **{1}** 模式。如果使用了 **{0}**，则 MVE 将搜索 LDAP 用户 DN。如果使用了 **{1}**，则 MVE 将搜索 MVE 用户登录名。

- **组角色属性** - 键入组全名的 LDAP 属性。LDAP 属性具有特定含义并定义属性与字段名之间的映射。例如，LDAP 属性 **cn** 与全名字段相关联。LDAP 属性 **commonname** 也映射到全名字段。通常，该属性必须保留为默认值 **cn**。
- **搜索用户库对象和整个子树** - 系统搜索组搜索库下的所有节点。

**8** 在 LDAP 组到 MVE 角色映射部分中，键入与 MVE 角色对应的 LDAP 组的名称。

**注意：**

- 如需更多信息，请参阅[第 27 页上的“理解用户角色”](#)。
- 您可以将一个 LDAP 组分配给多个 MVE 角色。您还可以在角色字段中键入多个 LDAP 组，使用竖线字符 (|) 分隔多个组。例如，要为管理员角色包含 **admin** 和 **assets** 组，请在管理员角色的 LDAP 组字段中键入 **admin|assets**。
- 如果只想使用管理员角色，而不使用其他 MVE 角色，请将这些字段留空。

**9** 单击**保存更改**。

## 安装 LDAP 服务器证书

要在 MVE 服务器和 LDAP 服务器之间建立加密通信，MVE 必须信任 LDAP 服务器证书。在 MVE 架构中，当 MVE 与 LDAP 服务器进行身份验证时，MVE 是客户端，而 LDAP 服务器是对等服务器。

- 1** 在页面的右上角单击 .
- 2** 单击 **LDAP**，然后配置 LDAP 设置。如需更多信息，请参阅[第 28 页上的“启用 LDAP 服务器验证”](#)。
- 3** 单击**测试 LDAP**。
- 4** 输入有效的 LDAP 用户名和密码，然后单击**开始测试**。
- 5** 检查证书的有效性，然后接受它。

# 发现打印机

## 创建发现配置文件

使用发现配置文件在网络中查找打印机，并将它们添加到系统中。在发现配置文件中，执行以下任一操作以包括或排除 IP 地址或主机名列表：

- 一次添加一项
- 使用 TXT 或 CSV 文件导入项

您还可以为兼容的打印机型号自动分配和执行配置。配置必须包含可部署到打印机的打印机设置、应用程序、许可证、固件和 CA 证书。

- 1 从打印机菜单中，单击**发现配置文件 > 创建**。
- 2 在常规部分中，键入发现配置文件的唯一名称和描述，然后配置以下内容：
  - **超时** - 系统等待打印机响应的的时间。
  - **重试次数** - 系统尝试与打印机通信的次数。
  - **自动管理发现的打印机** - 新发现的打印机会自动设置为受管状态，并且在发现期间跳过“新”状态。
- 3 在地址部分中，执行以下任一操作：

### 添加地址

- a 选择**包括或排除**。
- b 键入 IP 地址、主机名、子网或 IP 地址范围。

Addresses

Include

+ Add

🗑 Delete

➡ Import

Examples: 10.20.xx.xx,  
2001:dbx::x:xmyprinter.domain.com, 2001:dbx:x:x:x:x,x

Search Address/Range

| <input type="checkbox"/> | Address/Range              | Include/Exclude |
|--------------------------|----------------------------|-----------------|
| <input type="checkbox"/> | 10.195.x.x-10.195.x.xx.xxx | Include         |

一次仅添加一项。使用以下格式的地址：

- **10.195.10.1**（单个 IPv4 地址）
- **myprinter.example.com**（单个主机名）
- **10.195.10.3-10.195.10.255**（IPv4 地址范围）
- **10.195.\*.\***（通配符）
- **10.195.10.1/22**（IPv4 无类域间路由或 CIDR 表示法）
- **2001:db8:0:0:0:0:2:1**（完整 IPv6 地址）
- **2001:db8::2:1**（压缩 IPv6 地址）

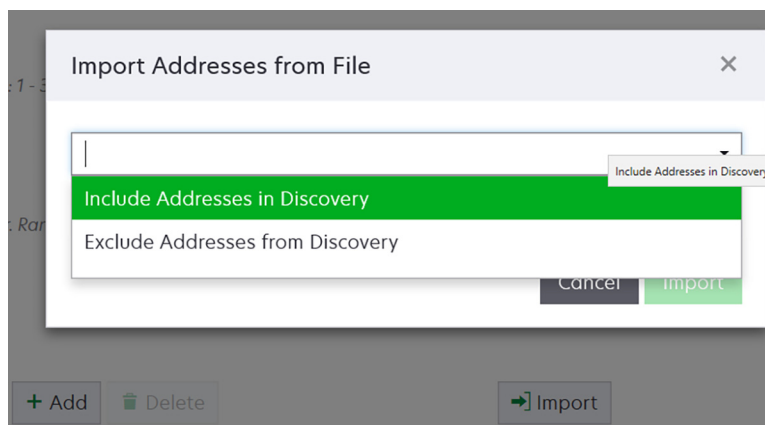
**注意：**如果为同一台打印机的 IPv6 和 IPv4 地址创建了不同的发现配置文件，则将显示最后发现的地址。例如，如果先使用 IPv6 发现打印机，随后使用 IPv4 再次发现打印机，则打印机列表中仅显示 IPv4 地址。

**c** 单击添加。

## 导入地址

**a** 单击导入。

**b** 选择在发现期间是包括还是排除 IP 地址。



**c** 浏览至包含地址列表的文本文件。每个地址项必须单独占一行。

示例文本文件

```
10.195.10.1 myprinter.example.com 10.195.10.3-10.195.10.255 10.195.*.*
10.195.10.1/22 2001:db8:0:0:0:0:2:1 2001:db8::2:1
```

**d** 单击导入。

**4** 从 **SNMP** 部分中，选择 **1 版本**、**2c 版本** 或 **3 版本**，然后设置访问权限。

**注意：**要使用 **SNMP 3** 版本发现打印机，请在打印机“嵌入式 **Web** 服务器”中创建用户名和密码，然后重新启动该打印机。如果无法建立连接，则重新发现打印机。如需更多信息，请参阅[嵌入式 \*\*Web\*\* 服务器管理员指南](#)。

**5** 如有必要，从输入凭证部分中，选择打印机使用的验证方法，然后输入凭证。

**注意：**此功能允许您在发现过程中与安全打印机建立通信。必须提供正确的凭证才能在安全打印机上执行任务，例如，审核、状态更新和固件更新。

**6** 如有必要，在分配配置部分中，将配置与打印机型号相关联。如需有关创建配置的信息，请参阅[第 62 页上的“创建配置”](#)。

**7** 如有必要，在分配关键字部分中，在发现过程中将关键字与打印机型号相关联。如需有关将关键字分配给打印机的信息，请参阅[第 60 页上的“分配关键字到打印机”](#)

**注意：**

- 对于通过此配置文件发现的所有打印机，都会为其分配新关键字。
- 新关键字将添加到已分配给打印机的现有关键字列表中。

**8** 单击保存配置文件或保存并运行配置文件。

**注意：**可以安排定期执行发现。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。



## 管理发现配置文件

1 从“打印机”菜单，单击**发现配置文件**。

2 执行下面的任何操作：

### 编辑配置文件

- a 选择一个配置文件，然后单击**编辑**。
- b 配置设置。
- c 单击**保存配置文件**或**保存并运行配置文件**。

### 复制配置文件

- a 选择一个配置文件，然后单击**复制**。
- b 配置设置。
- c 添加 IP 地址。如需更多信息，请参阅[第 31 页上的“添加地址”](#)。
- d 单击**保存配置文件**或**保存并运行配置文件**。

### 删除配置文件

- a 选择一个或多个配置文件。
- b 单击**删除**，然后确认删除。

### 运行配置文件

- a 选择一个或多个配置文件。
- b 单击**运行**。从“任务”菜单检查发现状态。

## 示例场景：发现打印机

ABC 公司是一家大型制造公司，占据了一幢 9 层大楼。该公司刚购买了 30 台新的利盟打印机，分布在 9 个楼层中。作为 IT 人员，您必须将这些新打印机添加到 MVE 中。打印机已经连接到网络，但是您不知道所有的 IP 地址。

您要保护财务部的以下新打印机。

**10.194.55.60**  
**10.194.56.77**  
**10.194.55.71**  
**10.194.63.27**  
**10.194.63.10**

### 示例实现

- 1 为财务部的打印机创建一个发现配置文件。
- 2 添加 5 个 IP 地址。
- 3 创建一个保护指定打印机的配置。
- 4 在发现配置文件中包含这些配置。

- 5 保存并运行配置文件。
- 6 为其余的打印机创建另一个发现配置文件。
- 7 使用通配符包括 IP 地址。使用以下格式：**10.194.\*.\***
- 8 排除财务部的 5 个打印机 IP 地址。
- 9 保存，然后运行该配置文件。

# 管理安全仪表板

## 概述

使用安全仪表板，您可以查看设备安全设置的运行状况。安全仪表板采用可视化方式表示各项安全设置，例如端口、协议、磁盘加密状态、设备管理员帐户和默认证书状态。它提供对设备群安全状况的可见性，有助于管理员识别和修复不合规的设置。

## 访问安全仪表板

- 1 在 MVE Web 门户中，单击**仪表板**。

**注意：**安全仪表板是管理员用户的默认登录页面。

- 2 单击下面的任一小组件：

- 设备安全信息
- 设备一致性检查

## 管理设备安全信息

此小组件汇总了设备群的安全视图。

- 1 单击图表的任意条形项以转到设备安全信息窗口。
- 2 将鼠标悬停在条形项上可查看以下详细信息：
  - 端口号
  - 相关打印机的数量
  - 是否开启/启用打印机设置
- 3 单击**打印**以获取可打印格式的详细视图。

**注意：**

- “设备安全信息”窗口为用户提供了“深入了解”功能。
- 通过单击图表中的任何条形项，用户可以导览到打印机列表页面的过滤视图。如需更多信息，请参阅[第 37 页上的“查看打印机列表”](#)。

## 管理设备一致性检查

此小组件汇总了设备群一致性检查的详细视图。

- 1 单击饼图的任何部分以转到设备一致性检查窗口。
- 2 从左窗格，应用日期范围过滤器。

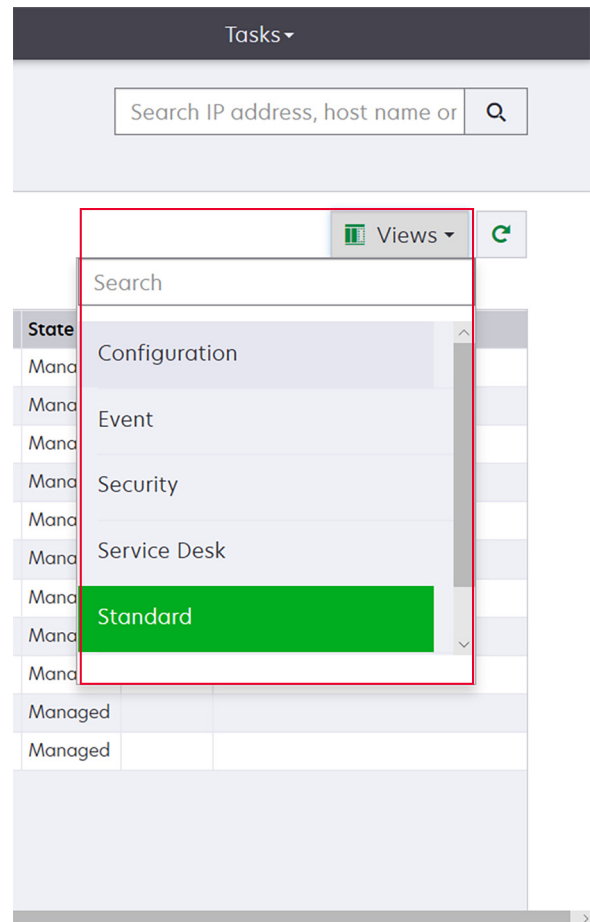
**注意：**默认范围为 7 天。
- 3 单击**打印**以获取可打印格式的详细视图。

**注意：**

- “设备一致性检查”窗口为用户提供了“深入了解”功能。
- 通过单击饼图的任何部分，用户可以导览到打印机列表页面的过滤视图。如需更多信息，请参阅[第 37 页上的“查看打印机列表”](#)。

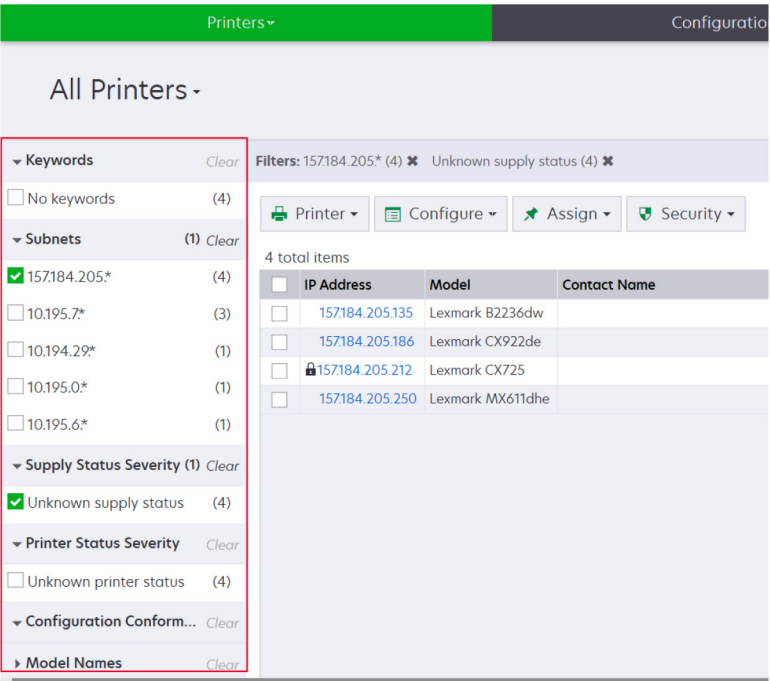


- 更改打印机列表视图。如需更多信息，请参阅[第 43 页上的“更改打印机列表视图”](#)。

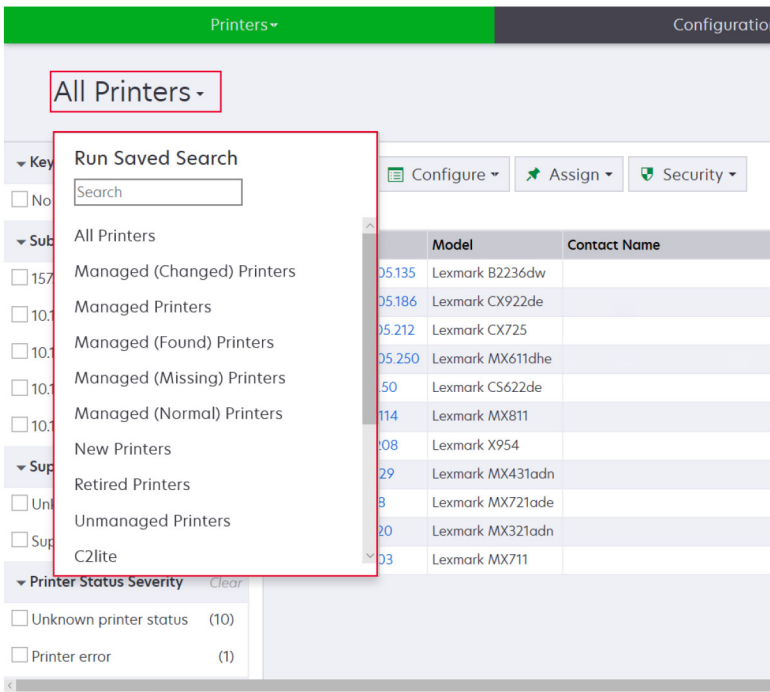


**注意：**如果您使用搜索框，那么应用程序会搜索系统中的所有打印机。忽略选定的过滤器和保存搜索。如果您运行保存搜索，那么使用保存搜索中指定的条件。忽略选定的过滤器和搜索框中键入的 IP 地址或主机名。您还可以使用过滤器来缩小当前搜索结果的范围。

— 使用过滤器。



— 运行保存搜索。如需更多信息，请参阅第 45 页上的“运行保存搜索”。



- 要对打印机进行排序，请从打印机列表单击任何列标题。打印机根据选定的列标题进行排序。
- 要查看有关打印机的更多信息，请调整列大小。将光标放在列标题的垂直边框上，然后将边框向左或向右拖动。

## 查看打印机信息

要查看完整的信息列表，请确保在打印机上执行了审核。如需更多信息，请参阅[第 56 页上的“审核打印机”](#)。

**1** 从打印机菜单，单击**打印机列表**。

**2** 单击打印机的 IP 地址。

**3** 查看以下信息：

- **状态**—打印机的状态。
- **耗材**—耗材详细信息和剩余耗材的百分比。
- **标识**—打印机网络标识信息。

**注意：**时区信息仅在某些打印机型号中可用。

- **日期**—打印机添加到系统的日期、发现日期和最近的审核日期。
- **固件**—打印机固件属性和代码级别。
- **功能**—打印机特性。
- **内存选件**—硬盘大小和用户闪存可用空间。
- **输入选项**—可用进纸匣的设置。
- **输出选项**—可用接纸架的设置。
- **eSF 应用程序**—有关打印机上已安装的“嵌入式解决方案框架 (eSF)”应用程序的信息。
- **打印机统计**—每一项打印机属性的特定值。
- **更改详细信息**—有关打印机更改的信息。

**注意：**此信息仅在处于“已托管（已更改）”状态的打印机中可用。如需更多信息，请参阅[第 43 页上的“理解打印机生命周期状态”](#)。

- **打印机凭证**—在分配给打印机的配置中使用的凭证。
- **打印机证书**—以下打印机证书的属性：

- 默认
- HTTPS
- 802.1x
- IPSec

**注意：**

- 此信息仅在某些打印机型号中可用。
- 一个即将到期的有效性状态指出到期日期，如系统配置下面的证书颁发机构部分所设置。
- **配置属性**—分配给打印机的配置的属性。
- **活动警报**—等待清除的打印机警报。
- **已分配的事件**—分配给打印机的事件。

## 导出打印机数据

MVE 允许您导出在当前视图中可用的打印机信息。

**1** 从打印机菜单，单击**打印机列表**。

**2** 选择一台或多台打印机。



3 单击打印机 > 导出数据。

注意：

- 导出的数据保存在 CSV 文件中。
- 导出数据可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

# 管理视图

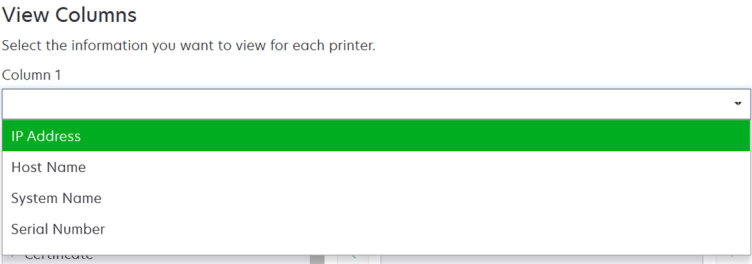
视图特性让您定制显示在打印机列表页中的信息。

1 从打印机菜单，单击视图。

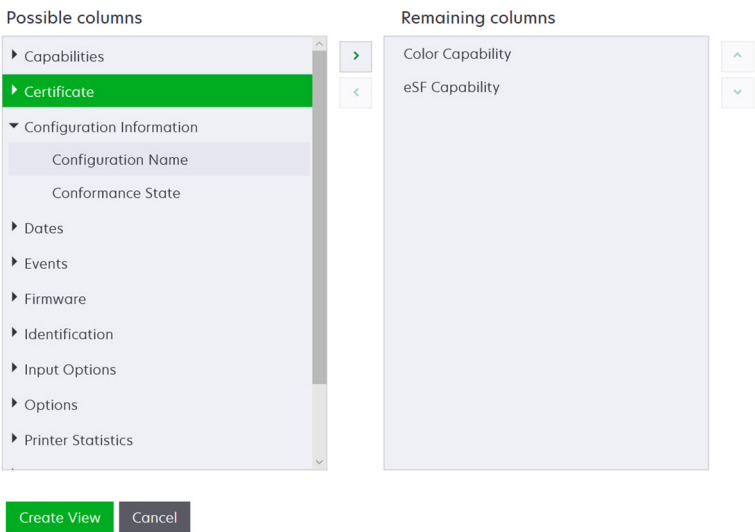
2 执行下面的任何操作：

## 创建视图

- a 单击**创建**。
- b 键入视图的唯一名称及其描述。
- c 从视图列部分，在列 1 菜单中，选择标识符列。



d 从可能的列部分，展开类别，选择要显示为列的信息，然后单击 >。



- **功能**—显示打印机是否支持选定特性。
- **证书**—显示打印机证书的创建日期、注册状态、到期日期、续订日期、修订号、证书主题、有效性和签名状态。
- **配置信息**—显示配置相关的打印机信息，如一致性、配置名称和状态。

- **日期**—显示上次审核、上次一致性检查、上次发现和打印机添加到系统的日期。
- **事件**—显示事件相关的打印机信息。
- **固件**—显示固件相关的信息，如固件版本。
- **标识**—显示有关打印机的信息，如 IP 地址、主机名和序列号。
- **输入选项**—显示有关输入选项的信息，如进纸匣大小和介质类型。
- **选件**—显示有关打印机选件的信息，如硬盘和闪存驱动器。
- **打印机统计**—显示有关打印机使用情况的信息，如打印或扫描的页数，以及传真作业的总数。
- **解决方案**—显示安装在打印机上的 eSF 应用程序及其版本号。
- **状态**—显示打印机和耗材状态。
- **耗材**—显示耗材相关的信息。
- **打印机端口**—显示端口相关的信息。

**注意：**端口值中的 **Unknown** 选项意味着该端口在打印机上不存在或者 MVE 无法检索该端口。

- **打印机安全选项**—显示 TLS 和密码信息。

**e** 单击**创建视图**。

## 编辑视图

- a** 选择一个视图。
- b** 单击**编辑**，然后编辑设置。
- c** 单击**保存更改**。

## 复制视图

- a** 选择一个视图。
- b** 单击**复制**，然后配置设置。
- c** 单击**创建视图**。

## 删除视图

- a** 选择一个或多个视图。
- b** 单击**删除**，然后确认删除。

## 设置默认视图

- a** 选择一个视图。
- b** 单击**设置为默认值**。

以下视图是系统生成的，不能编辑或删除：

- 配置
- 打印机列表
- 事件
- 安全
- 服务台
- 标准

## 更改打印机列表视图

如需更多信息，请参阅[第 41 页上的“管理视图”](#)。

- 1 从“打印机”菜单，单击**打印机列表**。
- 2 单击**视图**，然后选择一个视图。

## 使用搜索栏筛选打印机

当使用搜索栏来搜索打印机时，请注意以下事项。

- 要搜索 IP 地址，请确保键入完整的 IP 地址或范围。

例如：

- 10.195.10.1
- 10.195.10.3-10.195.10.255
- 10.195.\*.\*
- 2001:db8:0:0:0:0:2:1

- 如果搜索字符串不是完整的 IP 地址，则根据其主机名、系统名称或序列号来搜索打印机。
- 下划线字符 ( \_ ) 可以用作通配符。

## 管理关键字

关键字让您创建自定义标记并将它们分配给打印机。

- 1 从打印机菜单，单击**关键字**。
- 2 执行下面的任一操作：
  - 添加、编辑或删除类别。  
**注意：**类别将关键字组合在一起。
  - 添加、编辑或删除关键字。

如需有关分配关键字给打印机的信息，请参阅[第 60 页上的“分配关键字到打印机”](#)。

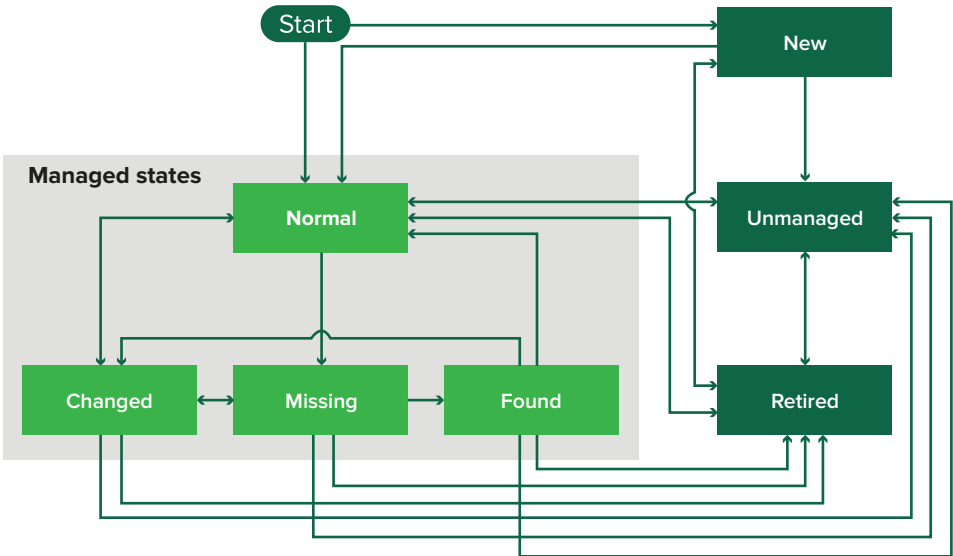
## 使用保存搜索

### 理解打印机生命周期状态

系统生成的保存搜索可以显示处于以下打印机生命周期状态中的打印机：

- **所有打印机**—系统中的所有打印机。
- **已托管的打印机**—出现的打印机可能是下面的任何状态：
  - 已托管（正常）
  - 已托管（已更改）
  - 已托管（缺少）
  - 已托管（已发现）

- **已托管（已更改）的打印机**—系统中在上次审核时其以下属性已经改变的打印机：
  - 属性标记
  - 主机名
  - 联系人名称
  - 联系人位置
  - 内存大小
  - 双面打印
  - 耗材（不含水平）
  - 输入选项
  - 输出选项
  - eSF 应用程序
  - 默认打印机证书
- **已托管（已发现）的打印机**—已报告为缺少，但是现在已经发现的打印机。
- **已托管（缺少）的打印机**—系统无法与之通信的打印机。
- **已托管（正常）的打印机**—系统中自上次审核以来其属性保持不变的打印机。
- **新打印机**—新发现并且没有自动设置为“已托管”状态的打印机。
- **报废的打印机**—系统中标记为不再活动的打印机。
- **未托管的打印机**—标记为从系统中执行的活动排除的打印机。



| 开始状态 | 结束状态            | 过渡                |
|------|-----------------|-------------------|
| 开始   | 正常              | 已发现。 <sup>1</sup> |
| 开始   | 新               | 已发现。 <sup>2</sup> |
| 任何   | “正常”、“未托管”或“报废” | 手动（“缺少”不更改为“正常”）。 |
| 报废   | 正常              | 已发现。 <sup>1</sup> |
| 报废   | 新               | 已发现。 <sup>2</sup> |

<sup>1</sup> 在发现配置文件中启用“自动管理已发现打印机”设置。

<sup>2</sup> 在发现配置文件中禁用“自动管理已发现打印机”设置。

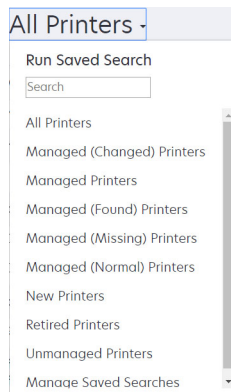
| 开始状态                                                                             | 结束状态 | 过渡             |
|----------------------------------------------------------------------------------|------|----------------|
| “正常”、“缺少”或“已发现”                                                                  | 已更改  | 当发现时是新地址。      |
| 正常                                                                               | 已更改  | 审核属性与数据库属性不匹配。 |
| “正常”、“已更改”或“已发现”                                                                 | 缺少   | 在审核或更新状态时没有发现。 |
| 已更改                                                                              | 正常   | 审核属性与数据库属性相匹配。 |
| 缺少                                                                               | 已发现  | 发现、审核或更新状态。    |
| 已发现                                                                              | 正常   | 发现、审核或更新状态。    |
| <sup>1</sup> 在发现配置文件中启用“自动管理已发现打印机”设置。<br><sup>2</sup> 在发现配置文件中禁用“自动管理已发现打印机”设置。 |      |                |

## 运行保存搜索

保存搜索是一组已保存的参数，它返回符合参数的最新打印机信息。

您可以创建并运行定制的保存搜索，或者运行默认的系统生成的保存搜索。系统生成的保存搜索可以显示处于其生命周期状态中的打印机。如需更多信息，请参阅[第 43 页上的“理解打印机生命周期状态”](#)。

- 1 从打印机菜单，单击**打印机列表**。
- 2 在下拉菜单中，选择一个保存搜索。



## 创建保存搜索

### 使用过滤器

- 1 从打印机菜单，单击**打印机列表**。
- 2 在页面的左边，选择过滤器。  
**注意：**选定的过滤器列在搜索结果标题的上方。
- 3 单击**保存**，然后键入保存搜索的唯一名称及其描述。
- 4 单击**创建保存搜索**。

## 使用“保存搜索”页面

- 1 从打印机菜单，单击**保存搜索 > 创建**。
- 2 从常规部分，键入保存搜索的唯一名称及其描述。
- 3 从规则和规则组部分，在匹配菜单中，指定搜索结果是否必须匹配所有规则或任何规则。
- 4 请执行下面的任一操作：

### 添加规则

- a 单击**添加规则**。
- b 为您的搜索规则指定参数、操作和值。如需更多信息，请参阅[第 46 页上的“理解搜索规则设置”](#)。

### 添加规则组

规则组可以包含规则的组合。如果匹配菜单设置为**任何规则和规则组**，那么系统会搜索匹配该规则组中所有规则的打印机。如果匹配菜单设置为**所有规则和规则组**，那么系统会搜索匹配该规则组中任何规则的打印机。

- a 单击**添加规则组**。
- b 为您的搜索规则指定参数、操作和值。如需更多信息，请参阅[第 46 页上的“理解搜索规则设置”](#)。
- c 要添加另一个规则，请单击**添加规则**。

- 5 单击**创建保存搜索**或**创建并运行保存搜索**。

## 理解搜索规则设置

使用下面的一个或多个参数搜索打印机：

| 参数                  | 描述             |
|---------------------|----------------|
| 资产标签                | 打印机上的资产标记设置的值。 |
| 证书创建日期 <sup>1</sup> | 创建证书的日期。       |

| 参数                   | 描述                                                                                                                                                                        |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 证书注册状态 <sup>1</sup>  | 证书的注册状态。                                                                                                                                                                  |
| 证书到期日期 <sup>1</sup>  | 证书到期的日期。                                                                                                                                                                  |
| 证书续订日期 <sup>1</sup>  | 续订证书的日期。                                                                                                                                                                  |
| 证书修订号 <sup>1</sup>   | 证书的修订号。                                                                                                                                                                   |
| 证书签名状态 <sup>1</sup>  | 证书的状态。                                                                                                                                                                    |
| 证书有效性状态 <sup>1</sup> | 证书的有效性。<br><b>注意：</b> 一个即将到期的状态指出证书会在 <b>30</b> 天内到期。                                                                                                                     |
| 彩色功能                 | 打印机以彩色或黑白色打印。                                                                                                                                                             |
| 配置                   | 分配给打印机的配置名称。                                                                                                                                                              |
| 配置一致性                | 打印机与指定配置的一致性状态。                                                                                                                                                           |
| 联系人位置                | 打印机上的联系人位置设置的值。                                                                                                                                                           |
| 联系人名称                | 打印机上的联系人名称设置的值。                                                                                                                                                           |
| 复印                   | 打印机支持复印功能。                                                                                                                                                                |
| 日期：已添加到系统            | 将打印机添加到系统中的日期。                                                                                                                                                            |
| 日期：上次审核              | 上次审核打印机的日期。                                                                                                                                                               |
| 日期：上次一致性检查           | 上次检查打印机配置一致性的日期。                                                                                                                                                          |
| 日期：上次发现              | 上次发现打印机的日期。                                                                                                                                                               |
| 磁盘加密                 | 打印机配置为磁盘加密。                                                                                                                                                               |
| 磁盘擦除                 | 打印机配置为磁盘擦除。                                                                                                                                                               |
| 双面打印                 | 打印机支持双面打印。                                                                                                                                                                |
| eSF 功能               | 打印机支持管理 eSF 应用程序。                                                                                                                                                         |
| eSF 信息               | 有关安装在打印机上的 eSF 应用程序的信息，如名称、状态和版本。                                                                                                                                         |
| 事件名称                 | 已分配事件的名称。                                                                                                                                                                 |
| 传真名称                 | 打印机上的传真名称设置的值。                                                                                                                                                            |
| 传真号码                 | 打印机上的传真号码设置的值。                                                                                                                                                            |
| 传直接收                 | 打印机支持接收传真。                                                                                                                                                                |
| 固件信息                 | 有关在打印机上安装的固件的信息。<br><ul style="list-style-type: none"> <li>名称—固件的名称。例如：<b>Base</b> 或 <b>Kernel</b>。</li> <li>版本—打印机固件版本。</li> </ul>                                       |
| 主机名                  | 打印机主机名。                                                                                                                                                                   |
| IP 地址                | 打印机 IP 地址。<br><b>注意：</b> 您可以在后三个八进制数中使用星号来搜索多个输入项。例如： <b>123.123.123.*</b> 、 <b>123.123.*.*</b> 、 <b>123.*.*.*</b> 、 <b>2001:db8::2:1</b> 和 <b>2001:db8:0:0:0:0:2:1</b> 。 |
| 关键字                  | 已分配的关键字。                                                                                                                                                                  |
| 使用寿命页计数              | 打印机的使用寿命页计数值。                                                                                                                                                             |
| MAC 地址               | 打印机 MAC 地址。                                                                                                                                                               |

| 参数         | 描述                                                                                 |
|------------|------------------------------------------------------------------------------------|
| 维护计数器      | 打印机维护计数器的值。                                                                        |
| 厂商         | 打印机厂商名称。                                                                           |
| 标记技术       | 打印机支持的标记技术。                                                                        |
| 多功能数码复合机功能 | 打印机是多功能数码复合机 (MFP)。                                                                |
| 型号         | 打印机型号名称。                                                                           |
| 模块化序列号     | 模块化序列号。                                                                            |
| 打印机状态      | 打印机状态。例如: <b>Ready</b> 、 <b>Paper Jam</b> 、 <b>Tray 1 Missing</b> 。                |
| 打印机状态严重性   | 打印机上出现的最严重状态的值。例如: <b>Unknown</b> 、 <b>Ready</b> 、 <b>Warning</b> 或 <b>Error</b> 。 |
| 配置文件       | 打印机支持配置文件。                                                                         |
| 扫描到电子邮件    | 打印机支持“扫描到电子邮件”。                                                                    |
| 扫描到传真      | 打印机支持“扫描到传真”。                                                                      |
| 扫描到网络      | 打印机支持“扫描到网络”。                                                                      |
| 安全通信状态     | 打印机安全性或验证状态。                                                                       |
| 序列号        | 打印机序列号。                                                                            |
| 状态         | 数据库中的当前打印机状态。                                                                      |
| 耗材状态       | 打印机耗材状态。                                                                           |
| 耗材状态严重性    | 打印机上出现的最严重耗材状态的值。例如: <b>Unknown</b> 、 <b>OK</b> 、 <b>Warning</b> 或 <b>Error</b> 。  |
| 系统名称       | 打印机系统名称。                                                                           |
| 时区         | 打印机所在地区的时区。                                                                        |
| TLI        | 打印机上的 TLI 设置的值。                                                                    |

<sup>1</sup> 证书相关的参数适用于以下设备证书:

- 默认
- HTTPS
- 802.1x
- IPSec

请在搜索打印机时使用下列运算符:

- 完全匹配—参数等于指定的值。
- 不是一参数不等于指定的值。
- 包含—参数包含指定的值。
- 不包含—参数不包含指定的值。
- 开头是一参数以指定的值开头。
- 结尾是一参数以指定的值结尾。
- 日期
  - 早于—用于搜索指定天数之前的天数的参数。
  - 在上次内—用于在今天之前的指定天数内搜索的参数。
  - 在下次内—用于在今天之后的指定天数内搜索的参数。



**注意：**要搜索具有带空值的参数的打印机，请使用 `_EMPTY_OR_NULL_`。例如，要搜索具有空的传真名称的打印机，请在值字段中键入 `_EMPTY_OR_NULL_`。

## 管理保存搜索

- 1 从“打印机”菜单，单击**保存搜索**。
- 2 执行下面的任何操作：

### 编辑保存搜索

- a 选择一个保存搜索，然后单击**编辑**。

**注意：**系统生成的保存搜索不能被编辑。如需更多信息，请参阅[第 43 页上的“理解打印机生命周期状态”](#)。

- b 配置设置。
- c 单击**保存更改**或**保存并运行**。

### 复制保存搜索

- a 选择一个保存搜索，然后单击**复制**。
- b 配置设置。
- c 单击**创建保存搜索**或**创建并运行保存搜索**。

### 删除保存搜索

- a 选择一个或多个保存搜索。

**注意：**系统生成的保存搜索不能被删除。如需更多信息，请参阅[第 43 页上的“理解打印机生命周期状态”](#)。

- b 单击**删除**，然后确认删除。

## 示例场景：监控设备群的碳粉水平

作为 ABC 公司的 IT 人员，您必须组织打印机设备群以方便地监控它们。您要监控打印机的碳粉使用情况，以确定耗材是否需要更换。

### 示例实现

- 1 创建一个保存搜索，检索其耗材有错误或警告的打印机。

保存搜索的示例规则

参数：**耗材状态严重性**  
操作：**不是**  
值：**耗材良好**

- 2 创建显示每台打印机的耗材状态、容量和水平的视图。

耗材视图中显示的示例列

**耗材状态**  
**黑色碳粉盒容量**  
**黑色碳粉盒水平**

青色碳粉盒容量  
青色碳粉盒水平  
品红色碳粉盒容量  
品红色碳粉盒水平  
黄色碳粉盒容量  
黄色碳粉盒水平

**3** 使用视图时运行保存搜索。

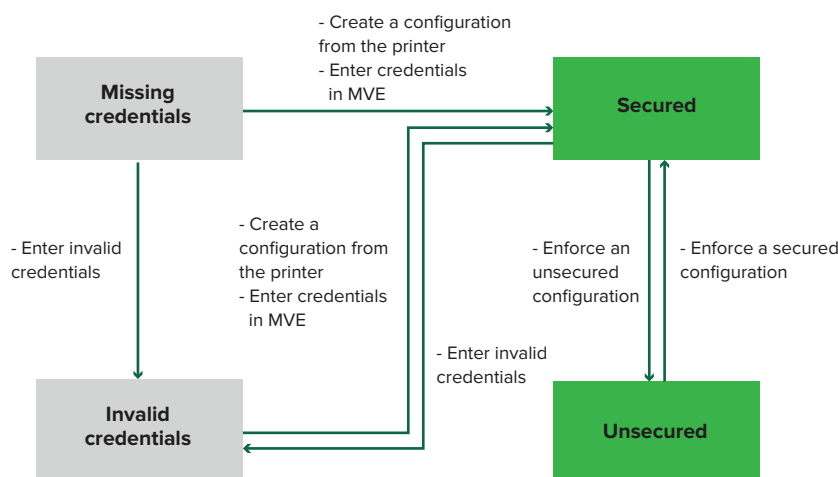
**注意：**打印机列表视图中显示的信息基于上次审核。执行审核和状态更新以获得当前的打印机状态。

# 保护打印机通信

## 理解打印机安全状态

在发现过程中，打印机可以处于下面任何一种安全状态：

- 不安全—MVE 不需要凭证来与设备通信。
-  安全—MVE 需要凭证，并且已提供凭证。
-  缺少凭证—MVE 需要凭证，但是没有提供凭证。
-  无效的凭证—MVE 需要凭证，但是提供了不正确的凭证。



在发现、审核、状态更新、一致性检查或配置执行期间发现凭证无效时，打印机处于无效的凭证状态。

仅在发现期间打印机不需要凭证时，打印机处于不安全状态。

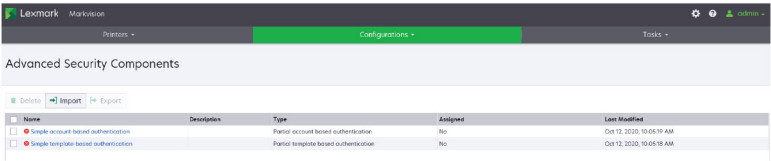
要将状态从不安全更改为安全，请执行安全配置。

要从缺少凭证或无效的凭证状态移出打印机，请在 **MVE** 中手动输入凭证或者从打印机创建配置。

## 使用默认配置保护打印机

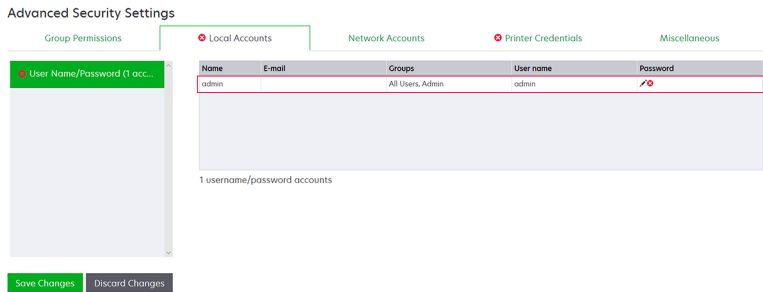
在某些打印机型号上，没有默认的管理员用户。“来宾”用户具有开放访问权限，并且没有登录。此设置授予用户访问所有打印机权限和访问控制的权限。**MVE** 通过默认配置处理此风险。全新安装后，将自动创建两个高级安全组件。每个组件都包含默认的安全设置和预配置的本地管理员帐户。您可以在创建配置时使用这些安全组件，然后将配置部署到新打印机并强制执行。

从配置菜单，单击**所有高级安全组件**。

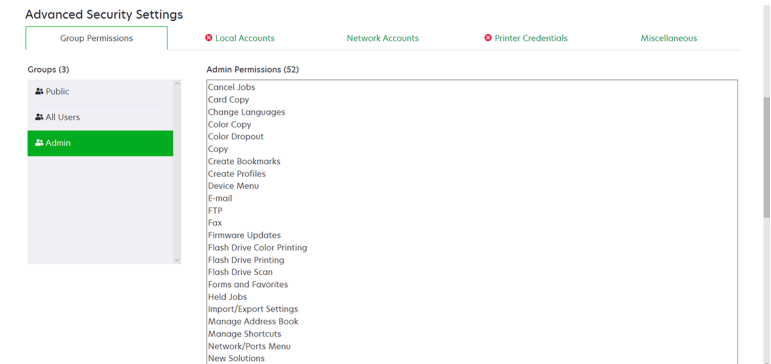


## 简单的基于帐户的身份验证

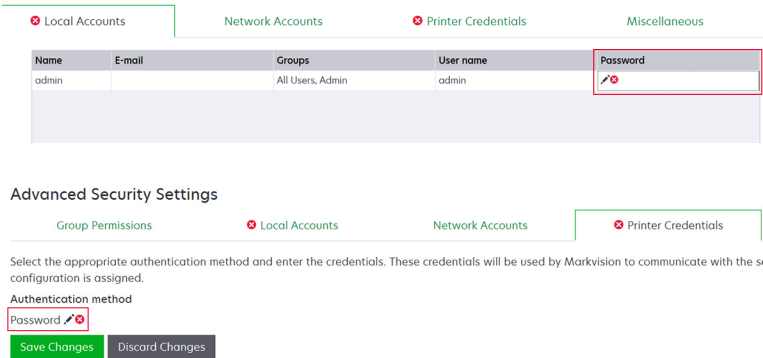
此安全组件包含称为**管理员**的用户名/密码 本地帐户。



**管理员**帐户是管理组的成员，其权限包括功能访问控制，以及保护打印机和限制公共访问的权限。如需更多信息，请参阅[第 53 页上的“理解权限和功能访问控制”](#)。



在将此组件添加到配置之前，请确保设置**管理员**密码和打印机凭证。



# 简单的基于模板的身份验证

此安全组件包含一个称为管理员密码保护的安全模板，配置有密码本地帐户。

Local Accounts

Network Accounts

Printer Credentials

Security Templates

Access Controls

Miscellaneous

Password (1 accounts)

| Name           | Admin Password | Password                 |
|----------------|----------------|--------------------------|
| Admin Password | Yes            | <input type="password"/> |

Advanced Security Settings

Local Accounts

Network Accounts

Printer Credentials

Security Templates

Access Controls

Miscellaneous

| Template Name            | Authentication Setup | Authorization Setup | Group Authorization Setup |
|--------------------------|----------------------|---------------------|---------------------------|
| Admin Password Protected | Admin Password       |                     |                           |

此安全模板应用于以下访问控制：

- 固件更新
- 远程管理
- 远程安全菜单

其余的访问控制设置为**无安全性**。但是，您始终可以将其他管理打印机菜单设置为使用安全模板以获得更多保护。如需有关访问控制的更多信息，请参阅[第 53 页上的“理解权限和功能访问控制”](#)。

在将此组件添加到配置之前，请确保设置密码和打印机凭证。

Advanced Security Settings

Local Accounts

Network Accounts

Printer Credentials

Security Templates

Access Controls

Miscellaneous

Password (1 accounts)

| Name           | Admin Password | Password                 |
|----------------|----------------|--------------------------|
| Admin Password | Yes            | <input type="password"/> |

Advanced Security Settings

Local Accounts

Network Accounts

Printer Credentials

Security Templates

Access Controls

Miscellaneous

Select the appropriate authentication method and enter the credentials. These credentials will be used by Markvisi configuration is assigned.

Authentication method

Save Changes

Discard Changes

# 理解权限和功能访问控制

打印机可以配置为限制对管理菜单和设备管理特性的公共访问。在较新的打印机型号中，可以通过不同类型的身份验证方法来保护访问打印机功能的权限。在较旧的打印机型号中，可以将安全模板应用于功能访问控制 (FAC)。

要与这些安全打印机打印机通信并管理它们，根据打印机型号，**MVE** 需要某些权限或 **FAC**。

下表解释了在 **MVE** 中可以管理哪些打印机管理功能，以及需要哪些权限或 **FAC**。

请注意，当远程管理受保护时，**MVE** 需要身份验证凭证。如果其他管理菜单和设备管理权限或 **FAC** 受保护，则远程管理也必须受保护。否则，**MVE** 无法执行这些功能。

这些权限和功能访问控制在 **MVE** 中被预定义为默认的高级安全组件，可以方便地在配置中使用。如需更多信息，请参阅[第 51 页上的“使用默认配置保护打印机”](#)。

如果您没有使用默认的高级安全组件，请确保在打印机中手动配置这些权限和功能访问控制。如需更多信息，请参阅[第 54 页上的“配置打印机安全性”](#)。

| 权限或 FAC                     | 描述                                             |
|-----------------------------|------------------------------------------------|
| 远程管理                        | 远程读写设置的能力。如果此表中列出的任何其他权限或 FAC 受保护，则远程管理也必须受保护。 |
| 固件更新                        | 从任何方法更新固件的能力。                                  |
| 应用程序配置                      | 从打印机安装或移除应用程序，以及将应用程序设置文件发送给打印机的能力。            |
| 导入/导出所有设置<br>或<br>配置文件导入/导出 | 发送配置文件给打印机的能力。                                 |
| 安全菜单<br>或<br>远程安全菜单         | 管理登录方法和配置打印机安全选项的能力。                           |

要在 MVE 中保护较新的打印机型号，请禁用对远程管理和安全菜单权限的公共访问。对于较旧的打印机型号，请将安全模板应用于远程管理 FAC。

# 配置打印机安全性

- 1 从打印机菜单，单击**打印机列表**。
- 2 单击打印机的 IP 地址，然后单击打开“**嵌入式 Web 服务器**”。
- 3 单击**设置或配置**。
- 4 根据您的打印机型号，执行以下任一操作：
  - 单击**安全 > 登录方法**，然后执行下列操作：

## 对于新款打印机型号

- a 从安全部分，创建登录方法。
  - b 单击登录方法旁边的**管理组/权限或管理权限**。
  - c 展开**管理菜单**，然后选择**安全菜单**。
  - d 展开**设备管理**，然后选择以下权限：
    - 远程管理
    - 固件更新
    - 应用程序配置
    - 导入/导出所有设置
  - e 单击**保存**。
  - f 从公有部分，单击**管理权限**。
  - g 展开**管理菜单**，然后清除**安全菜单**。
  - h 展开**设备管理**，然后清除**远程管理**。
  - i 单击**保存**。
- 单击**安全 > 安全设置或编辑安全设置**，然后执行下列操作：

## 对于旧款打印机型号

- a 从高级安全设置部分，创建组建模块和安全模板。
- b 单击**访问控制**，然后展开**管理菜单**。
- c 在远程安全菜单菜单中，选择安全模板。

d 展开**管理**，然后为以下功能访问控制选择安全模板：

- 应用程序配置
- 远程管理
- 固件更新
- 配置文件导入/导出

e 单击**提交**。

## 保护设备群中的打印机通信

1 发现安全的打印机。如需更多信息，请参阅[第 31 页上的“发现打印机”](#)。

注意：

- 当打印机旁边出现  时，说明它是安全的。如需有关保护打印机的信息，请参阅[help document](#)。
- 如需有关打印机安全状态的更多信息，请参阅[第 51 页上的“理解打印机安全状态”](#)。

2 从打印机创建配置。如需更多信息，请参阅[第 64 页上的“从打印机创建配置”](#)。

3 将配置分配给设备群。如需更多信息，请参阅[第 57 页上的“分配配置到打印机”](#)。

4 执行配置。如需更多信息，请参阅[第 57 页上的“执行配置”](#)。安全打印机旁边会出现一个挂锁符号。

## 保护打印机的其他方法

如需有关配置打印机安全设置的更多信息，请参阅打印机的[嵌入式 Web 服务器管理员指南](#)。

检查打印机的以下设置：

- 磁盘加密已启用。
- 以下端口受限制：
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- 默认的密码列表是 OWASP 密码字符串“B”。

## 管理打印机

### 重新启动打印机

- 1 从打印机菜单，单击**打印机列表**。
- 2 单击打印机的 IP 地址。
- 3 单击**重新启动打印机**。

### 查看打印机“嵌入式 Web 服务器”

“嵌入式 Web 服务器”是内置在打印机中的软件，提供从任何 Web 浏览器配置打印机的控制面板。

- 1 从打印机菜单，单击**打印机列表**。
- 2 单击打印机的 IP 地址。
- 3 单击打开“**嵌入式 Web 服务器**”。

### 审核打印机

审核从处于“已托管”状态的任何打印机收集信息，然后将信息存储在系统中。为确保系统中的信息是当前的，请定期执行审核。

- 1 从“打印机”菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**打印机 > 审核**。

**注意：**审核可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

### 更新打印机状态

“更新状态”特性让您更新打印机状态和耗材信息。为确保打印机状态和耗材信息是当前的，请定期更新状态。

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**打印机 > 更新状态**。

**注意：**状态更新可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

### 设置打印机状态

如需有关打印机状态的更多信息，请参阅[第 43 页上的“理解打印机生命周期状态”](#)。

- 1 从“打印机”菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。



3 单击**打印机**，然后选择下列状态之一：

- **设置状态为已托管**—打印机包含在系统中可以执行的所有活动中。
- **设置状态为未托管**—打印机被排除在系统中可以执行的所有活动外。
- **设置状态为已报废**—打印机从网络被移除。系统保留打印机信息，但并不希望在网络上再次看到打印机。

## 分配配置到打印机

在您开始之前，请确认打印机的配置已创建。将配置分配给打印机可以允许系统运行一致性检查和执行。如需更多信息，请参阅[第 62 页上的“创建配置”](#)。

1 从打印机菜单，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**配置 > 分配配置**。

4 从配置部分，选择一个配置。

**注意：**如果系统设置为使用 **Markvision** 管理设备证书，请选择**信任选定设备**。此确认是用户验证打印机是真实设备而非欺骗的方法。

5 单击**分配配置**。

## 取消配置分配

1 从“打印机”菜单，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**配置 > 取消配置分配**。

4 单击**取消配置分配**。

## 执行配置

MVE 对打印机进行一致性检查。如果某些设置不一致，那么 MVE 会在打印机上更改这些设置。MVE 在更改设置后会运行一次最终的一致性检查。要求打印机重新启动的更新（如固件更新）可能需要第二次执行才能完成。

在开始之前，请确认配置已经分配给打印机。如需更多信息，请参阅[第 57 页上的“分配配置到打印机”](#)。

1 从打印机菜单，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**配置 > 执行配置**。

**注意：**

- 如果打印机处于错误状态，那么一些设置可能不会被更新。
- 如需 MVE 将固件和解决方案文件部署到打印机，“固件更新”功能访问控制必须设置为**无安全性**。如果安全性已应用，那么“固件更新”功能访问控制必须使用与“远程管理”功能访问控制相同的安全模板。如需更多信息，请参阅[第 58 页上的“部署文件到打印机”](#)。
- 执行可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

## 检查打印机与配置的一致性

在一致性检查期间，MVE 会检查打印机设置，并检验它们是否与分配的配置相匹配。在此操作期间，MVE 不会对打印机做出更改。

在开始之前，请确认配置已经分配给打印机。如需更多信息，请参阅[第 57 页上的“分配配置到打印机”](#)。

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**配置 > 检查一致性**。

**注意：**

- 您可以在任务状态页面中查看结果。
- 一致性检查可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

## 部署文件到打印机

您可以将以下文件部署到打印机：

- **CA 证书**— 添加到打印机信任存储区的 .cer 或 .pem 文件。
- **配置包**— 从支持的打印机导出或者直接从 Lexmark 获得的 .zip 文件。
- **固件更新**— 快闪到打印机上的 .fls 文件。
- **常规文件**— 您要发送给打印机的任何文件。
  - **原始套接字**— 通过端口 9100 发送。打印机将其视为任何其他打印数据。
  - **FTP**— 通过 FTP 发送文件。此部署方法在安全打印机上不受支持。
- **打印机证书**— 作为默认证书安装在打印机上的签名证书。
- **通用配置文件 (UCF)**— 从打印机导出的配置文件。
  - **Web 服务**— 当打印机型号支持时，使用 HTTPS Web 服务。否则，打印机使用 HTTP Web 服务。
  - **FTP**— 通过 FTP 发送文件。此部署方法在安全打印机上不受支持。

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**配置 > 部署文件到打印机**。
- 4 单击**选择文件**，然后浏览文件。
- 5 选择一个文件类型，然后选择部署方法。
- 6 单击**部署文件**。

**注意：**

- 如需 MVE 将固件和解决方案文件部署到打印机，“固件更新”功能访问控制必须设置为**无安全性**。如果安全性已应用，那么“固件更新”功能访问控制必须使用与“远程管理”功能访问控制相同的安全模板。
- 文件部署可以预定为定期进行。如需更多信息，请参阅[第 128 页上的“创建时间表”](#)。

## 更新打印机固件

1 从打印机菜单，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**配置 > 更新固件到打印机**。

4 从资源库选择固件文件，或者单击**选择文件**，然后浏览固件文件。

**注意：**如需有关添加固件文件到资源库的更多信息，请参阅[第 68 页上的“将文件导入资源库”](#)。

5 如果需要，为预定更新，请选择**定义更新窗口**，然后选择开始日期、开始和暂停时间，以及每周的天数。

**注意：**固件在指定的开始时间和暂停时间内发送给打印机。任务在暂停时间后暂停，然后在下一个开始时间重新开始，直到完成。

6 单击**更新固件**。

**注意：**如需 MVE 更新打印机固件，“固件更新”功能访问控制必须设置为**无安全性**。如果安全性已应用，那么固件更新功能访问控制必须使用与远程管理功能访问控制相同的安全模板。在这种情况下，MVE 必须安全地管理打印机。如需更多信息，请参阅[第 51 页上的“保护打印机通信”](#)。

## 从打印机卸载应用程序

MVE 只能卸载以“软件包生成器”格式添加到系统中的应用程序。如需有关将应用程序上载到系统的更多信息，请参阅[第 68 页上的“将文件导入资源库”](#)。

1 在打印机菜单中，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**配置 > 从打印机卸载应用程序**。

4 选择应用程序。

5 单击**卸载应用程序**。

## 分配事件到打印机

将事件分配给打印机可以让 MVE 每当有一个相关联的警报出现在指定的打印机上时执行相关联的操作。如需有关创建事件的更多信息，请参阅[第 119 页上的“管理打印机警报”](#)。

**注意：**事件只能分配给不安全的打印机。

1 从“打印机”菜单，单击**打印机列表**。

2 选择一台或多台打印机。

3 单击**分配 > 事件**。

4 选择一个或多个事件。

**注意：**如果某些选定的打印机已经有分配给它们的事件，那么复选框中会出现一个破折号。如果您保留破折号，那么事件不会更改。如果您选择复选框，那么事件会分配给所有选定的打印机。如果您清除复选框，那么事件会从它先前分配的打印机取消分配。

5 单击**分配事件**。

## 分配关键字到打印机

分配关键字到打印机可以让您组织您的打印机。如需有关创建关键字的更多信息，请参阅[第 43 页上的“管理关键字”](#)。

- 1 从“打印机”菜单，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**分配 > 关键字**。
- 4 如果需要，在“视图”菜单中，选择一个类别。
- 5 选择一个或多个关键字。

**注意：**关键字按类别列出。如果某些选定的打印机已经有分配给它们的关键字，那么复选框中会出现一个破折号。如果您保留破折号，那么关键字不分配或取消分配给选定的打印机。如果您选择复选框，那么关键字会分配给所有选定的打印机。如果您清除复选框，那么关键字会从它先前分配的打印机取消分配。

- 6 单击**分配关键字**。

## 将凭证输入到安全打印机

可以发现并注册安全打印机。要与这些打印机通信，您可以执行配置或直接在 **MVE** 中输入凭证。

**注意：**当打印机旁边出现  时，说明它是安全的。

要输入凭证，请执行以下操作：

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择一台或多台安全打印机。
- 3 单击**安全 > 输入凭证**。
- 4 选择身份验证方法，然后输入凭证。
- 5 单击**输入凭证**。

**注意：**安全但没有在 **MVE** 中保存正确凭证的已注册打印机在通信过滤器下面被标记为缺少凭证。输入正确的凭证后，打印机被标记为安全。

## 手动配置默认的打印机证书

当不使用自动证书管理特性时，**MVE** 可以帮助简化在打印机设备群上签署默认打印机证书的过程。**MVE** 收集来自设备群的证书签名请求，然后在签名之后将签名证书部署到正确的打印机上。

系统管理员必须执行以下操作：

- 1 生成打印机证书签名请求。
  - a 在打印机菜单中，单击**打印机列表**。
  - b 选择一台或多台打印机。
  - c 单击**安全 > 生成打印机证书签名请求**。

**注意：**您可以在生成证书签名请求时选择一台或多台打印机，但一次只能存在一组请求。为避免覆盖任何现有的证书签名请求，必须先下载证书签名请求，然后再生成另一组证书签名请求。

- 2 等待任务完成，然后下载打印机证书签名请求。
  - a 在打印机菜单中，单击**打印机列表**。
  - b 单击**安全 > 下载打印机证书签名请求**。
- 3 使用受信任的 CA 签署证书签名请求。
- 4 将签名证书保存在一个 ZIP 文件中。

**注意：**所有签名证书必须位于 ZIP 文件的根位置。否则，MVE 无法解析该文件。
- 5 在打印机菜单中，单击**打印机列表**。
- 6 选择一台或多台打印机。
- 7 单击**配置 > 部署文件到打印机**。
- 8 单击**选择文件**，然后浏览至 ZIP 文件。
- 9 在文件类型菜单中，选择**打印机证书**。
- 10 单击**部署文件**。

## 移除打印机

- 1 在打印机菜单中，单击**打印机列表**。
- 2 选择一台或多台打印机。
- 3 单击**打印机**。
- 4 如果需要移除打印机证书，请选择**删除关联的设备证书**。

**注意：**如果 MVE 正在管理设备证书，则移除打印机证书会从打印机中移除默认证书。然后，打印机会生成一个新的自签名证书。
- 5 请执行下面的任一操作：
  - 要保留打印机信息，请单击**停用打印机**。
  - 要从系统中移除打印机，请单击**删除打印机**。

# 管理配置

## 概述

MVE 使用配置来管理设备群中的打印机。

配置是设置的集合，可以被分配并执行到一台打印机或一组打印机型号。在配置中，您可以修改打印机设置并部署应用程序、许可证、固件和打印机证书。

您可以创建由以下内容组成的配置：

- 基本打印机设置
- 高级安全设置
- 彩色打印权限

**注意：**此设置仅在支持的彩色打印机的配置中可用。

- 打印机固件
- 应用程序
- CA 证书
- 资源文件

使用配置，您可以执行以下操作来管理打印机：

- 分配配置到打印机。
- 将配置强制执行到打印机。配置中指定的设置应用于打印机。安装固件、应用程序、打印机证书、应用程序文件 (.fls) 和 CA 证书。
- 检查打印机是否符合配置。如果打印机不符合，那么可以将配置强制执行到打印机。

**注意：**配置执行和一致性检查可以预定为定期进行。

- 如果打印机支持配置设置但值不适用，则打印机显示为不一致。

## 创建配置

配置是设置的集合，可以被分配并执行到一台打印机或一组打印机。在配置中，您可以修改打印机设置并部署应用程序、许可证、固件和 CA 证书到打印机。

**1** 在配置菜单中，单击**所有配置 > 创建**。

**2** 键入配置的唯一名称及其描述。

3 在设置列表中，执行下面的一项或多项操作：

- 从基本选项卡中，选择一项或多项设置，然后指定值。如果值是变量设置，则使用 `${}` 将标头括起来。例如，`${Contact_Name}`。要使用某个变量设置文件，请从使用变量设置数据文件菜单中选择该文件，或导入该文件。如需更多信息，请参阅[第 66 页上的“理解变量设置”](#)。

Settings

Basic Advanced Security Color Print Permissions Firmware Apps Certificates Resource Files

Use variable setting data file

None Import

Show only included settings

Show settings for All models

View All settings Filter by setting name

| Setting          | Category | Value     |
|------------------|----------|-----------|
| Contact Location | General  | Demo CFCM |

- 选择一项或多项设置，然后指定值。如果值是变量设置，则使用 `${}` 将标头括起来。例如，`${Contact_Name}`。要使用某个变量设置文件，请从使用变量设置数据文件菜单中选择该文件，或导入该文件。如需更多信息，请参阅[第 66 页上的“理解变量设置”](#)。

Basic Advanced Security Color Print Permissions Firmware Apps Certificates Resource Files

Use variable setting data file

ConfigVariableTest- new.csv (Imported Aug 31, 2022 2:23:39) Import

Show only included settings

Show settings for All models

View All settings Filter by setting name

| Setting          | Category | Value               |
|------------------|----------|---------------------|
| Asset Tag        | General  | S{ASSET_TAG}        |
| Contact Location | General  | S{CONTACT_LOCATION} |
| Contact Name     | General  | S{CONTACT_NAME}     |

- 如果将一个或多个证书添加到此配置中，则可以从值下拉菜单中选择任何证书。
- 从高级安全选项卡中，选择一个高级安全组件。

注意：

- 要创建高级安全组件，请参阅[第 65 页上的“从打印机创建高级安全组件”](#)。
- 您只能在从选定的打印机创建配置时管理高级安全设置。如需更多信息，请参阅[第 64 页上的“从打印机创建配置”](#)。
- 从彩色打印权限选项卡中，配置相关的设置。如需更多信息，请参阅[第 66 页上的“配置彩色打印权限”](#)。

注意：此设置仅在支持的彩色打印机的配置中可用。

- 从固件选项卡中，选择一个固件文件。如果配置中存在同一固件的多个版本，则在一致性检查和执行过程中只考虑较高的固件版本。要导入固件文件，请参阅[第 68 页上的“将文件导入资源库”](#)。

- 从应用程序选项卡中，选择一个或多个要部署的应用程序。如需更多信息，请参阅[第 67 页上的“创建应用程序软件包”](#)。

**注意：**MVE 不支持部署具有试用许可证的应用程序。您只能部署免费应用程序或具有生产许可证的应用程序。

- 从证书选项卡中，选择一个或多个要部署的证书。要导入证书文件，请参阅[第 68 页上的“将文件导入资源库”](#)。

**注意：**选择使用 **Markvision 管理设备证书**，让 MVE 评估缺少、无效、吊销和过期的证书，然后自动更换这些证书。

选择下面的任一选项：

- 默认设备证书
- 命名设备证书

**注意：**默认情况下，用户可以在每次 MVE 安装时添加 10 个命名证书，在每个 MVE 配置中添加 5 个命名证书。

**注意：**如需更多信息，请参阅[第 71 页上的“为自动证书管理配置 MVE”](#)。

- 从资源文件选项卡中，选择下面要部署的任何文件类型：
  - 应用程序文件 (.fls)
  - 配置包 (.zip)
  - 通用配置文件 (.ucf)

**注意：**

- “资源”选项卡下面的任何选项都不做一致性检查。
- 不建议在一个配置中使用多个 UCF 和配置包。
- 在旧打印机上配置“扫描到网络”时，此方法不适用于 UCF 文件。必须使用部署文件到打印机操作来部署 UCF 文件。

#### 4 单击**创建配置**。

**注意：**下面的列表显示配置中的部署顺序：

- **CA 证书**
- 应用程序文件
- 解决方案软件包
- 高级安全
- 设备证书
- 基本设置
- **UCF 和配置包**
- 固件

## 从打印机创建配置

不包括以下组成部分：

- 打印机固件
- 应用程序
- 证书



要添加固件、应用程序和证书，请在 **MVE** 中编辑配置。

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择打印机，然后单击**配置 > 从打印机创建配置**。
- 3 如果需要，请选择**包括高级安全设置**来从选定的打印机创建高级安全组件。
- 4 如果打印机是安全的，请选择身份验证方法，然后输入凭证。
- 5 键入配置的唯一名称及其描述，然后单击**创建配置**。
- 6 从配置菜单，单击**所有配置**。
- 7 选择配置，然后单击**编辑**。
- 8 如果需要，请编辑设置。
- 9 单击**保存更改**。

## 示例场景：克隆配置

15 台 **Lexmark MX812** 打印机在发现后被添加到系统中。作为 IT 人员，您必须将现有打印机的设置应用于新发现的打印机。

**注意：**您还可以从打印机克隆配置，然后将配置强制执行到一组打印机型号。

### 示例实现

- 1 从现有的打印机列表中选择 **Lexmark MX812** 打印机。
- 2 从打印机创建配置。  
**注意：**为保护打印机，请包括高级安全设置。
- 3 分配，然后将配置强制执行到新发现的打印机。

## 从打印机创建高级安全组件

从打印机创建高级安全组件以管理高级安全设置。**MVE** 从该打印机读取所有设置，然后创建包含设置的组件。组件可以关联到具有相同安全框架的打印机型号的多个配置。

- 1 从打印机菜单，单击**打印机列表**。
- 2 选择打印机，然后单击**配置 > 从打印机创建高级安全组件**。
- 3 键入组件的唯一名称及其描述。
- 4 如果打印机是安全的，请选择身份验证方法，然后输入凭证。
- 5 单击**创建组件**。

**注意：**使用包含本地帐户的高级安全组件创建并强制执行配置时，会将本地帐户添加到打印机。打印机中预先配置的任何现有本地帐户都将保留。

## 生成配置设置的可打印版本

- 1 编辑配置或高级安全组件。
- 2 单击打印机友好版本。

## 理解动态设置

- 这些设置包括 802.1x 设备证书、HTTPS 设备证书和 IPSec 设备证书（在配置的基本选项卡下列出）。
- 所有这些设置的选项都是使用证书选项卡中选择的证书进行填充。
- 在克隆、导出或导入配置时，会清除这些设置的预选值。您必须手动选择这些值。

## 理解变量设置

变量设置让您管理整个设备群中每台打印机所独有的设置，如主机名或资产标记。当创建或编辑配置时，您可以选择 CSV 文件以关联到配置。

### Sample CSV format:

```
IP_ADDRESS,Contact_Name,Address,Disp_Info
1.2.3.4,John Doe,1600 Penn. Ave., Blue
4.3.2.1,Jane Doe,1601 Penn. Ave., Red
2.3.6.5,"Joe, Jane and Douglas",1601 Penn. Ave.,Yellow
2.3.6.7,"Joe, Jane and Douglas",1600 Penn. Ave.,He is 6'7" tall
```

在变量文件的标题行中，第一列是唯一的打印机标识符令牌。令牌必须是以下内容之一：

- **HOSTNAME**
- **IP\_ADDRESS**
- **SYSTEM\_NAME**
- **SERIAL\_NUMBER**

变量文件的标题行中的每一个后续列是用户定义的替换令牌。此令牌必须使用 **\${HEADER}** 格式在配置中引用。当执行配置时，使用后续行中的值替换它。确认令牌不包含任何空格。

您可以在创建或编辑配置时导入包含变量设置的 CSV 文件。如需更多信息，请参阅[第 62 页上的“创建配置”](#)。

## 配置彩色打印权限

MVE 让您限制主计算机和特定用户的彩色打印。

**注意：**此设置仅在支持的彩色打印机的配置中可用。

- 1 从“配置”菜单，单击**所有配置**。
- 2 创建或编辑配置。
- 3 从“彩色打印权限”选项卡，执行下面的任一操作：

### 配置主计算机的彩色打印权限

- a** 在“视图”菜单中，选择**主计算机**，然后选择**包括主计算机的彩色打印权限**。
- b** 单击**添加**，然后键入主计算机名。
- c** 要让主计算机用彩色打印，请选择**允许彩色打印**。
- d** 要让登录到主计算机的用户用彩色打印，请选择**覆盖用户权限**。
- e** 单击**保存并添加或保存**。

### 配置用户的彩色打印权限

- a** 在“视图”菜单中，选择**用户**，然后选择**包括用户的彩色打印权限**。
- b** 单击**添加**，然后键入用户名。
- c** 选择**允许彩色打印**。
- d** 单击**保存并添加或保存**。

## 创建应用程序软件包

- 1** 使用“导出数据”特性从 MVE 导出“打印机列表”视图。

- a** 从打印机菜单，单击**视图**。
- b** 选择**打印机列表**，然后单击**导出数据**。
- c** 选择一个保存搜索。
- d** 在“选择数据导出的文件类型”菜单中，选择 **CSV**。
- e** 单击**导出数据**。

- 2** 访问“软件包生成器”。

**注意：**如果您需要访问“软件包生成器”，请与您的 Lexmark 代表联系。

- a** 在 [cdp.lexmark.com/package-builder](http://cdp.lexmark.com/package-builder) 上登录到“软件包生成器”。
- b** 导入打印机列表，然后单击**下一步**。
- c** 键入软件包描述，然后键入您的电子邮件地址。
- d** 在产品菜单中，选择应用程序，然后在需要时添加许可证。
- e** 单击**下一步 > 完成**。将软件包下载链接发送到您的电子邮箱。

- 3** 下载软件包。

#### 注意：

- MVE 不支持部署具有试用许可证的应用程序。您只能部署免费应用程序或具有生产许可证的应用程序。如果您需要激活码，请与您的 Lexmark 代表联系。
- 要将应用程序添加到配置，请将应用程序软件包导入到资源库中。如需更多信息，请参阅[第 68 页上的“将文件导入资源库”](#)。

## 导入或导出配置

在开始导入配置文件之前，请确保它是从相同的 **MVE** 版本导出的。

- 1 从配置菜单，单击**所有配置**。
- 2 执行下面的任一操作：
  - 要导入配置文件，请单击**导入**，浏览配置文件，然后单击**导入**。
  - 要导出配置文件，请选择配置，然后单击**导出**。

**注意：**

- 当导出配置时，会排除密码。请在导入之后手动添加密码。
- UCF、配置包和应用程序文件不是导出配置的一部分。

## 将文件导入资源库

资源库是导入到 **MVE** 的固件文件、**CA** 证书和应用程序软件包的集合。这些文件可以关联到一个或多个配置。

- 1 从配置菜单，单击**资源库**。
- 2 单击**导入 > 选择文件**，然后浏览文件。

**注意：**只能导入固件文件 (.fls)、应用程序文件 (.fls)、应用程序软件包或配置包 (.zip)、CA 证书 (.pem) 和通用配置文件 (.ucf)。

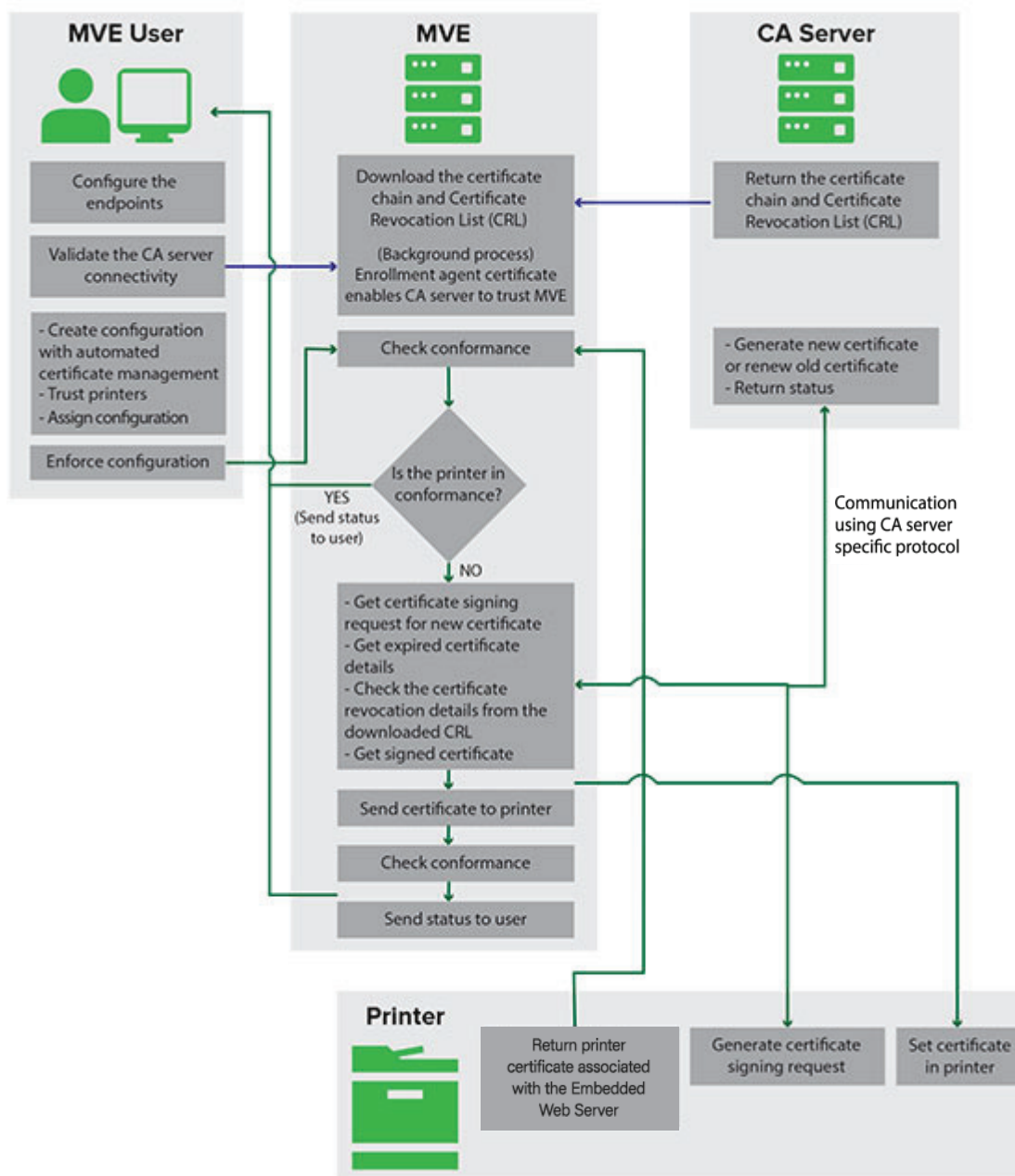
- 3 单击**导入资源**。

# 管理证书

## 设置 MVE 来自动管理证书

### 理解自动证书管理特性

您可以配置 **MVE** 来自动管理打印机证书，然后通过配置执行将它们安装到打印机上。下图描述了自动证书管理特性的端到端流程。



证书颁发机构端点（如 **CA** 服务器和服务器地址）必须在 **MVE** 中定义。

支持以下 CA 服务器：

- **OpenXPKI CA** - 用户可以使用下面的任一协议：
  - 安全证书加密协议 (SCEP)
  - EST 连接器

**注意：**

- EST 是连接到 OpenXPKI 服务器的推荐方式。
- 如需有关使用 EST 协议配置 OpenXPKI CA 的更多信息，请参阅 [第 105 页上的“通过 EST 使用 OpenXPKI 证书颁发机构管理证书”](#)
- 如需有关使用 SCEP 协议配置 OpenXPKI CA 的更多信息，请参阅 [第 90 页上的“通过 SCEP 使用 OpenXPKI 证书颁发机构管理证书”](#)

- **Microsoft CA 企业版** - 用户可以使用下面的任一协议：
  - 安全证书加密协议 (SCEP)
  - Microsoft 证书注册 Web 服务 (MSCEWS)

**注意：**

- MSCEWS 是连接到 Microsoft CA 企业版服务器的推荐方式。
- 如需有关使用 MSCEWS 协议配置 Microsoft CA 的更多信息，请参阅 [第 80 页上的“通过 MSCEWS 使用 Microsoft 证书颁发机构管理证书”](#)
- 如需有关使用 SCEP 协议配置 Microsoft CA 的更多信息，请参阅 [第 73 页上的“通过 SCEP 使用 Microsoft 证书颁发机构管理证书”](#)

必须验证 MVE 和 CA 服务器之间的连接。在验证期间，MVE 与 CA 服务器通信以下载证书链和证书吊销列表 (CRL)。还生成注册代理证书或测试证书。此证书使 CA 服务器能够信任 MVE。

如需有关定义端点和验证的更多信息，请参阅[第 71 页上的“为自动证书管理配置 MVE”](#)。

必须为打印机分配并实施已设置为使用 **Markvision 管理设备证书** 的配置。

如需更多信息，请参阅以下主题：

- [第 62 页上的“创建配置”](#)
- [第 57 页上的“执行配置”](#)

在执行期间，MVE 检查打印机的一致性。

对于**默认设备证书**

- 根据从 CA 服务器下载的证书链验证证书。
- 如果打印机不符合，则会为打印机引发“证书签名请求 (CSR)”。

对于**命名设备证书**

- 根据从 CA 服务器下载的证书链验证证书。
- MVE 在设备上创建自签名的命名设备证书。
- 如果打印机不符合，则会为打印机引发 CSR。

**注意：**

- MVE 使用所配置的协议与 CA 服务器通信。
- CA 服务器生成新证书，然后 MVE 将证书发送给打印机。
- 如果打印机中存在命名证书，则不会创建新的命名证书，但会为打印机引发 CSR。

## 为自动证书管理配置 MVE

1 单击页面右上角的 .

2 单击证书颁发机构 > 使用证书颁发机构服务器。

**注意：**使用证书颁发机构服务器按钮仅在第一次配置证书颁发机构时或在删除证书时出现。

3 配置服务器端点。

- **CA 服务器** - 生成打印机证书的证书颁发机构 (CA) 服务器。您可以选择下面的任一选项：

- **OpenXPKI CA**
- **Microsoft CA 企业版**

**注意：**用户还可以配置一台支持 **Enrollment over Secure Transport (EST)** 协议的 CA 服务器。

- CA 服务器必须实施 RFC 7030 中定义的 EST 协议。

**注意：**任何与规范的偏差都可能导致设置无效。

- EST 是连接到 OpenXPKI CA 服务器的推荐协议。

**注意：**Microsoft CA 企业版服务器不支持 EST 协议。

- **CA 服务器地址** - CA 服务器的 IP 地址或主机名。该字段仅适用于 SCEP 和 EST 协议。

**注意：**键入以下任何内容：

- 对于 MSCA 服务器（使用 SCEP）：<服务器 IP 地址或主机名>/certsrv/mscep/mscep.dll
- 对于 OpenXPKI 服务器（使用 SCEP）：<服务器 IP 地址或主机名>/scep/scep
- 对于 EST，键入以下任何内容：
  - https://172.87.95.240
  - https://estserver.com
  - estserver.com

- **CA 服务器标签（可选）** - 如果用户创建了新领域，则必须在此字段中输入相同的领域名称。

- **CEP 服务器地址** - 此字段仅适用于 MSCEWS 协议。

**注意：**键入以下任何内容：

- 对于用户名和密码身份验证：  
https://democep.com/ADPolicyProvider\_CEP\_UsernamePassword/service.svc/CEP
- 对于 Windows 集成身份验证：  
https://democep.com/ADPolicyProvider\_CEP\_Kerberos/service.svc/CEP
- 对于客户端证书身份验证：  
https://democep.com/ADPolicyProvider\_CEP\_Certificate/service.svc/CEP

- **CA 服务器主机名** - CA 服务器的主机名。

**注意：**例如，对于 MSCEWS 协议，用户可以选择 **democa.lexmark.com**

- **CES 服务器主机名** - CES 服务器的主机名。

**注意：**例如，对于 MSCEWS 协议，用户可以选择 **democes.lexmark.com**

- **质询密码** - 需要质询密码才能向 CA 服务器声明 MVE 身份。只有 OpenXPKI CA 需要此密码。Microsoft CA 企业版不支持。

**注意：**根据您的 CA 服务器，您必须配置服务器身份验证模式。执行下面的任一操作：

- 如果选择 **EST** 协议，则从 **CA 服务器身份验证模式** 菜单中选择以下任何一项：
  - 用户名和密码身份验证
  - 客户端证书身份验证
- 如果选择 **MSCEWS** 协议，则从 **CA 服务器身份验证模式** 菜单中选择以下任何一项：
  - 用户名和密码身份验证
  - 客户端证书身份验证
  - **Windows 集成身份验证**
- **SCEP** 协议仅支持质询密码身份验证模式。

**注意：**根据您的 CA 服务器，请参阅下面的任何部分：

- [第 90 页上的“通过 SCEP 使用 OpenXPki 证书颁发机构管理证书”](#)
- [第 73 页上的“通过 SCEP 使用 Microsoft 证书颁发机构管理证书”](#)
- [第 80 页上的“通过 MSCEWS 使用 Microsoft 证书颁发机构管理证书”](#)
- [第 105 页上的“通过 EST 使用 OpenXPki 证书颁发机构管理证书”](#)

#### 4 单击保存更改并验证 > 确定。

**注意：**

- **放弃更改**选项仅在尚未保存或者尚未保存和验证更改时才有效。
- 用户无法从无效配置中恢复数据，因为 **MVE** 不存储任何配置的最后一个有效状态。**MVE** 一次只存储一个证书配置（此配置可能有效，也可能无效）。

**注意：**

- 必须验证 **MVE** 和 **CA** 服务器之间的连接。在验证期间，**MVE** 与 **CA** 服务器通信以下载证书链和证书吊销列表 (CRL)。还生成注册代理证书或测试证书。此证书使 **CA** 服务器能够信任 **MVE**。
- 使用 **MSCEWS** 协议时，您可以选择一个或多个 **CEP** 模板。执行以下操作：

**a** 在单击**保存更改并验证**后，将出现“**CEP 模板选择**”窗口。

**b** 从可用模板中选择一个或多个模板。

- “使用证书颁发机构服务器”对话框将获取证书吊销列表。
- 将显示一个对话框来确认证书验证成功。

**c** 您可以在 **CA** 服务器配置页面中看到所选的 **CEP** 模板。

**注意：**当您对任何设备实施此配置时，将根据所选模板来创建证书。

#### 5 导览回系统配置页面，然后查看 CA 证书。

**注意：**您还可以下载或删除 CA 证书。

## 使用 NDES 配置 Microsoft 企业 CA

### 概述

在以下部署场景中，所有权限都基于在域控制器中发布的证书模板上设置的权限。发送到 **CA** 的证书请求基于证书模板。

对于此设置，请确保您具有以下条件：

- 托管从属 **CA** 的机器
- 托管 **NDES** 服务的机器



- 域控制器

### 所需用户

在域控制器中创建以下用户：

- 服务管理员
  - 命名为 **SCEPAdmin**
  - 必须是**本地管理**和**企业管理**组的成员
  - 在触发 **NDES** 角色安装时必须在本机登录
  - 具有证书模板的**注册权限**
  - 在 **CA** 上具有**添加模板权限**
- 服务帐户
  - 命名为 **SCEPSvc**
  - 必须是本地 **IIS\_IUSRS** 组的成员
  - 必须是一个域用户，并在已配置模板上具有**读**和**注册**权限
  - 在 **CA** 上具有**请求**权限
- 企业 **CA** 管理员
  - 命名为 **CAAdmin**
  - **企业管理**组的成员
  - 必须是**本地管理**组的一部分

## 通过 **SCEP** 使用 **Microsoft** 证书颁发机构管理证书

本节提供有关以下项目的说明：

- 使用 **Microsoft** 网络设备注册服务 (**NDES**) 配置 **Microsoft** 企业证书颁发机构 (**CA**)
- 创建根 **CA** 服务器

**注意：**Windows Server 2016 操作系统用于本文档中的所有设置。

### 概述

根 **CA** 服务器是任何组织中的主要 **CA** 服务器，并且是 **PKI** 基础设施的顶部。根 **CA** 对从属 **CA** 服务器进行身份验证。此服务器通常保持脱机模式，以防止任何入侵并保护私钥。

要配置根 **CA** 服务器，请执行以下操作：

- 1 确保根 **CA** 服务器已安装。如需更多信息，请参阅[第 73 页上的“安装根 CA 服务器”](#)。
- 2 配置“证书分发点”和“颁发机构信息访问”设置。如需更多信息，请参阅[第 76 页上的“配置证书分发点和颁发机构信息访问设置”](#)。
- 3 配置 **CRL** 可访问性。如需更多信息，请参阅[第 77 页上的“配置 CRL 可访问性”](#)。

### 安装根 **CA** 服务器

- 1 从“服务器管理器”，单击**管理 > 添加角色和特性**。
- 2 单击**服务器角色**，选择 **Active Directory 证书服务** 及其所有特性，然后单击**下一步**。

- 3 从 AD CS 角色服务部分，选择**证书颁发机构**，然后单击**下一步 > 安装**。
- 4 安装后，单击**配置目标服务器上的 Active Directory 证书服务**。
- 5 从角色服务部分，选择**证书颁发机构 > 下一步**。
- 6 从设置类型部分，选择**独立 CA**，然后单击**下一步**。
- 7 从 CA 类型部分，选择**根 CA**，然后单击**下一步**。
- 8 选择**创建一个新的私钥**，然后单击**下一步**。
- 9 从选择译电员提供程序菜单中，选择 **RSA#Microsoft 软件密钥存储提供程序**。
- 10 从密钥长度菜单中，选择 **4096**。
- 11 在哈希算法列表中，选择 **SHA512**，然后单击**下一步**。
- 12 在此 CA 的常用名字段中，键入托管服务器名称。
- 13 在可分辨名称后缀字段中，键入域组件。

#### 示例 CA 名称配置

机器完全合格域名 (FQDN): **test.dev.lexmark.com**

常用名 (CN): **TEST**

可分辨名称后缀: **DC=DEV, DC=LEXMARK, DC=COM**

- 14 单击**下一步**。
- 15 指定有效期，然后单击**下一步**。  
**注意：**通常，有效期为 10 年。
- 16 不要更改数据库位置窗口中的任何内容。
- 17 完成安装。

## 使用 NDES 配置 Microsoft 企业 CA

### 概述

在以下部署场景中，所有权限都基于在域控制器中发布的证书模板上设置的权限。发送到 CA 的证书请求基于证书模板。

对于此设置，请确保您具有以下条件：

- 托管从属 CA 的机器
- 托管 NDES 服务的机器
- 域控制器

### 所需用户

在域控制器中创建以下用户：

- 服务管理员
  - 命名为 **SCEPAdmin**
  - 必须是**本地管理**和**企业管理**组的成员
  - 必须在触发 NDES 角色安装时在本地登录

- 具有证书模板的注册权限
- 在 CA 上具有添加模板权限
- 服务帐户
  - 命名为 **SCEPSvc**
  - 必须是本地 **IIS\_IUSRS** 组的成员
  - 必须是一个域用户，并在已配置模板上具有读和注册权限
  - 在 CA 上具有请求权限

## 配置从属 CA 服务器

### 概述

从属 CA 服务器是中间 CA 服务器，并且始终处于联机状态。它通常处理证书的管理。

要配置从属 CA 服务器，请执行以下操作：

- 1 确保从属 CA 服务器已安装。如需更多信息，请参阅[第 75 页上的“安装从属 CA 服务器”](#)。
- 2 配置“证书分发点”和“颁发机构信息访问”设置。如需更多信息，请参阅[第 76 页上的“配置证书分发点和颁发机构信息访问设置”](#)。
- 3 配置 CRL 可访问性。如需更多信息，请参阅[第 77 页上的“配置 CRL 可访问性”](#)。

### 安装从属 CA 服务器

- 1 从服务器，以 **CAAdmin** 域用户身份登录。
- 2 从“服务器管理器”，单击**管理 > 添加角色和特性**。
- 3 单击**服务器角色**，选择 **Active Directory 证书服务**及其所有特性，然后单击**下一步**。
- 4 从 AD CS 角色服务部分，选择**证书颁发机构和证书颁发机构 Web 注册**，然后单击**下一步**。  
**注意：**确保添加证书颁发机构 Web 注册的所有特性。
- 5 从 Web 服务器角色 (IIS) 角色服务部分，保留默认设置。
- 6 安装后，单击**配置目标服务器上的 Active Directory 证书服务**。
- 7 从角色服务部分，选择**证书颁发机构和证书颁发机构 Web 注册**，然后单击**下一步**。
- 8 从设置类型部分，选择**企业 CA**，然后单击**下一步**。
- 9 从 CA 类型部分，选择**从属 CA**，然后单击**下一步**。
- 10 选择**创建一个新的私钥**，然后单击**下一步**。
- 11 从选择译电员提供程序菜单中，选择 **RSA#Microsoft 软件密钥存储提供程序**。
- 12 从密钥长度菜单中，选择 **4096**。
- 13 在哈希算法列表中，选择 **SHA512**，然后单击**下一步**。
- 14 在此 CA 的常用名字段中，键入主机服务器名称。
- 15 在可分辨名称后缀字段中，键入域组件。

### 示例 CA 名称配置

机器完全合格域名 (FQDN): `test.dev.lexmark.com`

常用名 (CN): `TEST`

可分辨名称后缀: `DC=DEV,DC=LEXMARK,DC=COM`

- 16 在证书请求对话框中, 保存请求文件, 然后单击下一步。
- 17 不要更改数据库位置窗口中的任何内容。
- 18 完成安装。
- 19 签署根 CA 的 CA 请求, 然后以 PKCS7 格式导出签名证书。
- 20 从从属 CA, 打开证书颁发机构。
- 21 从左侧面板, 用鼠标右键单击 CA, 然后单击**所有任务 > 安装 CA 证书**。
- 22 选择签名证书, 然后启动 CA 服务。

## 配置证书分发点和颁发机构信息访问设置

**注意:** 为证书吊销列表 (CRL) 配置证书分发点 (CDP) 和颁发机构信息访问 (AIA) 设置。

- 1 从“服务器管理器”, 单击**工具 > 证书颁发机构**。
- 2 从左侧面板, 用鼠标右键单击 CA, 然后单击**属性 > 扩展**。
- 3 在选择扩展菜单中, 选择 **CRL 分发点 (CDP)**。
- 4 在证书吊销列表中, 选择 **C:\Windows\system32\** 条目, 然后执行以下操作:
  - a 选择将 CRL 发布到此位置。
  - b 清除将 Delta CRL 发布到此位置。
- 5 删除除 **C:\Windows\system32\** 外的所有其他条目。
- 6 单击**添加**。
- 7 在位置字段中, 添加  
`http://serverIP/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl`, 其中 **serverIP** 是服务器的 IP 地址。

**注意:** 如果您的服务器可以使用 FQDN 进行访问, 则使用 **<ServerDNSName>**, 而不是服务器 IP 地址。
- 8 单击**确定**。
- 9 为创建的条目选择**包括在已颁发证书的 CDP 扩展中**。
- 10 在选择扩展菜单中, 选择**颁发机构信息访问 (AIA)**。
- 11 删除除 **C:\Windows\system32\** 外的所有其他条目。
- 12 单击**添加**。
- 13 在位置字段中, 添加  
`http://serverIP/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt`, 其中 **serverIP** 是服务器的 IP 地址。

**注意:** 如果您的服务器可以使用 FQDN 进行访问, 则使用 **<ServerDNSName>**, 而不是服务器 IP 地址。

- 14 单击**确定**。
- 15 为创建的条目选择**包括在已颁发证书的 AIA 扩展中**。
- 16 单击**应用 > 确定**。  
**注意：**如果需要，请重新启动证书服务。
- 17 从左侧面板，展开 **CA**，用鼠标右键单击**已吊销证书**，然后单击**属性**。
- 18 指定 **CRL 发布间隔**和**发布 Delta CRL 发布间隔**的值，然后单击**应用 > 确定**。
- 19 从左侧面板，用鼠标右键单击**已吊销证书**，单击**所有任务**，然后发布新 **CRL**。

## 配置 CRL 可访问性

**注意：**在开始之前，请确保“Internet 信息服务 (IIS) 管理器”已安装。

- 1 从“IIS 管理器”，展开 **CA**，然后展开**站点**。
- 2 用鼠标右键单击**默认 Web 站点**，然后单击**添加虚拟目录**。
- 3 在别名字段中，键入 **CertEnroll**。
- 4 在物理路径字段中，键入 **C:\Windows\System32\CertSrv\CertEnroll**。
- 5 单击**确定**。
- 6 用鼠标右键单击 **CertEnroll**，然后单击**编辑权限**。
- 7 从安全选项卡，移除除系统外的所有写访问权限。
- 8 单击**确定**。

## 配置 NDES 服务器

- 1 从服务器，以 **SCEPAdmin** 域用户身份登录。
- 2 从“服务器管理器”，单击**管理 > 添加角色和特性**。
- 3 单击**服务器角色**，选择 **Active Directory 证书服务**及其所有特性，然后单击**下一步**。
- 4 从 **AD CS 角色服务**部分，清除**证书颁发机构**。
- 5 选择**网络设备注册服务**及其所有特性，然后单击**下一步**。
- 6 从 **Web 服务器角色 (IIS)** 角色服务部分，保留默认设置。
- 7 安装后，单击**配置目标服务器上的 Active Directory 证书服务**。
- 8 从角色服务部分，选择**网络设备注册服务**，然后单击**下一步**。
- 9 选择 **SCEPSvc** 服务帐户。
- 10 从 **NDES 的 CA** 部分，选择 **CA 名称**或**计算机名称**，然后单击**下一步**。
- 11 从 **RA 信息**部分，指定信息，然后单击**下一步**。
- 12 从 **NDES 的加密**部分，执行以下操作：
  - 选择适当的签名和加密密钥提供程序。
  - 从密钥长度菜单中，选择与 **CA 服务器**相同的密钥长度。

**13** 单击下一步。

**14** 完成安装。

您现在可以作为 SCEPSvc 用户从 Web 浏览器访问 NDES 服务器。从 NDES 服务器，可以查看 CA 证书缩略图，注册质询密码，以及质询密码的有效期。

### 访问 NDES 服务器

打开 Web 浏览器，然后键入 `http://NDESServerIP/certsrv/mscep_admin`，其中 **NDESServerIP** 是 NDES 服务器的 IP 地址。

## 为 MVE 配置 NDES

**注意：**在开始之前，请确保 NDES 服务器正常工作。

### 创建证书模板

- 1 从从属 CA (certserv)，打开证书颁发机构。
- 2 从左侧面板，展开 CA，用鼠标右键单击**证书模板**，然后单击**管理**。
- 3 在证书模板控制台中，创建 **Web 服务器**的副本。
- 4 从常规选项卡，键入 **MVEWebServer** 作为模板名称。
- 5 从安全选项卡，为 **SCEPAdmin** 和 **SCEPSvc** 用户赋予适当的权限。  
**注意：**如需更多信息，请参阅[第 74 页上的“所需用户”](#)。
- 6 从主题名称选项卡，选择在请求中提供。
- 7 从从属 CA (certserv)，打开证书颁发机构。
- 8 从扩展选项卡，选择**应用程序策略 > 编辑**。
- 9 单击**添加 > 客户端身份验证 > 确定**。
- 10 从左侧面板，展开 CA，用鼠标右键单击**证书模板**，然后单击**新建 > 要发布的证书模板**。
- 11 选择新创建的证书，然后单击**确定**。

您现在可以使用 CA Web 注册门户访问模板。

### 访问模板

- 1 打开 Web 浏览器，然后键入 `http://CAserverIP/certsrv/certrqxt.asp`，其中 **CAserverIP** 是 CA 服务器的 IP 地址。
- 2 在证书模板菜单中，查看模板。

## 为 NDES 设置证书模板

- 1 从您的计算机，启用注册表编辑器。
- 2 导览至 **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**。

**3** 配置以下项目，然后将它们设置为 **MVEWebServer**:

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

**4** 向 SCEPSvc 用户授予 MSCEP 的完全权限。

**5** 从“IIS 管理器”，展开 CA，然后单击**应用程序池**。

**6** 从右侧面板，单击**回收**来重新启动 SCEP 应用程序池。

**7** 从“IIS 管理器”，展开 CA，然后展开**站点 > 默认 Web 站点**。

**8** 从右侧面板，单击**重新启动**。

## 在 Microsoft CA 服务器中禁用质询密码

**1** 从您的计算机，启用注册表编辑器。

**2** 导览至 **HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**。

**3** 将 EnforcePassword 设置为 **0**。

**4** 从“IIS 管理器”，展开 CA，单击**应用程序池**，然后选择 **SCEP**。

**5** 从右侧面板，单击**高级设置**。

**6** 将加载用户配置文件设置为**真**，然后单击**确定**。

**7** 从右侧面板，单击**回收**来重新启动 SCEP 应用程序池。

**8** 从“IIS 管理器”，展开 CA，然后展开**站点 > 默认 Web 站点**。

**9** 从右侧面板，单击**重新启动**。

从 Web 浏览器打开 NDES 时，您现在只能查看 CA 缩略图。

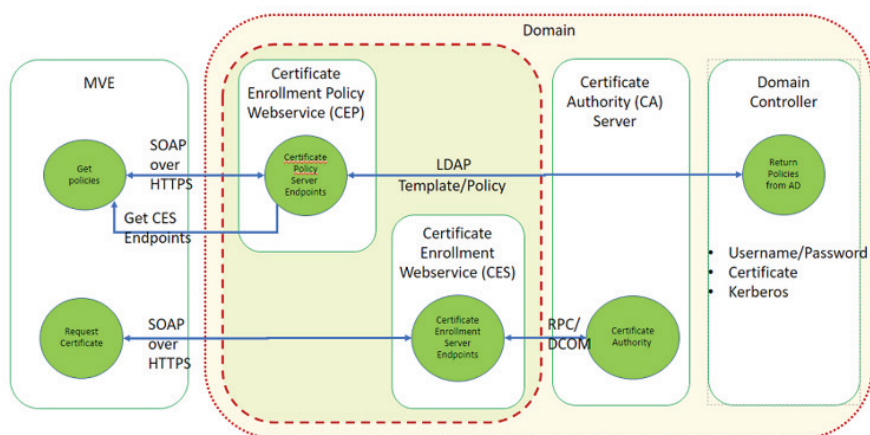
## 通过 MSCEWS 使用 Microsoft 证书颁发机构管理证书

本节提供有关配置“证书注册策略 Web 服务 (CEP)”和“证书注册 Web 服务 (CES)”的信息。由于 Microsoft 建议在两台不同的机器上安装 CEP 和 CES，我们在本文档中也遵循相同的原则。我们分别将这些 Web 服务称为 CEP 服务器和 CES 服务器。

**注意：**用户必须拥有预配置的“企业证书颁发机构 (CA)”和域控制器。

### 系统要求

Windows Server 2012 R2 和以后的操作系统用于本节中的所有设置。除非另有规定，否则以下安装要求和功能同时适用于 CEP 和 CES。



在域控制器中创建以下类型的帐户：

- 服务管理员：命名为 **CEPAdmin** 和 **CESAdmin**
  - 此用户必须是各自 CEP 和 CES 服务器中的**本地管理组**的一部分。
  - 此用户必须是**企业管理组**的成员。
- 服务帐户：命名为 **CEPSvc** 和 **CESSvc**
  - 此用户必须是**本地 IIS\_IUSRS**组的一部分。
  - 在 CA 上，需要各自 **CEPSvc** 和 **CESSvc** 的**请求证书**权限。

### 网络连接性要求

- 网络连接性要求是部署规划的一个关键部分，特别是对于 CEP 和 CES 托管在外围网络中的场景。
- 到这两个服务的所有客户端连接都发生在 HTTPS 会话中，因此在客户端和 Web 服务之间只允许 HTTPS 流量。
- CEP 使用标准的“轻型目录访问协议 (LDAP)”和安全 LDAP (LDAPS) 端口（分别为 TCP 389 和 636）与“Active Directory 域服务 (AD DS)”进行通信。
- CES 使用“分布式组件对象模型 (DCOM)”与 CA 进行通信。

**注意：**

- 默认情况下，DCOM 使用随机的临时端口。
- CA 可以配置为保留特定范围的端口，以简化防火墙配置。



## 为 CEP 和 CES 服务器创建 SSL 证书

CES 和 CEP 必须使用“安全套接字层 (SSL)”与客户端进行通信（通过使用 HTTPS）。每个服务都必须有一个有效的证书，它在本地计算机证书存储中具有服务器身份验证的“增强型密钥使用 (EKU)”策略。

- 1 在服务器中安装 IIS 服务。
- 2 登录到 CEP 服务器，然后在受信任的根证书颁发机构存储中添加根 CA 证书。
- 3 启动 IIS 管理器控制台，然后选择**服务器主页**。
- 4 从主视图部分，打开**服务器证书**。
- 5 单击**操作 > 创建证书请求**。
- 6 在可分辨名称属性窗口中，提供必要的信息，然后单击**下一步**。
- 7 在加密服务提供程序属性对话框中，选择位长度，然后单击**下一步**。
- 8 保存文件。
- 9 获取您计划用于 CEP 和 CES 的 CA 签名的文件。  
**注意：**确保在签名证书中启用服务器身份验证 EKU。
- 10 将签名文件复制回 CEP 服务器。
- 11 从 IIS 管理器控制台，选择**服务器主页**。
- 12 从主视图部分，打开**服务器证书**。
- 13 单击**操作 > 完成证书请求**。
- 14 在指定证书颁发机构响应窗口中，选择签名文件。
- 15 键入名称，然后在证书存储菜单中，选择**个人**。
- 16 完成证书安装。
- 17 从 IIS 管理器控制台，选择默认网站。
- 18 单击**操作 > 绑定**。
- 19 在网站绑定对话框中，单击**添加**。
- 20 在添加网站绑定对话框中，将类型设置为 **https**，然后从 SSL 证书浏览新创建的证书。
- 21 从 IIS 管理器控制台，选择**默认 Web 站点**，然后打开 SSL 设置。
- 22 启用要求 SSL，并将客户端证书设置为**忽略**。
- 23 重新启动 IIS。

**注意：**对 CES 服务器遵循相同的过程。

## 创建证书模板

用户必须为证书注册创建证书模板。执行以下操作以从现有的证书模板进行复制：

- 1 使用 CA 管理员凭证登录到企业 CA。
- 2 展开 CA，用鼠标右键单击**证书模板**，然后单击**管理**。
- 3 在证书模板控制台中，用鼠标右键单击 **Web 服务器证书模板**，然后单击**复制模板**。

- 4 从模板的常规选项卡，将模板命名为 **MVEWebServer**。
- 5 在安全选项卡中，授予 CA 管理员以**读**、**写**和**注册**权限。
- 6 向已通过身份验证的用户授予**读**和**注册**权限。
- 7 在主题名称选项卡中，选择请求中的**耗材**。
- 8 在常规选项卡中，设置证书有效期。
- 9 如果您计划使用此证书模板为打印机颁发 **802.1x** 证书，请执行以下操作：
  - a 从**扩展**选项卡，从此模板包含的扩展列表中选择**应用程序策略**。
  - b 单击**编辑 > 添加**。
  - c 在添加应用程序策略对话框中，选择**客户端身份验证**。
  - d 单击**确定**。
- 10 在证书模板属性对话框中，单击**确定**。
- 11 在 CA 窗口中，用鼠标右键单击**证书模板**，然后单击**新建 > 证书模板**。
- 12 选择 **MVEWebServer**，然后单击**确定**。

## 理解验证方法

CEP 和 CES 支持以下身份验证方法：

- Windows 集成身份验证，也称为 **Kerberos 身份验证**
- 客户端证书身份验证，也称为 **X.509 证书身份验证**
- 用户名和密码身份验证

### Windows 集成身份验证

Windows 集成身份验证使用 **Kerberos** 为连接到内部网络的设备提供不间断的身份验证流。此方法是内部部署的首选方法，因为它使用 AD DS 中现有的 **Kerberos** 基础机构。它还需要对证书客户端计算机进行最少的更改。

**注意：**如果需要客户端在直接连接到内部网络时仅访问 **Web** 服务，请使用此身份验证方法。

### 客户端证书身份验证

此方法优于用户名和密码身份验证，因为它更安全。它不需要直接连接到公司网络。

**注意：**

- 如果您计划为客户端提供数字 **X.509** 证书以进行身份验证，请使用此身份验证方法。
- 此方法启用 **Internet** 上可用的 **Web** 服务。

### 用户名和密码身份验证

用户名和密码方法是最简单的身份验证形式。此方法通常用于为不直接连接到内部网络的客户端提供服务。这是比客户端证书身份验证更不安全的身份验证选项，但是它不需要提供证书。

**注意：**当您可以访问内部网络或 **Internet** 上的 **Web** 服务时，请使用此身份验证方法。

## 委派要求

委派使服务能够模拟用户或计算机帐户来访问整个网络的资源。

当以下所有场景都适用时，CES 服务器需要委派：

- CA 和 CES 不在同一台计算机上。
- CES 可以处理初始注册请求，而不是仅处理证书续订请求。
- 身份验证类型设置为 **Windows 集成身份验证**或**客户端证书身份验证**。

在以下场景中，CES 服务器不需要委派：

- CA 和 CES 在同一台计算机上。
- 用户名和密码是身份验证方法。

注意：

- Microsoft 建议运行 CEP 和 CES 作为域用户帐户。
- 用户必须在域用户帐户上配置委派之前创建适当的服务主体名称 (SPN)。

## 启用委派

1 要为域用户帐户创建 SPN，请按如下方式使用 **setspn** 命令：

```
setspn -s http/ces.msca.com msca\CESSvc
```

注意：

- 帐户名称是 CESSvc。
- CES 正在 msca.com 域中完全合格域名 (FQDN) 为 **ces.msca.com** 的计算机上运行。

2 在域控制器中打开 CESSvc 域用户帐户。

3 从委派选项卡中，选择**仅信任此用户以委派给指定的服务**。

4 根据身份验证方法选择适当的委派。

注意：

- 如果选择 **Windows 集成身份验证**，请将委派配置为使用**仅 Kerberos**。
- 如果该服务使用客户端证书身份验证，则将委派配置为使用任何身份验证协议。
- 如果您计划配置多个身份验证方法，则将委派配置为使用任何身份验证协议。

5 单击**添加**。

6 在添加服务对话框中，选择**用户或计算机**。

7 键入您的 CA 服务器主机名，然后单击**检查名称**。

8 从添加服务对话框中，选择下面的任一服务进行委派：

- 该 CA 服务器的主机服务 (HOST)
- 该 CA 服务器的“远程过程调用系统服务 (RPCSS)”

9 关闭域用户属性对话框。

对于使用 Windows 集成身份验证的 CEP 域用户，请执行以下操作：

- 1 要为域用户帐户创建 SPN，请按如下方式使用 **setspn** 命令：

```
setspn -s http/cep.msca.com msca\CEPSvc
```

**注意：**帐户名称是 CEPSvc。

- 2 在域控制器中打开 CEPSvc 域用户帐户。
- 3 从委派选项卡中，选择不信任此用户进行委派。

## 配置 Windows 集成身份验证

要安装 CEP 和 CES，请使用 Windows PowerShell。

### 配置 CEP

**Install-AdcsEnrollmentPolicyWebService** cmdlet 配置“证书注册策略 Web 服务 (CEP)”。它还用于在现有安装中创建服务的其他实例。

- 1 使用 CEPAdmin 用户名登录到 CES 服务器，然后以管理模式启动 PowerShell。
- 2 运行命令 **Import-Module ServerManager**。
- 3 运行命令 **Add-WindowsFeature Adcs-Enroll-Web-Pol**。
- 4 运行命令 **Install-AdcsEnrollmentPolicyWebService -AuthenticationType Kerberos -SSLCertThumbprint "sslCertThumbPrint"**。

**注意：**删除指纹值之间的空格后，将 `<sslCertThumbPrint>` 替换为为 CEP 服务器创建的 SSL 证书的指纹。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启动“IIS 管理器控制台”。
- 7 在连接窗格中，展开托管 CEP 的 Web 服务器。
- 8 展开**站点**，展开**默认 Web 站点**，然后单击适当的安装虚拟应用程序名称：**ADPolicyProvider\_CEP\_Kerberos**。
- 9 在名为 **Home** 的虚拟应用程序中，双击应用程序设置，然后双击 **FriendlyName**。
- 10 在值下面键入一个名称，然后关闭该对话。
- 11 双击 **URI**，然后复制值。

**注意：**

- 如果要在同一 CEP 服务器上配置另一种身份验证方法，则必须更改 ID。
- 此 URL 在 MVE 或任何客户端应用程序中使用。

- 12 从左窗格，单击**应用程序池**。
- 13 选择 **WSEnrollmentPolicyServer**，然后从右窗格，单击**操作 > 高级设置**。
- 14 选择流程模型下面的标识字段。
- 15 在应用程序池标识对话框中，选择自定义帐户，然后键入 **CEPSvc** 作为域用户名。

16 关闭所有对话框，然后从 IIS 管理器控制台的右窗格回收 IIS。

17 从 PowerShell，键入 **iisreset** 以重新启动 IIS。

## 配置 CES

**Install-AdcsEnrollmentWebService** cmdlet 将配置“证书注册 Web 服务 (CES)”。它还用于在现有安装中创建服务的其他实例。

- 1 使用 **CESAdmin** 作为用户名登录到 CES 服务器，然后以管理模式启动 PowerShell。
- 2 运行 **Import-Module ServerManager** 命令。
- 3 运行 **Add-WindowsFeature Adcs-Enroll-Web-Svc** 命令。
- 4 运行 **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Kerberos** 命令。

注意：

- 删除指纹值之间的空格后，将 `<sslCertThumbPrint>` 替换为针对 CES 服务器创建的 SSL 证书的指纹。
- 将 **CA1.contoso.com** 替换为您的 CA 计算机名称。
- 将 **contoso-CA1-CA** 替换为您的 CA 常用名。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启用“IIS 管理器控制台”。
- 7 在连接窗格中，展开用于托管 CES 的 Web 服务器。
- 8 依次展开**站点**和**默认网站**，然后单击相应的安装虚拟应用程序名称：**contoso-CA1-CA\_CES\_Kerberos**。
- 9 从左窗格，单击**应用程序池**。
- 10 选择 **WSEnrollmentServer**，然后从右窗格中单击**操作 > 高级设置**。
- 11 选择流程模型下的“标识”字段。
- 12 在**应用程序池标识**对话框中，选择自定义帐户，然后键入 **CESSvc** 作为域用户名。
- 13 关闭所有对话框，然后从 IIS 管理器控制台的右窗格中重新启动 IIS。
- 14 在 PowerShell 中，键入 **iisreset** 以重新启动 IIS。
- 15 对于 CESSvc 域用户，启用委派。如需更多信息，请参阅[第 83 页上的“启用委派”](#)。

## 配置客户端证书身份验证

### 配置 CEP

**Install-AdcsEnrollmentPolicyWebService** cmdlet 配置 CEP。它还用于在现有安装中创建服务的其他实例。

- 1 使用 CEPAdmin 用户名登录到 CES 服务器，然后以管理模式启动 PowerShell。
- 2 运行命令 **Import-Module ServerManager**。
- 3 运行命令 **Add-WindowsFeature Adcs-Enroll-Web-Pol**。

- 4 运行命令 **Install-AdcsEnrollmentPolicyWebService -AuthenticationType Certificate -SSLCertThumbprint "sslCertThumbPrint"**。

**注意：**删除指纹值之间的空格后，将 `<sslCertThumbPrint>` 替换为为 CEP 服务器创建的 SSL 证书的指纹。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启用“IIS 管理器控制台”。
- 7 在连接窗格中，展开托管 CEP 的 Web 服务器。
- 8 展开站点，展开**默认 Web 站点**，然后单击适当的安装虚拟应用程序名称：**ADPolicyProvider\_CEP\_Certificate**。
- 9 在名为 **Home** 的虚拟应用程序中，双击应用程序设置，然后双击 **FriendlyName**。
- 10 在值下面键入一个名称，然后关闭该对话。
- 11 双击 **URI**，然后复制值。

**注意：**

- 如果要在同一 CEP 服务器上配置另一种身份验证方法，则必须更改 ID。
- 此 URL 在 MVE 或任何客户端应用程序中使用。

- 12 从左窗格，单击**应用程序池**。
- 13 选择 **WSEnrollmentPolicyServer**，然后从右窗格，单击**操作 > 高级设置**。
- 14 选择流程模型下面的标识字段。
- 15 在应用程序池标识对话框中，选择自定义帐户，然后键入 **CEPSvc** 作为域用户名。
- 16 关闭所有对话框，然后从 IIS 管理器控制台的右窗格回收 IIS。
- 17 从 PowerShell，键入 **iisreset** 以重新启动 IIS。

## 配置 CES

**Install-AdcsEnrollmentWebService** cmdlet 将配置“证书注册 Web 服务 (CES)”。它还用于在现有安装中创建服务的其他实例。

- 1 使用 **CESAdmin** 作为用户名登录到 CES 服务器，然后以管理模式启动 PowerShell。
- 2 运行 **Import-Module ServerManager** 命令。
- 3 运行 **Add-WindowsFeature Adcs-Enroll-Web-Svc** 命令。
- 4 运行 **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Certificate** 命令。

**注意：**

- 删除指纹值之间的空格后，将 `<sslCertThumbPrint>` 替换为针对 CES 服务器创建的 SSL 证书的指纹。
- 将 **CA1.contoso.com** 替换为您的 CA 计算机名称。
- 将 **contoso-CA1-CA** 替换为您的 CA 常用名。
- 如果您已经在主机中配置了一种身份验证方法，请从命令中移除 **ApplicationPoolIdentity**。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启用“**IIS 管理器控制台**”。
- 7 在连接窗格中，展开用于托管 CEP 的 Web 服务器。
- 8 依次展开**站点**和**默认网站**，然后单击相应的安装虚拟应用程序名称：**contoso-CA1-CA\_CES\_Certificate**。
- 9 从左窗格，单击**应用程序池**。
- 10 选择 **WSEnrollmentServer**，然后从右窗格中单击**操作 > 高级设置**。
- 11 选择流程模型下的“**标识**”字段。
- 12 在应用程序池标识对话框中，选择自定义帐户，然后键入 **CESSvc** 作为域用户名。
- 13 关闭所有对话框，然后从 IIS 管理器控制台的右窗格中重新启动 IIS。
- 14 在 PowerShell 中，键入 **iisreset** 以重新启动 IIS。
- 15 对于 CESSvc 域用户，启用委派。如需更多信息，请参阅[第 83 页上的“启用委派”](#)。

## 创建客户端证书

- 1 从任何域用户帐户，打开 **certlm.msc**。
- 2 单击**证书 > 个人 > 证书 > 所有任务 > 请求新证书**。
- 3 单击**下一步**。
- 4 单击 **Active Directory 注册 > 客户端访问**。  
**注意：** 如果不想使用 **Active Directory 注册** 选项，请执行以下操作：
  - a 单击**由您配置 > 添加新项**。
  - b 输入注册策略服务器 URI 作为用于 Username\_Password 或 Kerberos 验证的 CEP 服务器地址。
  - c 将验证类型指定为 **Windows 集成**。
  - d 单击**验证服务器**。
  - e 验证成功后，单击**添加**。
  - f 单击**下一步**。
  - g 选择任何模板。
- 5 单击**详细信息 > 属性**。
- 6 单击**注册**。
- 7 在主题选项卡中，提供完全合格域名 (FQDN)。
- 8 在私钥选项卡中，选择**使私钥可导出**。
- 9 单击**应用 > 注册**。

注册客户端证书后，执行以下操作以 PFX 格式导出客户端证书。

- 1 单击**证书 > 所有任务 > 导出**。
- 2 单击**下一步 > 是**，导出私钥。
- 3 单击**下一步**。

- 4 键入客户端提供的密码。
- 5 单击下一步。
- 6 在证书导出对话框中指定文件名。
- 7 单击下一步 > 完成。

## 配置用户名密码身份验证

### 配置 CEP

**Install-AdcsEnrollmentPolicyWebService** cmdlet 配置“证书注册策略 Web 服务 (CEP)”。它还用于在现有安装中创建服务的其他实例。

- 1 使用 CEPAdmin 用户名登录到 CEP 服务器，然后以管理模式启动 PowerShell。
- 2 运行命令 **Import-Module ServerManager**。
- 3 运行命令 **Add-WindowsFeature Adcs-Enroll-Web-Pol**。
- 4 运行命令 **Install-AdcsEnrollmentPolicyWebService -AuthenticationType UserName -SSLCertThumbprint "sslCertThumbPrint"**。

**注意：**删除指纹值之间的空格后，将 `<sslCertThumbPrint>` 替换为为 CEP 服务器创建的 SSL 证书的指纹。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启用“IIS 管理器控制台”。
- 7 在连接窗格中，展开托管 CEP 的 Web 服务器。
- 8 展开站点，展开默认 Web 站点，然后单击适当的安装虚拟应用程序名称：**ADPolicyProvider\_CEP\_UsernamePassword**。
- 9 在名为 **Home** 的虚拟应用程序中，双击应用程序设置，然后双击 **FriendlyName**。
- 10 在值下面键入一个名称，然后关闭该对话。
- 11 双击 **URI**，然后复制值。

**注意：**

- 如果要在同一 CEP 服务器上配置另一种身份验证方法，则必须更改 ID。
- 此 URL 在 MVE 或任何客户端应用程序中使用。

- 12 从左窗格，单击应用程序池。
- 13 选择 **WSEnrollmentPolicyServer**，然后从右窗口，单击操作 > 高级设置。
- 14 选择流程模型下面的标识字段。
- 15 在应用程序池标识对话框中，选择自定义帐户，然后键入 **CEPSvc**。
- 16 关闭所有对话框，然后从 IIS 管理器控制台的右窗格回收 IIS。
- 17 从 PowerShell，键入 **iisreset** 来重新启动 IIS。



## 配置 CES

**Install-AdcsEnrollmentWebService** cmdlet 将配置“证书注册 Web 服务 (CES)”。它还用于在现有安装中创建服务的其他实例。

- 1 使用 **CESAdmin** 作为用户名登录到 CES 服务器，然后以管理模式启动 PowerShell。
- 2 运行 **Import-Module ServerManager** 命令。
- 3 运行 **Add-WindowsFeature Adcs-Enroll-Web-Svc** 命令。
- 4 运行 **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig “CA1.contoso.com\contoso-CA1-CA” -SSLCertThumbprint “sslCertThumbPrint” -AuthenticationType UserName** 命令。

**注意：**

- 删除指纹值之间的空格后，将 *<sslCertThumbprint>* 替换为针对 CES 服务器创建的 SSL 证书的指纹。
- 将 **CA1.contoso.com** 替换为您的 CA 计算机名称。
- 将 **contoso-CA1-CA** 替换为您的 CA 常用名。
- 如果您已经在主机中配置了一种身份验证方法，请从命令中移除 **ApplicationPoolIdentity**。

- 5 通过选择 **Y** 或 **A** 来完成安装。
- 6 启用“IIS 管理器控制台”。
- 7 在连接窗格中，展开用于托管 CES 的 Web 服务器。
- 8 依次展开**站点**和**默认网站**，然后单击相应的安装虚拟应用程序名称：**contoso-CA1-CA\_CES\_UsernamePassword**。
- 9 从左窗格，单击**应用程序池**。
- 10 选择 **WSEnrollmentServer**，然后从右窗格中，单击**操作 > 高级设置**，在操作下。
- 11 选择流程模型下的“标识”字段。
- 12 在应用程序池标识对话框中，选择自定义帐户，然后键入 **CESSvc** 作为域用户名。
- 13 关闭所有对话框，然后从 IIS 管理器控制台的右窗格中重新启动 IIS。
- 14 在 PowerShell 中，键入 **iisreset** 以重新启动 IIS。

## 通过 SCEP 使用 OpenXPki 证书颁发机构管理证书

本节提供有关如何使用简单证书注册协议 (SCEP) 配置 OpenXPki CA 2.5.x 版本的说明。

注意:

- 确保您使用 Debian 8 Jessie 操作系统。
- 如需有关 OpenXPki 的更多信息, 请转到 [www.openxpki.org](http://www.openxpki.org)。

### 配置 OpenXPki CA

#### 安装 OpenXPki CA

- 1 使用 PuTTY 或另一个客户端连接机器。
- 2 从客户端, 运行 **sudo su -** 命令以转到根用户。
- 3 输入根密码。
- 4 在 **nano /etc/apt/sources.list** 中, 更改安装更新的源。
- 5 更新文件。例如:

```
#  
  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
# deb cdrom:[Debian GNU/Linux 8.11.1 _Jessie_ - Official amd64 CD Binary-1  
20190211-02:10]/ jessie local main  
  
deb http://security.debian.org/ jessie/updates main  
deb-src http://security.debian.org/ jessie/updates main  
  
# jessie-updates, previously known as 'volatile'  
# A network mirror was not selected during install. The following entries  
# are provided as examples, but you should amend them as appropriate  
# for your mirror of choice.  
#  
deb http://ftp.debian.org/debian/jessie-updates main  
deb-src http://ftp.debian.org/debian/jessie-updates main  
deb http://ftp.us.debian.org/debian/jessie main
```

- 6 保存文件。
- 7 运行以下命令:
  - **apt-get update**
  - **apt-get upgrade**
- 8 使用 **apt-get install ca-certificates** 更新服务器中的 CA 证书列表。
- 9 使用 **dpkg-reconfigure locales** 安装 **en\_US.utf8 locale**。
- 10 选择 **en\_US.UTF-8 UTF-8** 区域设置, 然后使其成为系统的默认区域设置。  
注意: 使用 Tab 和空格键选择和导览菜单。
- 11 检查您已经使用 **locale -a** 生成的区域设置。

#### Sample output

```
C  
C.UTF-8
```

```
en_IN
en_IN.utf8
en_US.utf8
POSIX
```

- 12 使用 **nano /home/Release.key** 复制 OpenXPki 软件包的指纹。对于此实例，复制 **/home** 中的密钥。
- 13 键入 **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** 作为值。
- 14 运行以下命令：  

```
gpg --print-md sha256 /home/Release.key
```
- 15 使用 **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -** 命令添加软件包。
- 16 使用 **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list**，然后使用 **aptitude update**，将存储库添加到源列表 (jessie) 中。
- 17 使用 **aptitude install mysql-server libdbd-mysql-perl** 安装 MySQL 和 Perl MySQL 绑定。
- 18 使用 **aptitude install apache2.2-common** 安装 apache2.2-common。
- 19 在 **nano /etc/apt/sources.list** 中，安装 **fastcgi** 模块以加速用户界面。  
注意：我们建议使用 **mod\_fcgid**。
- 20 在文件中添加 **deb http://http.us.debian.org/debian/jessie main** 行，然后保存。
- 21 运行以下命令：  

```
apt-get update
aptitude install libapache2-mod-fcgid
```
- 22 使用 **a2enmod fcgid** 启用 fastcgi 模块。
- 23 使用 **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n** 安装 OpenXPki 内核软件包。
- 24 使用 **service apache2 restart** 重新启动 Apache® 服务器。
- 25 使用 **openxpkiadm version** 检查安装是否成功。  
注意：如果安装成功，则系统会显示已安装的 OpenXPki 版本。例如：版本（内核）：2.5.5。
- 26 创建空数据库，然后使用 **mysql -u root -p** 分配数据库用户。

注意：

- 此命令必须在客户端中键入。否则，您无法输入密码。
- 键入 MySQL 的密码。对于此实例，**root** 是 MySQL 用户。
- **openxpki** 是安装 OpenXPki 的用户。

```
CREATE DATABASE openxpki CHARSET utf8;
CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki';
GRANT ALL ON openxpki.* TO 'openxpki'@'localhost';
flush privileges;
```

如果 MySQL 服务没有运行，则运行 **/etc/init.d/mysql start** 来启动服务。

- 27 键入 **quit** 以退出 MySQL。

**28** 将使用的凭证存储在 `/etc/openxpki/config.d/system/database.yaml` 中。

### Sample file content

```
debug: 0
type: MySQL
name: openxpki
host: localhost
port: 3306
user: openxpki
passwd: openxpki
```

**注意：**更改 **user** 和 **passwd** 以匹配 MySQL 用户名和密码。

**29** 保存文件。

**30** 对于空数据库架构，请从提供的架构文件运行 **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki**。

**31** 输入数据库的密码。

### 使用默认脚本配置 OpenXPki CA

**注意：**默认脚本只配置默认领域，**ca-one**。不配置 CDP 和 CRL。

**1** 使用 **gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz** 解压缩安装证书的示例脚本。

**2** 使用 **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh** 运行脚本。

**3** 使用 **openxpkiadm alias --realm ca-one** 确认设置。

### Sample output

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
not set
```

4 使用 **openxpkictl start** 检查安装是否成功。

## Sample output

```
Starting OpenXPKI...
OpenXPKI Server is running and accepting requests.
DONE.
```

5 执行以下操作以访问 OpenXPKI 服务器：

- a 从 Web 浏览器，键入 **http://ipaddress/openxpki/**。
- b 以操作员身份登录。默认密码是 **openxpki**。

注意：“操作员”登录有两个预配置的操作员帐户，**raop** 和 **raop2**。

6 创建一个证书请求，然后进行测试。

## 手动配置 OpenXPKI CA

### 概述

注意：在开始之前，请确保您具有创建 OpenSSL 证书的基本知识。

要手动配置 OpenXPKI CA，请创建以下内容：

- 1 根 CA 证书。如需更多信息，请参阅[第 94 页上的“创建根 CA 证书”](#)。
- 2 CA 签名者证书，由根 CA 签名。如需更多信息，请参阅[第 94 页上的“创建签名者证书”](#)。
- 3 数据保管库证书，自签名。如需更多信息，请参阅[第 95 页上的“创建保管库证书”](#)。
- 4 SCEP 证书，由签名者证书签名。

注意：

- 选择签名哈希时，请使用 SHA256 或 SHA512。
- 更改公钥大小是可选的。

对于此实例，我们使用 **/etc/certs/openxpki\_ca-one/** 目录生成证书。但是，您可以使用任何目录。

## 创建 OpenSSL 配置文件

1 运行以下命令：

```
nano /etc/certs/openxpki_ca-one/openssl.conf
```

注意：如果您的服务器可以使用完全合格域名 (FQDN) 进行访问，则使用服务器的 DNS 而不是其 IP 地址。

### 示例文件

```
# x509_extensions = v3_ca_extensions # x509_extensions = v3_issuing_extensions #
x509_extensions = v3_datavault_extensions # x509_extensions = v3_scep_extensions #
x509_extensions = v3_web_extensions # x509_extensions = v3_ca_reqexts # not for root self-
signed, only for issuing ## x509_extensions = v3_datavault_reqexts # not required self-
signed # x509_extensions = v3_scep_reqexts # x509_extensions = v3_web_reqexts [ req ]
default_bits = 4096 distinguished_name = req_distinguished_name [ req_distinguished_name ]
domainComponent = Domain Component commonName = Common Name [ v3_ca_reqexts ]
subjectKeyIdentifier = hash keyUsage = digitalSignature, keyCertSign, cRLSign
[ v3_datavault_reqexts ] subjectKeyIdentifier = hash keyUsage = keyEncipherment
extendedKeyUsage = emailProtection [ v3_scep_reqexts ] subjectKeyIdentifier = hash
[ v3_web_reqexts ] subjectKeyIdentifier = hash keyUsage = critical, digitalSignature,
```

```
keyEncipherment extendedKeyUsage = serverAuth, clientAuth [ v3_ca_extensions ]
subjectKeyIdentifier = hash keyUsage = digitalSignature, keyCertSign, cRLSign
basicConstraints = critical,CA:TRUE authorityKeyIdentifier = keyid:always,issuer
[ v3_issuing_extensions ] subjectKeyIdentifier = hash keyUsage = digitalSignature,
keyCertSign, cRLSign basicConstraints = critical,CA:TRUE authorityKeyIdentifier =
keyid:always,issuer:always cRLDistributionPoints = URI:http://FQDN of the
server/CertEnroll/MYOPENXPKI.crl authorityInfoAccess = caIssuers;URI:http://FQDN of the
server/CertEnroll/MYOPENXPKI.crt [ v3_datavault_extensions ] subjectKeyIdentifier = hash
keyUsage = keyEncipherment extendedKeyUsage = emailProtection basicConstraints = CA:FALSE
authorityKeyIdentifier = keyid:always,issuer [ v3_scep_extensions ] subjectKeyIdentifier =
hash basicConstraints = CA:FALSE authorityKeyIdentifier = keyid,issuer [ v3_web_extensions ]
subjectKeyIdentifier = hash keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth basicConstraints = critical,CA:FALSE
subjectAltName = DNS:stlopenxpkgi.lexmark.com cRLDistributionPoints = URI:http://FQDN of the
server/CertEnroll/MYOPENXPKI_ISSUINGCA.crl authorityInfoAccess = caIssuers;URI:http://FQDN
of the server/CertEnroll/MYOPENXPKI_ISSUINGCA.crt
```

2 使用您的设置信息更改 IP 地址和 CA 证书名称。

3 保存该文件。

## 为证书密钥创建密码文件

1 运行以下命令：

```
nano /etc/certs/openxpkgi_ca-one/pd.pass
```

2 键入您的密码。

3 保存文件。

## 创建根 CA 证书

**注意：**您可以创建自签名的根 CA 证书或生成证书请求，然后使它由根 CA 签名。

运行以下命令：

**注意：**用适当的值替换密钥长度、签名算法和证书名称。

```
1 openssl genrsa -out /etc/certs/openxpkgi_ca-one/ca-root-1.key -passout  
file:/etc/certs/openxpkgi_ca-one/pd.pass 4096
```

```
2 openssl req -new -key /etc/certs/openxpkgi_ca-one/ca-root-1.key -  
subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ROOTCA -  
out /etc/certs/openxpkgi_ca-one/ca-root-1.csr
```

```
3 openssl req -config /etc/certs/openxpkgi_ca-one/openssl.conf -extensions  
v3_ca_extensions -x509 -days 3560 -in /etc/certs/openxpkgi_ca-one/ca-  
root-1.csr -key /etc/certs/openxpkgi_ca-one/ca-root-1.key -  
out /etc/certs/openxpkgi_ca-one/ca-root-1.crt -sha256
```

## 创建签名者证书

**注意：**用适当的值替换密钥长度、签名算法和证书名称。

1 运行以下命令：

```
openssl genrsa -out /etc/certs/openxpkgi_ca-one/ca-signer-1.key -passout  
file:/etc/certs/openxpkgi_ca-one/pd.pass 4096
```

- 2 使用 `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_ca_reqexts -new -key /etc/certs/openxpki_ca-one/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ISSUINGCA -out /etc/certs/openxpki_ca-one/ca-signer-1.csr`，用 CA 信息更改请求中的主题。
- 3 使用 `openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_ca-one/ca-signer-1.csr -CA /etc/certs/openxpki_ca-one/ca-root-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/ca-signer-1.crt -sha256` 获取由根 CA 签名的证书。

## 创建保管库证书

注意：

- 保管库证书是自签名的。
- 用适当的值替换密钥长度、签名算法和证书名称。

- 1 运行以下命令：

```
openssl genrsa -out /etc/certs/openxpki_ca-one/vault-1.key -passout  
file:/etc/certs/openxpki_ca-one/pd.pass 4096
```

- 2 使用 `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_datavault_reqexts -new -key /etc/certs/openxpki_ca-one/vault-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/DC=STLOPENXPKI_INTERNAL/CN=MYOPENXPKI_DATAVAULT -out /etc/certs/openxpki_ca-one/vault-1.csr`，用 CA 信息更改请求中的主题。

- 3 运行以下命令：

```
openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions  
v3_datavault_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-  
one/vault-1.csr -key /etc/certs/openxpki_ca-one/vault-1.key -  
out /etc/certs/openxpki_ca-one/vault-1.crt
```

## 创建 SCEP 证书

注意：SCEP 证书由签名者证书签名。

运行以下命令：

注意：用适当的值替换密钥长度、签名算法和证书名称。

- 1 `openssl genrsa -out /etc/certs/openxpki_ca-one/scep-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096`
- 2 `openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -reqexts v3_scep_reqexts -new -key /etc/certs/openxpki_ca-one/scep-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_SCEPCA -out /etc/certs/openxpki_ca-one/scep-1.csr`
- 3 `openssl x509 -req -extfile /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_scep_extensions -days 900 -in /etc/certs/openxpki_ca-one/scep-1.csr -CA /etc/certs/openxpki_ca-one/ca-signer-1.crt -CAkey /etc/certs/openxpki_ca-one/ca-signer-1.key -CAcreateserial -out /etc/certs/openxpki_ca-one/scep-1.crt -sha256`

## 复制密钥文件并创建符号链接

- 1 将密钥文件复制到 `/etc/openxpki/ca/ca-one/`。

**注意：** 密钥文件必须由 OpenXPki 可读。

```
cp /etc/certs/openxpki_ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/vault-1.key /etc/openxpki/ca/ca-one/
cp /etc/certs/openxpki_ca-one/scep-1.key /etc/openxpki/ca/ca-one/
```

- 2 创建符号链接。

**注意：** 符号链接是默认配置使用的别名。

```
ln -s /etc/openxpki/ca/ca-one/ca-signer-1.key /etc/openxpki/ca/ca-one/ca-signer-1.pem
ln -s /etc/openxpki/ca/ca-one/scep-1.key /etc/openxpki/ca/ca-one/scep-1.pem
ln -s /etc/openxpki/ca/ca-one/vault-1.key /etc/openxpki/ca/ca-one/vault-1.pem
```

## 导入证书

使用适当的令牌将根证书、签名者证书、保管库证书和 SCEP 证书导入数据库中。

运行以下命令：

- 1 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/ca-root-1.crt**
- 2 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/ca-signer-1.crt --realm ca-one --token certsign**
- 3 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/scep-1.crt --realm ca-one --token scep**
- 4 **openxpkiadm certificate import --file /etc/certs/openxpki\_ca-one/vault-1.crt --realm ca-one --token datasafe**
- 5 使用 **openxpkiadm alias --realm ca-one** 检查导入是否成功。

## Sample output

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEhbtI9pE
NotBefore  : 2015-01-30 20:44:40
NotAfter   : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cg1XCc
```



```
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39
```

```
upcoming root ca:
  not set
```

## 启动 OpenXPki

- 1 运行 `openxpkictl start` 命令。

### Sample output

```
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

- 2 执行以下操作以访问 OpenXPki 服务器:

- a 从 Web 浏览器, 键入 `http://ipaddress/openxpki/`。

**注意:** 您还可以使用服务器的 FQDN, 而不是 `ipaddress`。

- b 以操作员身份登录。默认密码是 `openxpki`。

**注意:** “操作员”登录有两个预配置的操作员帐户, `raop` 和 `raop2`。

- 3 创建一个证书请求, 然后进行测试。

## 生成 CRL 信息

**注意:** 如果您的服务器可以使用 FQDN 进行访问, 则使用服务器的 DNS 而不是其 IP 地址。

- 1 使用 `openxpkictl stop` 停止 OpenXPki 服务。

- 2 在 `nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml` 中, 将 `connectors: cdp` 部分更新为以下内容:

```
class: Connector::Builtin::File::Path
LOCATION: /var/www/openxpki/CertEnroll/
file: "[% ARGS.0 %].crl"
content: "[% pem %]"
```

- a 在 `nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml` 中, 更新以下内容:

- `crl_distribution_points:` 部分

```
critical: 0
uri:
  - http://FQDN of the server/CertEnroll/[% ISSUER.CN.0 %].crl
  - ldap://localhost/[% ISSUER.DN %]
```

- `authority_info_access:` 部分

```
critical: 0
ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPki.crt
ocsp: http://ocsp.openxpki.org/
```

根据您的 CA 服务器更改 IP 地址和 CA 证书名称。

- b 在 `nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml` 中, 执行以下操作:

- 如果需要, 请更新 `nextupdate` 和 `renewal`。
- 将 `ca_issuers` 添加到以下部分:

```
extensions:
  authority_info_access:
    critical: 0
```

```
# ca_issuers and ocsp can be scalar or list
ca_issuers: http://FQDN of the server/CertEnroll/MYOPENXPKI.crt
#ocsp: http://ocsp.openxpki.org/
```

根据您的 CA 服务器更改 IP 地址和 CA 证书名称。

**3** 使用 **openxpkictl start** 启动 OpenXPKI 服务。

## 配置 CRL 可访问性

**1** 使用 **service apache2 stop** 停止 Apache 服务。

**2** 在 **/var/www/openxpki/** 目录中为 **crl** 创建 **CertEnroll** 目录。

**3** 将 **openxpki** 设置为此目录的所有者，然后配置权限以允许 Apache 读取和执行，并且其他服务为只读。  
**chown openxpki /var/www/openxpki/CertEnroll**  
**chmod 755 /var/www/openxpki/CertEnroll**

**4** 使用 **nano /etc/apache2/mods-enabled/alias.conf** 添加对 Apache alias.conf 文件的引用。

**5** 在 **<Directory "/usr/share/apache2/icons">** 部分之后，添加以下内容：

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/"
<Directory "/var/www/openxpki/CertEnroll">
    Options FollowSymlinks
    AllowOverride None
    Require all granted
</Directory>
```

**6** 使用 **nano /etc/apache2/apache2.conf** 在 **apache2.conf** 文件中添加引用。

**7** 在 **Apache2 HTTPD server** 部分中添加以下内容：

```
<Directory /var/www/openxpki/CertEnroll>
    Options FollowSymlinks
    AllowOverride None
    Allow from all
</Directory>
```

**8** 使用 **service apache2 start** 启动 Apache 服务。

## 启用 SCEP 服务

**1** 使用 **openxpkictl stop** 停止 OpenXPKI 服务。

**2** 使用 **aptitude install openca-tools** 安装 openca-tools 软件包。

**3** 使用 **openxpkictl start** 启动 OpenXPKI 服务。

使用任何客户端（如带有 SSCEP 的 **certnanny**）测试服务。

**注意：**SSCEP 是 SCEP 的命令行客户端。您可以从 <https://github.com/cernanny/sscep> 下载 SSCEP。

## 启用签名者代表（注册代理）证书

对于自动证书请求，我们使用 OpenXPki 的“签名者代表”证书特性。

1 使用 **openxpkictl stop** 停止 OpenXPki 服务。

2 在 **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml** 中，从 **authorized\_signer:** 部分，为签名者证书的主题名称添加规则。

```
rule1:
    # Full DN
    subject: CN=Markvision_.*
```

### 注意：

- 在此规则中，任何以 **Markvision\_** 开头的证书 CN 是“签名者代表”证书。
- 在 MVE 中设置主题名称以生成“签名者代表”证书。
- 检查脚本文件中的空格和缩进。
- 如果在 MVE 中更改了 CN，则在 OpenXPki 中添加更新的 CN。
- 您只能指定一个证书为“签名者代表”，然后指定完整的 CN。

3 保存文件。

4 使用 **openxpkictl start** 启动 OpenXPki 服务。

## 在 OpenXPki CA 中启用证书请求的自动批准

1 使用 **openxpkictl stop** 停止 OpenXPki 服务。

2 在 **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml** 中，更新 **eligible:** 部分：

### Old content

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
    args: "[% context.cert_subject_parts.CN.0 %]"
    expect:
      - Build
      - New
```

### New content

```
eligible:
  initial:
    value: 1
    # value@: connector:scep.generic.connector.initial
    # args: "[% context.cert_subject_parts.CN.0 %]"
    # expect:
    #   - Build
    #   - New
```

### 注意：

- 检查脚本文件中的空格和缩进。
- 要手动批准证书，请注释 **value: 1**，然后取消以前注释的其他行的注释。

3 保存文件。

4 使用 `openxpkictl start` 启动 OpenXPki 服务。

## 创建第二个领域

在 OpenXPki 中，您可以在同一系统中配置多个 PKI 结构。以下主题说明如何为名为 **ca-two** 的 MVE 创建另一个领域。

### 复制并设置目录

1 将 `/etc/openxpki/config.d/realm/ca-one` 示例目录树复制到领域目录内的新目录 (`cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two`) 中。

2 在 `/etc/openxpki/config.d/system/realms.yaml` 中，更新以下部分：

#### Old content

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: Verbose name of this realm
  baseurl: https://pki.example.com/openxpki/

#ca-two:
#   label: Verbose name of this realm
#   baseurl: https://pki.acme.org/openxpki/
```

#### New content

```
# This is the list of realms in this PKI
# You only need to enable the realms which are visible on the server

ca-one:
  label: CA-ONE
  baseurl: https://pki.example.com/openxpki/

ca-two:
  label: CA-TWO
  baseurl: https://pki.example.com/openxpki/
```

3 保存文件。

## 创建证书

以下说明显示如何生成签名者证书、保管库证书和 SCEP 证书。根 CA 签署签名者证书，然后签名者证书签署 SCEP 证书。保管库证书是自签名的。

1 生成，然后签署证书。如需更多信息，请参阅[第 93 页上的“手动配置 OpenXPki CA”](#)。

**注意：**更改证书常用名，以便用户可以轻松分辨用于不同领域的不同证书。您可以将 **DC=CA-ONE** 更改为 **DC=CA-TWO**。证书文件被创建在 `/etc/certs/openxpki_ca-two/` 目录中。

2 将密钥文件复制到 `/etc/openxpki/ca/ca-two/`。

**注意：**密钥文件必须由 OpenXPki 可读。

```
cp /etc/certs/openxpki_ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/
cp /etc/certs/openxpki_ca-two/vault-1.key /etc/openxpki/ca/ca-two/
```

```
cp /etc/certs/openxpki_ca-two/scep-1.key /etc/openxpki/ca/ca-two/
```

### 3 创建符号链接。另外，创建根 CA 证书的符号链接。

**注意：**符号链接是默认配置使用的别名。

```
ln -s /etc/openxpki/ca/ca-one/ca-root-1.crt /etc/openxpki/ca/ca-two/ca-root-1.crt
```

```
ln -s /etc/openxpki/ca/ca-two/ca-signer-1.key /etc/openxpki/ca/ca-two/ca-signer-1.pem
```

```
ln -s /etc/openxpki/ca/ca-two/scep-1.key /etc/openxpki/ca/ca-two/scep-1.pem
```

```
ln -s /etc/openxpki/ca/ca-two/vault-1.key /etc/openxpki/ca/ca-two/vault-1.pem
```

### 4 使用 **ca-two** 的适当令牌将签名者证书、保管库证书和 SCEP 证书导入数据库中。

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/ca-signer-1.crt --realm ca-two --issuer /etc/openxpki/ca/ca-two/ca-one-1.crt --token certsign
```

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/scep-1.crt --realm ca-two --token scep
```

```
openxpkiadm certificate import --file /etc/certs/openxpki_ca-two/vault-1.crt --realm ca-two --token datasafe
```

### 5 使用 **openxpkiadm alias --realm ca-two** 检查导入是否成功。

#### Sample output

```
=== functional token ===
scep (scep):
Alias      : scep-1
Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

vault (datasafe):
Alias      : vault-1
Identifier: lZILS1l6Km5aIGS6pA7P7azAJic
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2016-01-30 20:44:40

ca-signer (certsign):
Alias      : ca-signer-1
Identifier: Sw_IY7AdoGUp28F_cFEdhbtI9pE
NotBefore : 2015-01-30 20:44:40
NotAfter  : 2018-01-29 20:44:40

=== root ca ===
current root ca:
Alias      : root-1
Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39
NotAfter  : 2020-01-30 20:44:39

upcoming root ca:
not set
```

在此实例中，**ca-one** 和 **ca-two** 的根 CA 信息相同。

### 6 如果您在证书创建期间更改了证书密钥密码，请更新 **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**。

### 7 生成此领域的 CRL。如需更多信息，请参阅[第 97 页上的“生成 CRL 信息”](#)。

### 8 发布此领域的 CRL。如需更多信息，请参阅[第 98 页上的“配置 CRL 可访问性”](#)。

9 使用 **openxpkictl restart** 重新启动 OpenXPki 服务。

### Sample output

```
Stopping OpenXPki
Stopping gracefully, 3 (sub)processes remaining...
DONE.
Starting OpenXPki...
OpenXPki Server is running and accepting requests.
DONE.
```

10 执行以下操作以访问 OpenXPki 服务器：

- a 从 Web 浏览器，键入 **http://ipaddress/openxpki/**。
- b 以操作员身份登录。默认密码是 **openxpki**。

注意：“操作员”登录有两个预配置的操作员帐户，**raop** 和 **raop2**。

### 为多个领域配置 SCEP 端点

默认的领域 SCEP 端点是 **http://<ipaddress>/scep/scep**。如果您有多个领域，则为每一个领域配置唯一的 SCEP 端点（不同的配置文件）。在下面的说明中，我们使用两个 PKI 领域，**ca-one** 和 **ca-two**。

1 复制 **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf** 中的默认配置文件。

注意：将文件命名为 **ca-one.conf**。

2 在 **nano /etc/openxpki/scep/ca-one.conf** 中，将领域值更改为 **realm=ca-one**。

3 在 **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf** 中创建另一个配置文件。

注意：将文件命名为 **ca-two.conf**。

4 在 **nano /etc/openxpki/scep/ca-two.conf** 中，将领域值更改为 **realm=ca-two**。

5 使用 **openxpkictl restart** 重新启动 OpenXPki 服务。

SCEP 端点是以下内容：

- **ca-one**—**http://ipaddress/scep/ca-one**
- **ca-two**—**http://ipaddress/scep/ca-two**

如果您要区分不同 PKI 领域的登录凭证和默认证书模板，您可能需要高级配置。

### 允许同时存在具有相同主题的多个活动证书

默认情况下，在 OpenXPki 中一次只能激活一个具有相同主题名称的证书。但是，当强制执行多个命名证书时，必须同时存在具有相同主题名称的多个活动证书。

1 在 **/etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml** 中，从 **policy** 部分，将 **max\_active\_certs** 的值从 1 更改为 0。

注意：

- **REALM NAME** 是领域的名称。例如：**ca-one**。
- 检查脚本文件中的空格和缩进。

2 使用 **openxpkictl restart** 重新启动 OpenXPki 服务。

## 为 OpenXPki CA 设置默认端口号

默认情况下, Apache 侦听端口号 80。为 OpenXPki CA 设置默认端口号以避免冲突。

- 1 在 `/etc/apache2/ports.conf` 中, 添加或修改端口。例如: `Listen 8080`。
- 2 在 `/etc/apache2/sites-enabled/000-default.conf` 中, 添加或修改 `VirtualHost` 部分以映射新端口。例如: `<VirtualHost *:8080>`。
- 3 使用 `systemctl restart apache2` 重新启动 Apache 服务器。

要检查状态, 请运行 `netstat -tlnp | grep apache`。OpenXPki SCEP URL 现在是 `http://ipaddress:8080/scep/ca-one`, 并且 Web URL 是 `http://ip address:8080/openxpki`。

## 在 OpenXPki CA 中拒绝不带质询密码的证书请求

默认情况下, OpenXPki 接收请求而不检查质询密码。证书请求不会被拒绝, 并且 CA 和 CA 管理员决定是否批准或拒绝请求。为避免潜在的安全隐患, 请禁用此特性, 以便立即拒绝所有包含无效密码的证书请求。在 MVE 中, 仅当生成注册代理证书时才需要质询密码。

- 1 在 `etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml` 中, 从 `policy` 部分, 将 `allow_man_authn` 的值从 1 更改为 0。

注意:

- REALM NAME 是领域的名称。例如: `ca-one`。
- 检查脚本文件中的空格和缩进。

- 2 使用 `openxpkictl restart` 重新启动 OpenXPki 服务。

## 在证书中添加客户端身份验证 Eku

- 1 在 `/etc/openxpki/config.d/realm/REALM NAME/profile/l18n_OPENXPki_PROFILE_TLS_SERVER.yaml` 中, 从 `extended_key_usage` 部分, 将 `client_auth` 的值更改为 1。

注意:

- REALM NAME 是领域的名称。例如: `ca-one`。
- 检查脚本文件中的空格和缩进。

- 2 使用 `openxpkictl restart` 重新启动 OpenXPki 服务。

## 当通过 SCEP 请求时获得完整的证书科目

默认情况下, OpenXPki 仅读取请求证书的主题的 CN。其余信息, 如国家、地区和 DC, 都是硬编码的。例如, 如果证书主题是 `C=US、ST=KY、L=Lexington、O=Lexmark、OU=ISS、CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`, 则在通过 SCEP 签署证书之后, 主题被更改为 `DC=Test Deployment、DC= OpenXPki、CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`。

**注意：**REALM NAME 是领域的名称。例如：**ca-one**。

**1** 在 **/etc/openxpki/config.d/realm/REALM**

**NAME/profile/I18N\_OPENXPKI\_PROFILE\_TLS\_SERVER.yaml** 中，从 **enroll** 部分，将 **dn** 的值更改为以下内容：

```
CN=[% CN.0 %][% IF OU %][% FOREACH entry = OU %],OU=[% entry %][% END %][% END %][% IF O
%][% FOREACH entry = O %],O=[% entry %][% END %][% END %][% IF L %],L=[% L.0 %][% END %]
[% IF ST %],ST=[% ST.0 %][% END %][% IF C %],C=[% C.0 %][% END %][% IF DC %][% FOREACH
entry = DC %],DC=[% entry %][% END %][% END %][% IF EMAIL %][% FOREACH entry = EMAIL
%],EMAIL=[% entry %][% END %][% END %]
```

**2** 保存文件。

**3** 在 **/etc/openxpki/config.d/realm/REALM NAME/profile/template** 目录中创建一个名为 **l.yaml** 的文件。

**4** 添加以下内容：

```
id: L
label: L
description: I18N_OPENXPKI_UI_PROFILE_L_DESC
preset: L
type: freetext
width: 60
placeholder: Kolkata
```

**5** 保存文件。

**6** 在 **/etc/openxpki/config.d/realm/REALM NAME/profile/template** 目录中创建一个名为 **st.yaml** 的文件。

**7** 添加以下内容：

```
id: ST
label: ST
description: I18N_OPENXPKI_UI_PROFILE_ST_DESC
preset: ST
type: freetext
width: 60
placeholder: WB
```

**8** 保存文件。

**注意：**OpenXPki 必须拥有这两个文件，并且必须是可读、可写和可执行的。

**9** 使用 **openxpkictl restart** 重新启动 OpenXPki 服务。

## 吊销证书并发布 CRL

**1** 访问 OpenXPki 服务器。

**a** 从 Web 浏览器，键入 **http://ipaddress/openxpki/**。

**b** 以操作员身份登录。默认密码是 **openxpki**。

**注意：**“操作员”登录有两个预配置的操作员帐户，**raop** 和 **raop2**。

**2** 单击 **workflow搜索 > 立即搜索**。

**3** 单击要吊销的证书，然后单击证书链接。

**4** 从操作部分，单击**吊销请求**。

**5** 键入适当的值，然后单击**继续 > 提交请求**。

**6** 在下一页上，批准请求。证书吊销等待下一次 CRL 发布。

**7** 从 PKI 操作部分，单击**发布证书吊销列表 (CRL)**。



- 8 单击**强制创建吊销列表** > **继续**。
- 9 从 PKI 操作部分，单击**发布 CA/CRL**。
- 10 单击 **workflows 搜索** > **立即搜索**。
- 11 单击具有 **certificate\_revocation\_request\_v2** 类型的已吊销证书。
- 12 单击**强制唤醒**。

在新的 CRL 中，可以找到已吊销证书的序列号和吊销原因。

## 通过 EST 使用 OpenXPki 证书颁发机构管理证书

本节将帮助用户使用 EST 协议配置 OpenXPki CA 3.x.x 版本。

注意：

- 确保您使用的是 Debian 10 Buster 操作系统。
- 如需有关 OpenXPki 的更多信息，请转到 [www.openxpki.org](http://www.openxpki.org)。

## 配置 OpenXPki CA

### 安装 OpenXPki CA

- 1 使用 PuTTY 或其他客户端来连接机器。
- 2 从客户端，运行 **sudo su -** 命令以转到 root 用户。
- 3 输入 root 用户密码。
- 4 在 **nano /etc/apt/sources.list** 中，更改用于安装更新的来源。
- 5 更新该文件。例如：

```
# # deb cdrom:[Debian GNU/Linux testing _Buster_ - Official Snapshot amd64 DVD Binary-1
20190527-04:04]/ buster contrib main # deb cdrom:[Debian GNU/Linux testing _Buster_ -
Official Snapshot amd64 DVD Binary-1 20190527-04:04]/ buster contrib main deb
http://security.debian.org/debian-security buster/updates main contrib deb-src
http://security.debian.org/debian-security buster/updates main contrib # buster-updates,
previously known as 'volatile' # A network mirror was not selected during install.The
following entries # are provided as examples, but you should amend them as appropriate #
for your mirror of choice.# deb http://ftp.debian.org/debian/ buster-updates main deb-src
http://ftp.debian.org/debian/ buster-updates main deb http://ftp.us.debian.org/debian/
buster main
```
- 6 保存该文件。
- 7 运行以下命令：
  - **apt-get update**
  - **apt-get upgrade**
- 8 更新服务器中的 CA 证书列表，使用 **apt-get install ca-certificates** 命令。
- 9 安装 **en\_US.utf8 locale**，使用 **dpkg-reconfigure locales** 命令。
- 10 选择 **en\_US.UTF-8 UTF-8 locale**，然后将其设为系统的默认 locale。

注意：使用 Tab 键和空格键来选择和导览菜单。

11 检查您使用 `locale -a` 生成的 locale。

### 示例输出

```
C C.UTF-8 en_IN en_IN.utf8 en_US.utf8 POSIX
```

12 复制 OpenXPki 软件包的指纹，使用 `nano /home/Release.key` 命令。在此例中，复制 `/home` 中的键。

13 键入 `55D89776 006F632B E0196E3E D2495509 BAFDDC74 22FEAAD2 F055074E 0FE3A724` 作为值。

14 运行以下命令：

```
gpg --print-md sha256 /home/Release.key
```

15 使用 `wget https://packages.openxpki.org/v3/debian/Release.key -O - | apt-key add -` 命令添加软件包。

16 使用 `echo " deb http://packages.openxpki.org/v3/debian/ buster release" > /etc/apt/sources.list.d/openxpki.list` 和 `apt update` 命令将存储库添加到来源列表 (buster) 中。

17 使用 `apt install mariadb-server libdbd-mariadb-perl` 命令安装 MySQL 和 Perl MySQL 绑定。

18 使用 `apt install apache2` 命令安装 apache2.2-common。

19 在 `nano /etc/apt/sources.list` 中，安装 `fastcgi` 模块来加速用户界面。

注意：建议使用 `mod_fcgid`。

20 在该文件中添加 `deb http://http.us.debian.org/debian/ buster main` 行，然后保存该文件。

21 运行以下命令：

```
apt-get update
```

```
apt install libapache2-mod-fcgid
```

22 使用 `a2enmod fcgid` 命令启用 `fastcgi` 模块。

23 使用 `apt install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n` 命令安装 OpenXPki 核心软件包。

24 重新启动 Apache 服务器，使用 `service apache2 restart` 命令。

25 使用 `openxpkiadm version` 命令检查是否安装成功。

注意：如果安装成功，则系统会显示所安装的 OpenXPki 版本。例如，**Version (core): 3.18.2**。

26 创建空数据库，然后使用 `mariadb -u root -p` 命令分配数据库用户。

注意：

- 必须在客户端中键入此命令。否则，您无法输入密码。
- 键入 MySQL 的密码。在此例中，`root` 是 MySQL 用户。
- `openxpki` 是安装 OpenXPki 的用户。

```
CREATE DATABASE openxpki CHARSET utf8; CREATE USER 'openxpki'@'localhost' IDENTIFIED BY 'openxpki'; GRANT ALL ON openxpki.* TO 'openxpki'@'localhost'; flush privileges;
```

如果 MySQL 服务没有运行，则运行 `/etc/init.d/mysql start` 来启动该服务。

27 键入 `quit` 以退出 MySQL。

**28** 将所使用的凭证存储在 `/etc/openxpki/config.d/system/database.yaml` 中。

### 示例文件内容

```
main: debug: 0 type: MariaDB name: openxpki host: localhost port: 3306 user: openxpki
passwd: openxpki
```

**注意：**更改 **user** 和 **passwd** 以匹配 MariaDB 用户名和密码。

**29** 保存该文件。

**30** 对于空数据库模式，请从提供的模式文件中运行 `zcat /usr/share/doc/libopenxpki-perl/examples/schema-mariadb.sql.gz | \ mysql -u root --password --database openxpki`。

**31** 键入数据库的密码。

## 使用默认脚本配置 OpenXPki CA

**注意：**默认脚本仅配置默认领域 **ca-one**。未配置 CDP 和 CRL。

- 1** 使用 `bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh` 命令运行该脚本。
- 2** 使用 `openxpkiadm alias --realm democa` 命令确认设置。

### 示例输出

```
=== functional token === scep (scep): Alias : scep-1 Identifier: YsBNZ7JYTbx89F_-Z4jn_RPFFWo
NotBefore : 2015-01-30 20:44:40 NotAfter : 2016-01-30 20:44:40 vault (datasafe): Alias :
vault-1 Identifier: lZILS1l6Km5aIGS6pA7P7azAJic NotBefore : 2015-01-30 20:44:40 NotAfter :
2016-01-30 20:44:40 ca-signer (certsign): Alias : ca-signer-1 Identifier:
Sw_IY7AdoGUp28F_cFEhbtI9pE NotBefore : 2015-01-30 20:44:40 NotAfter : 2018-01-29 20:44:40
=== root ca === current root ca: Alias : root-1 Identifier: fVrqJAlpotPaisOAsnxa9cglXCc
NotBefore : 2015-01-30 20:44:39 NotAfter : 2020-01-30 20:44:39 upcoming root ca: not set
```

- 3** 使用 `openxpkictl start` 命令检查是否安装成功。

### 示例输出

```
Starting OpenXPki... OpenXPki Server is running and accepting requests. DONE.
```

- 4** 执行以下操作以访问 OpenXPki 服务器：
  - a** 从 Web 浏览器，键入 `http://ipaddress/openxpki/`。
  - b** 在 `userdb.yaml` 文件中添加用户名及其对应的密码。要添加用户名和密码，请执行以下操作：
    - 查看 `/home/pkiadm`，然后查看 `nano userdb.yaml`。
    - 粘贴以下内容：

```
estRA: digest:{"ssh256}somePassword" role: RA Operator
```

**注意：**在此例中，**estRA** 指的是用户名。要生成密码，请键入 `openxpkiadm hashpwd`。当出现用于询问密码和 **ssh256** 加密密码的消息时，将其复制并粘贴到任何用户的摘要中。

**注意：**“操作员”登录中可用的角色为“RA 操作员”、“CA 操作员”和“用户”。

- 5** 输入用户名和密码。
- 6** 创建一个证书请求，然后进行测试。

## 手动配置 OpenXPki CA

### 概述

**注意：**在开始之前，请确保您具备有关创建 OpenSSL 证书的基本知识。

要手动配置 OpenXPki CA，请创建以下内容：

- 1 根 CA 证书。如需更多信息，请参阅[第 94 页上的“创建根 CA 证书”](#)。
- 2 CA 签名者证书（由根 CA 签名的证书）。如需更多信息，请参阅[第 94 页上的“创建签名者证书”](#)。
- 3 保管库证书（自签名证书）。如需更多信息，请参阅[第 95 页上的“创建保管库证书”](#)。
- 4 Web 证书（通过签名者证书签名的证书）。如需更多信息，请参阅[第 111 页上的“设置 Web 服务器”](#)。

**注意：**

- 选择签名哈希时，请使用 SHA256 或 SHA512。
- 可以选择更改公钥大小。

对于 3.10 或更高版本，您可以使用“openxpkiadm alias”命令直接管理密钥：

- 运行 **mkdir -p /etc/openxpki/local/keys** 命令创建目录。该目录的默认位置为 **/etc/openxpki/local/keys**。
- 运行 **openxpki start** 命令启动服务器。

在此例中，我们使用 **/etc/certs/openxpki\_democa/** 目录来生成证书。但您可以使用任何目录。

### 创建 OpenSSL 配置文件

OpenSSL 配置文件包含用于生成和签署证书请求的 X.509 扩展。

1 运行以下命令：

```
nano /etc/certs/openxpki_democa/openssl.conf
```

**注意：**如果您的服务器可以使用完全合格域名 (FQDN) 进行访问，则使用服务器的 DNS 而不是其 IP 地址。

### 示例文件

```
# x509_extensions = v3_ca_extensions # x509_extensions = v3_issuing_extensions #
x509_extensions = v3_datavault_extensions # x509_extensions = v3_scep_extensions #
x509_extensions = v3_web_extensions # x509_extensions = v3_ca_reqexts # not for root self-
signed, only for issuing ## x509_extensions = v3_datavault_reqexts # not required self-
signed # x509_extensions = v3_scep_reqexts # x509_extensions = v3_web_reqexts [ req ]
default_bits = 4096 distinguished_name = req_distinguished_name [ req_distinguished_name ]
domainComponent = Domain Component commonName = Common Name [ v3_ca_reqexts ]
subjectKeyIdentifier = hash keyUsage = digitalSignature, keyCertSign, cRLSign
[ v3_datavault_reqexts ] subjectKeyIdentifier = hash keyUsage = keyEncipherment
extendedKeyUsage = emailProtection [ v3_scep_reqexts ] subjectKeyIdentifier = hash
[ v3_web_reqexts ] subjectKeyIdentifier = hash keyUsage = critical, digitalSignature,
keyEncipherment extendedKeyUsage = serverAuth, clientAuth [ v3_ca_extensions ]
subjectKeyIdentifier = hash keyUsage = digitalSignature, keyCertSign, cRLSign
basicConstraints = critical,CA:TRUE authorityKeyIdentifier = keyid:always,issuer
[ v3_issuing_extensions ] subjectKeyIdentifier = hash keyUsage = digitalSignature,
keyCertSign, cRLSign basicConstraints = critical,CA:TRUE authorityKeyIdentifier =
keyid:always,issuer:always cRLDistributionPoints = URI:https://FQDN of your
system/openxpki/CertEnroll/MYOPENXPki.crt authorityInfoAccess = caIssuers;URI:https://FQDN
of your system/download/MYOPENXPki.crt [ v3_datavault_extensions ] subjectKeyIdentifier =
hash keyUsage = keyEncipherment extendedKeyUsage = emailProtection basicConstraints =
CA:FALSE authorityKeyIdentifier = keyid:always,issuer [ v3_scep_extensions ]
```

```
subjectKeyIdentifier = hash basicConstraints = CA:FALSE authorityKeyIdentifier =
keyId,issuer [ v3_web_extensions ] subjectKeyIdentifier = hash keyUsage = critical,
digitalSignature, keyEncipherment extendedKeyUsage = serverAuth, clientAuth basicConstraints
= critical,CA:FALSE subjectAltName = DNS:FQDN of est server crlDistributionPoints =
URI:https://FQDN of your system/openxpki/CertEnroll/MYOPENXPki_ISSUINGCA.cr
authorityInfoAccess = caIssuers;URI:https://FQDN of your
system/download/MYOPENXPki_ISSUINGCA.crt
```

2 将 IP 地址和 CA 证书名称替换为您的设置信息。

3 保存该文件。

## 为证书密钥创建密码文件

1 运行以下命令：

```
nano /etc/certs/openxpki_democa/pd.pass
```

2 键入您的密码。

3 保存该文件。

## 创建根 CA 证书

您可以创建自签名的根 CA 证书，也可以生成证书请求并让根 CA 对其进行签名。

**注意：**将密钥长度、签名算法和证书名称替换为适当的值。

1 运行以下命令：

```
openssl genrsa -out /etc/certs/openxpki_democa/ca-root-1.key -passout
file:/etc/certs/openxpki_democa/pd.pass 4096
```

2 使用 **openssl req -new -key /etc/certs/openxpki\_democa/ca-root-1.key -out /etc/certs/openxpki\_democa/ca-root-1.csr** 命令将请求中的主题替换为您的 CA 信息。

3 使用 **openssl req -config /etc/certs/openxpki\_democa/openssl.conf -extensions v3\_ca\_extensions -x509 -days 3560 -in /etc/certs/openxpki\_democa/ca-root-1.csr -key /etc/certs/openxpki\_democa/ca-root-1.key -out /etc/certs/openxpki\_democa/ca-root-1.crt -sha256** 命令获取由根 CA 签名的证书。

4 请转到用于保存 **ca-root-1.crt** 的 **/etc/certs/openxpki\_democa/**。

5 运行以下命令：

```
openxpkiadm certificate import --file ca-root-1.crt
```

## 创建签名者证书

**注意：**将密钥长度、签名算法和证书名称替换为适当的值。

1 运行以下命令：

```
openssl genrsa -out /etc/certs/openxpki_democa/ca-signer-1.key -passout
file:/etc/certs/openxpki_democa/pd.pass 4096
```

2 使用 **openssl req -config /etc/certs/openxpki\_democa/openssl.conf -reqexts v3\_ca\_reqexts -new -key /etc/certs/openxpki\_democa/ca-signer-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPki\_ISSUINGCA -out /etc/certs/openxpki\_democa/ca-signer-1.csr** 命令将请求中的主题替换为您的 CA 信息。

- 3 使用 `openssl x509 -req -extfile /etc/certs/openxpki_democa/openssl.conf -extensions v3_issuing_extensions -days 3650 -in /etc/certs/openxpki_democa/ca-signer-1.csr -CA /etc/certs/openxpki_democa/ca-root-1.crt -CAkey /etc/certs/openxpki_democa/ca-root-1.key -CAcreateserial -out /etc/certs/openxpki_democa/ca-signer-1.crt -sha256` 命令获取由根 CA 签名的证书。
- 4 运行以下命令：  

```
openxpkiadm alias --realm democa --token certsign --file ca-signer-1.crt --key ca-signer-1.key
```

## 创建保管库证书

注意:

- 保管库证书是自签名证书。
- 将密钥长度、签名算法和证书名称替换为适当的值。

- 1 运行以下命令：  

```
openssl req -new -x509 -keyout vault.key -out vault.crt -days 1100 -config /etc/certs/openxpki_democa/openssl.conf
```
- 2 使用 `openxpkiadm certificate import --file vault.crt` 命令将请求中的主题更改为您的 CA 信息。
- 3 运行以下命令：  

```
openxpkiadm alias --realm democa --token datasafe --file vault.crt --key vault.key
```

注意: 提供必要的值, 但保留 `/CN=DataVault` 作为主题。

## 创建 Web 证书

- 1 运行以下命令：  

```
openssl genrsa -out /etc/certs/openxpki_democa/web-1.key -passout file:/etc/certs/openxpki_democa/pd.pass 4096
```
- 2 使用 `openssl req -config /etc/certs/openxpki_democa/openssl.conf -reqexts v3_web_reqexts -new -key /etc/certs/openxpki_democa/web-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=FQDN of your system -out /etc/certs/openxpki_democa/web-1.csr` 命令将请求中的主题替换为您的 CA 信息。
- 3 运行以下命令：  

```
openssl x509 -req -extfile /etc/certs/openxpki_democa/openssl.conf -extensions v3_web_extensions -days 900 -in /etc/certs/openxpki_democa/web-1.csr -CA /etc/certs/openxpki_democa/ca-signer-1.crt -CAkey /etc/certs/openxpki_democa/ca-signer-1.key -CAcreateserial -out /etc/certs/openxpki_democa/web-1.crt -sha256
```

## 设置 Web 服务器

### 1 运行以下命令：

```
a2enmod ssl rewrite headers
a2ensite openxpk
a2disssite 000-default default-ssl
mkdir -m755 -p /etc/openxpk/tls/chain
cp /etc/certs/openxpk_democa/ca-root-1.crt /etc/openxpk/tls/chain/
cp /etc/certs/openxpk_democa/ca-signer-1.crt /etc/openxpk/tls/chain/
c_rehash /etc/openxpk/tls/chain/
mkdir -m755 -p /etc/openxpk/tls/identity
mkdir -m700 -p /etc/openxpk/tls/private
cp /etc/certs/openxpk_democa/web-1.crt /etc/openxpk/tls/identity/openxpk
ki.crt
cat /etc/certs/openxpk_democa/ca-signer-1.crt
>> /etc/openxpk/tls/identity/openxpk.crt
openssl rsa -in /etc/certs/openxpk_democa/web-1.key -passin
file:/etc/certs/openxpk_democa/pd.pass -
out /etc/openxpk/tls/private/openxpk.pem
chmod 400 /etc/openxpk/tls/private/openxpk.pem
```

### 2 使用 `apache2 restart` 命令重新启动 Apache 服务。

### 3 运行以下命令来检查是否成功导入文件：

```
openxpkidm alias --realm democa
```

## 示例输出

```
=== functional token === ca-signer (certsign): Alias : ca-signer-2 Identifier:
XjC6MPbsnyfLZki9Poi9vm4Z5rk NotBefore : 2022-04-06 10:03:01 NotAfter : 2032-04-03 10:03:01
vault (datasafe): Alias : vault-2 Identifier: G8ekluAsskGVC0N-jZhB2n9kvdM NotBefore :
2022-04-06 09:53:57 NotAfter : 2025-04-10 09:53:57 scep (scep): not set ratoken (cmcra): not
set === root ca === current root ca: Alias : root-2 Identifier: prTHU5vCfcJuCnQWyb5wUknvXQM
NotBefore : 2022-04-06 09:40:27 NotAfter : 2032-01-04 09:40:27
```

## 使证书密钥密码可用于 OpenXPki

### 1 更改 `nano /etc/openxpk/config.d/system/crypto.yaml` 文件中的值。

### 2 取消注释 `secret: default` 下的 “cache: daemon”：

```
secret: default: label: Global Secret group export: 0 method: literal value: root cache:
daemon
```

## 启动 OpenXPki

### 1 运行 `openxpkictl start` 命令。

## 示例输出

```
Starting OpenXPki...OpenXPki Server is running and accepting requests.DONE.
```

## 2 访问 OpenXPki 服务器:

**a** 从 Web 浏览器, 键入 **http://ipaddress/openxpi/**。

**b** 在 **userdb.yaml** 文件中添加用户名及其对应的密码:

- 查看 **/home/pkiadm**, 然后查看 **nano userdb.yaml**。
- 粘贴以下内容:

```
estRA: digest:"{ssha256}somePassword" role: RA Operator
```

**注意:** 在这里, **estRA** 指的是用户名。

- 要生成密码, 请键入 **openxpiadm hashpwd**。此时会出现一条显示密码和 **ssha256** 加密密码的消息。
- 复制密码, 然后将其粘贴到任何用户的摘要中。

**注意:** “操作员”登录有两个预配置的可用角色: **RA 操作员**、**CA 操作员**和**用户**。

## 3 键入您的用户名和密码。

## 4 创建一个证书请求, 然后进行测试。

## 生成 CRL 信息

**注意:** 如果您的服务器可以使用 **FQDN** 进行访问, 则使用服务器的 **DNS** 而不是其 **IP 地址**。

### 1 使用 **openxpkictl stop** 命令停止 OpenXPki 服务。

### 2 在 **nano /etc/openxpi/config.d/realm/democa/publishing.yaml** 中, 将 **connectors: cdp** 部分更新为以下内容:

```
class: Connector::Builtin::File::Path LOCATION: /var/www/openxpi/CertEnroll/ file: "[%
ARGS.0 %].crl" content: "[% pem %]"
```

**a** 在 **nano /etc/openxpi/config.d/realm/democa/profile/default.yaml** 中, 更新以下内容:

- **crl\_distribution\_points:** 部分
 

```
critical: 0 uri: - https://FQDN of the est/openxpi/CertEnroll/[% ISSUER.CN.0
%].crl - ldap://localhost/[% ISSUER.DN %]
```
- **authority\_info\_access:** 部分
 

```
critical: 0 ca_issuers: https://FQDN of the est/download/MYOPENXPKI.crt ocs:
http://ocsp.openxpi.org/
```

根据您的 **CA 服务器**更改 **IP 地址**和 **CA 证书名称**。

**注意:** **authority\_info\_access (AIA)** 路径保存在 **Download** 文件夹中, 但您可以根据自己的喜好来设置此位置。

**b** 在 **nano /etc/openxpi/config.d/realm/democa/crl/default.yaml** 中, 执行以下操作:

- 如有必要, 请更新 **nextupdate** 和 **renewal**。
- 将 **ca\_issuers** 添加到以下部分:
 

```
extensions: authority_info_access: critical: 0 # ca_issuers and ocs: can be scalar
or list ca_issuers: https://FQDN of the est/download/MYOPENXPKI.crt #ocsp:
http://ocsp.openxpi.org/
```

根据您的 **CA 服务器**更改 **IP 地址**和 **CA 证书名称**。

### 3 使用 **openxpkictl start** 命令启动 OpenXPki 服务。



## 发布 CRL 信息

在创建 CRL 之后，您必须发布它们以供所有人访问。

- 1 使用 **service apache2 stop** 命令停止 Apache 服务。
- 2 为 **/var/www/openxpki/** 目录中的 CRL 创建 **CertEnroll** 目录。
- 3 将 **openxpki** 设置为该目录的所有者，然后配置相应的权限以允许 Apache 读取和执行内容并允许其他服务只读取内容。  
**chown openxpki /var/www/openxpki/CertEnroll**  
**chmod 755 /var/www/openxpki/CertEnroll**
- 4 使用 **nano /etc/apache2/mods-enabled/alias.conf** 命令在 Apache alias.conf 文件中添加一个引用。
- 5 在 **<Directory "/usr/share/apache2/icons">** 部分后面，添加以下内容：  

```
Alias /CertEnroll/ "/var/www/openxpki/CertEnroll/" <Directory  
"/var/www/openxpki/CertEnroll"> Options FollowSymlinks AllowOverride None Require all  
granted </Directory>
```
- 6 使用 **nano /etc/apache2/apache2.conf** 命令在 apache2.conf 文件中添加一个引用。
- 7 在 **Apache2 HTTPD server** 部分中添加以下内容：  

```
<Directory /var/www/openxpki/CertEnroll> Options FollowSymlinks AllowOverride None Allow  
from all </Directory>
```
- 8 使用 **service apache2 start** 命令启动 Apache 服务。

## 在 OpenXPki CA 中启用证书请求的自动批准

- 1 使用 **openxpkictl stop** 命令停止 OpenXPki 服务。
- 2 在 **/etc/openxpki/config.d/realm/democa/est/default.yaml** 中，更新 **eligible:** 部分：

### 旧内容

```
eligible: initial: value@: connector:scep.generic.connector.initial args: '[%  
context.cert_subject_parts.CN.0 %]' expect: - Build - New
```

### 新内容

```
eligible: initial: value: 1 # value@: connector:scep.generic.connector.initial # args: '[%  
context.cert_subject_parts.CN.0 %]' # expect: # - Build # - New
```

### 注意：

- 检查脚本文件中的空格和缩进。
- 要手动批准证书，请注释掉 **value: 1**，然后取消注释之前注释掉的其他行。

- 3 保存该文件。
- 4 使用 **openxpkictl start** 命令启动 OpenXPki 服务。

## 更改详细信息以启用 CA 证书下载

1 运行以下命令：

```
nano /usr/lib/cgi-bin/est.fcgi
```

2 将 `my $mime = "application/pkcs7-mime; smime-type=certs-only";` 替换为 `my $mime = "application/pkcs7-mime";`。

3 使用 `openxpkiectl` 命令启动 OpenXPki 服务。

## 创建第二个领域

在 OpenXPki 中，您可以在同一系统中配置多个 PKI 结构。以下主题说明如何为名为 **democa-two** 的 MVE 创建另一个领域。

### 复制和设置目录

1 为 `/etc/openxpki/config.d/realm` 中的第二个领域创建名为 **democa2** 的目录。

2 将 `/etc/openxpki/config.d/realm/ca-one` 示例目录树复制到 `realm` 目录内的新目录 (`cp -r /etc/openxpki/config.d/realm.tpl/* /etc/openxpki/config.d/realm/democa2`) 中。

3 在 `/etc/openxpki/config.d/system/realms.yaml` 中，更新以下部分：

### 旧内容

```
# This is the list of realms in this PKI # You only need to enable the realms which are
visible on the server democa: label: Verbose name of this realm baseurl:
https://pki.example.com/openxpki/ #democa2: # label: Verbose name of this realm # baseurl:
https://pki.acme.org/openxpki/
```

### 新内容

```
# This is the list of realms in this PKI # You only need to enable the realms which are
visible on the server democa: label: Example.org Demo CA baseurl:
https://pki.example.com/openxpki/ democa2: label: Example.org Demo CA2 baseurl:
https://pki.example.com/openxpki/
```

4 保存该文件。

## 为多个领域配置 EST 端点

您可以使用由 URI 的权限部分和可选标签（例如，`www.example.com:80` 和 `arbitraryLabel1`）组成的元组来配置 EST 端点。在以下说明中，我们使用以下两个 PKI 领域：**democa** 和 **democa2**。

1 将默认配置文件复制到 `cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa.conf` 中。

**注意：**将该文件命名为 **democa.conf**。

2 在 `nano /etc/openxpki/est/democa.conf` 中，将领域值更改为 `realm=democa`。

**注意：**根据您的需要，您可能需要取消注释 `simpleenroll`、`simplereenroll`、`csrattrs` 和 `cacerts` 部分的相应行。保持注释掉环境部分。对 `default.conf` 执行同样的操作。

3 在 `cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa2.conf` 中创建另一个配置文件。

**注意：**将该文件命名为 **democa2.conf**。

4 在 `nano /etc/openxpki/est/democa2.conf` 中，将领域值更改为 `realm=democa2`。

**注意：**根据您的需要，您可能需要取消注释 `simpleenroll`、`simplereenroll`、`csrattrs` 和 `cacerts` 部分的相应行。保持注释掉环境部分。

5 将 `default.yaml` 文件复制到以下位置：

- `cp /etc/openxpki/config.d/realm/democa/est/default.yaml`
- `/etc/openxpki/config.d/realm/democa/est/democa.yaml`

**注意：**将该文件命名为 `democa.yaml`。

6 将 `default.yaml` 文件复制到以下位置：

- `cp /etc/openxpki/config.d/realm/democa2/est/default.yaml`
- `/etc/openxpki/config.d/realm/democa2/est/democa2.yaml`

**注意：**将该文件命名为 `democa2.yaml`。

7 使用 `openxpkictl restart` 命令重新启动 OpenXPki 服务。

选择以下 URL 以通过 Web 浏览器打开与领域对应的 EST 服务器：

- `democa`—`http://ipaddress/est/democa`
- `democa2`—`http://ipaddress/est/democa2`

如果您想区分不同 PKI 领域的登录凭证和默认证书模板，则可能需要高级配置。

## 创建签名者证书

以下说明介绍了如何在第二个领域中生成签名者证书。您可以使用与第一个领域中相同的根证书和保管库证书。

1 在 `nano /etc/certs/openxpki_democa2/openssl.conf` 中创建一个 OpenSSL 配置文件。

**注意：**更改证书常用名，以便用户可以轻松区分不同领域的不同证书。将在 `/etc/certs/openxpki_democa2/` 目录中创建证书文件。

2 转到第一个领域的保管库证书目录，然后从第一个领域中导入证书。

3 运行以下代码：

```
openxpkiadm alias --realm democa2 --token datasafe --file vault.crt
```

## 为证书密钥创建密码文件

1 运行以下命令：

```
nano /etc/certs/openxpki_democa2/pd.pass
```

2 键入您的密码。

3 创建签名者证书。如需更多信息，请参阅[第 94 页上的“创建签名者证书”](#)。

4 使用 `openxpkiadm alias --realm democa2` 命令检查是否导入成功。

**注意：**如果您在创建证书期间更改了证书的密钥密码，请更新 `nano /etc/openxpki/config.d/realm/democa2/crypto.yaml`。

5 为第二个领域生成 CRL。如需更多信息，请参阅[第 97 页上的“生成 CRL 信息”](#)。

**注意：**确保根据领域使用了正确的 CA 证书名称。

6 发布此领域的 CRL。如需更多信息，请参阅[第 113 页上的“发布 CRL 信息”](#)。

7 使用 **openxpkictl restart** 命令重新启动 OpenXPki 服务。

## 示例输出

```
Stopping OpenXPki Stopping gracefully, 3 (sub)processes remaining... DONE.Starting
OpenXPki...OpenXPki Server is running and accepting requests.DONE.
```

## 允许同时存在具有相同主题的多个活动证书

默认情况下，在 OpenXPki 中一次只能激活一个具有相同主题名称的证书。但是，当强制执行多个命名证书时，必须同时存在具有相同主题名称的多个活动证书。

1 在 **/etc/openxpki/config.d/realm/REALM NAME/est/< REALM NAME >.yaml** 的 **policy** 部分中，将 **max\_active\_certs** 的值从 1 更改为 0。

注意：

- REALM NAME 是领域的名称。例如，**ca-one**。
- 检查脚本文件中的空格和缩进。

2 使用 **openxpkictl restart** 命令重新启动 OpenXPki 服务。

## 为 OpenXPki CA 设置默认端口号

默认情况下，Apache 在端口号 443 上侦听 https。为 OpenXPki CA 设置默认端口号以避免发生冲突。

1 在 **/etc/apache2/ports.conf** 中，将 443 端口修改为任何其他端口。例如：

### 旧内容

```
Listen 80 <IfModule ssl_module> Listen 443 </IfModule> <IfModule mod_gnutls.c> Listen 443
</IfModule>
```

### 新内容

```
Listen 80 <IfModule ssl_module> Listen 9443 </IfModule> <IfModule mod_gnutls.c> Listen 9443
</IfModule>
```

2 在 **/etc/apache2/sites-available/openxpki.conf** 中，添加或修改 **VirtualHost** 部分以映射新端口。例如，**<VirtualHost \*:443>** 更改为 **<VirtualHost \*:9443>**。

3 在 **/etc/apache2/sites-available/default-ssl.conf** 中，添加或修改 **VirtualHost\_default** 部分以映射新端口。例如，将 **<VirtualHost \*:443>** 更改为 **<VirtualHost \*:9443>**。

4 使用 **systemctl restart apache2** 命令重新启动 Apache 服务器。

注意：如果要求提供 SSL/TLS 密码，请在 EST 服务器中添加 TLS Web 服务器证书时键入密码。

5 在 **tinddopenxpkiweb01.dhcp.dev.lexmark.com:9443 (RSA)** 中，输入 SSL/TLS 密钥的密码。

要检查状态，请运行 **netstat -tlnp| grep apache**。OpenXPki SCEP URL 现在为 **https://ipaddress**，而 Web URL 为 **FQDN:9443/openxpki**。

## 启用基本身份验证

1 运行以下命令：

```
apt -y install apache2-utils
```

2 创建一个有权访问服务器的用户帐户。输入以下详细信息：

```
htpasswd -c /etc/apache2/.htpasswd <username> New password: Re-type new password: Adding password for user <username>
```

3 转到以下目录：`cd /etc/apache2/sites-enabled/`。

4 在 `nano openxpk.conf` 中，将以下行添加到 `<VirtualHost *: 443 block>` 中：

```
#HTTPS BASIC AUTH FOR LABELS Location /.well-known/est/*/simpleenroll AuthType Basic
AuthName "estrealm" AuthUserFile /etc/apache2/.htpasswd require valid-user </Location>
#HTTPS BASIC AUTH FOR NO LABEL <Location /.well-known/est/simpleenroll> AuthType Basic
AuthName "estrealm" AuthUserFile /etc/apache2/.htpasswd require valid-user </Location>
```

5 将 `ErrorDocument 401 %{unescape:%00}` 添加到同一虚拟主机块中的 `SSLEngine` 之前。

### 示例

```
ServerAlias * DocumentRoot /var/www/ ErrorDocument 401 %{unescape:%00} SSLEngine On
```

6 使用 `service apache2 restart` 命令重新启动 `apache2` 服务。

**注意：**需要使用上述用户名和密码来进行基本身份验证。

## 启用客户端证书身份验证

1 转到以下目录：`cd /etc/apache2/sites-enabled/`。

2 对于 `nano openxpk.conf` 中的必需主机，添加 `SSLVerifyClient require`。

例如，如果您使用端口 443，请将 `VirtualHost` 部分修改为：

```
<VirtualHost *:443> SSLVerifyClient require </VirtualHost>
```

3 移除 `SSLVerifyClient optional_no_ca` 命令。

4 保存该文件，然后键入 `quit` 以退出 MySQL。

5 转到以下目录：`cd /etc/openxpk/config.d/realm/democa/est`。

6 打开 `default.yaml` 和 `democa.yaml`。

**注意：**如果标签不同，则更改 YAML 文件。

7 运行以下命令：

```
vi default.yaml
```

8 在 `authorized_signer` 部分中，添加以下内容：

```
authorized_signer: rule2: subject: CN=,.
```

例如，如果您的客户端证书主题名称为 `test123`，请将以下内容添加到 `authorized_signer` 部分中：

```
authorized_signer: rule1: # Full DN subject: CN=.:pkiclient,. rule2: subject:
CN=test123,.*
```

9 保存该文件，然后键入 `quit` 以退出 MySQL。

**10** 使用 `openxpkictl restart` 命令重新启动 OpenXPKI 服务。

**11** 使用 `service apache2 restart` 命令重新启动 Apache 服务。

### 导致系统无法获取 CRL 的 SAN 不匹配错误的原因是什么？

启用 CRL 信息时可能会出现 SAN 不匹配错误。此错误表明 IP 或主机名与 Web 证书中的 SAN 值不匹配。为避免出现此错误，请在 CRL 路径中使用 FQDN，而不是使用 IP。您还可以在 SAN 字段中配置 Web 证书并使用系统的 FQDN。

### ca-signer-1 和 vault-1 令牌为何会脱机？

如果系统状态页面显示您的 ca-signer-1 和 vault-1 令牌处于脱机状态，请执行以下操作：

- 1** 在 `/etc/openxpki/config.d/realm/realm name/crypto.yaml` 中，更改对应的密钥值。
- 2** 重新启动 OpenXPKI 服务。

# 管理打印机警报

## 概述

当打印机需要关注时触发警报。当出现警报时，操作让您发送定制的电子邮件或运行脚本。事件定义在特定警报活动时执行哪些操作。要从打印机注册警报，请创建操作，然后将它们与事件相关联。将事件分配给您要监控的打印机。

**注意：**此特性不适用于安全打印机。

## 创建操作

操作是电子邮件通知或事件查看器日志。当出现打印机警报时触发分配给事件的操作。

- 1 从打印机菜单，单击**事件和操作 > 操作 > 创建**。
- 2 键入操作的唯一名称及其描述。
- 3 选择操作类型。

### 电子邮件

**注意：**在开始之前，确认电子邮件设置已配置。如需更多信息，请参阅[第 130 页上的“配置电子邮件设置”](#)。

- a 在类型菜单中，选择**电子邮件**。
- b 在字段中键入适当的值。您还可以使用可用的占位符作为主题标题的全部或一部分，或者作为电子邮件消息的一部分。如需更多信息，请参阅[第 120 页上的“理解操作占位符”](#)。

Type

E-mail

From (Optional)

admin@mycompany.com

To

scott.summers@mycompany.com

CC (Optional)

Subject (Optional)

\$ {alert.type}

alert.type

Body

\$ {alert.type}\$ {alert.location}\$ {alert.name}

alert.name

Create Action

Cancel

- c 单击**创建操作**。

## 日志事件

- a** 在类型菜单中，选择**日志事件**。
- b** 键入事件参数。您还可以在下拉菜单中使用可用的占位符。如需更多信息，请参阅[第 120 页上的“理解操作占位符”](#)。

General

Name

New Action - 2019-12-09T14:08:02+08:00

Description (Optional)

Type

Log event

Event parameters (Optional)

\$[alert.type]

Maximum length for field is 255

alert.type

alert.location

alert.state

alert.name

configurationItem.manufacturer

configurationItem.contactInformation

Create ActionCancel

- C** 单击创建操作。

## 理解操作占位符

在主题标题或电子邮件消息中使用可用的占位符。占位符代表变量元素，当使用时可用实际值替换。

- **\${eventHandler.timestamp}**—MVE 处理事件的日期和时间。例如：**2017 年 3 月 14 日下午 1:42:24**。
- **\${eventHandler.name}**—事件的名称。
- **\${configurationItem.name}**—触发警报的打印机的系统名称。
- **\${configurationItem.address}**—触发警报的打印机的 MAC 地址。
- **\${configurationItem.ipAddress}**—触发警报的打印机的 IP 地址。
- **\${configurationItem.ipHostname}**—触发警报的打印机的主机名。
- **\${configurationItem.model}**—触发警报的打印机的型号名称。
- **\${configurationItem.serialNumber}**—触发警报的打印机的序列号。
- **\${configurationItem.propertyTag}**—触发警报的打印机的属性标记。
- **\${configurationItem.contactName}**—触发警报的打印机的联系人名称。
- **\${configurationItem.contactLocation}**—触发警报的打印机的联系人位置。
- **\${configurationItem.manufacturer}**—触发警报的打印机的厂商。
- **\${alert.name}**—所触发的警报的名称。
- **\${alert.state}**—警报的状态。它可能是活动或已清除。
- **\${alert.location}**—打印机内部出现触发警报的位置。
- **\${alert.type}**—触发警报的严重性，如**警告**或**要求干预**。



## 管理操作

- 1 从“打印机”菜单，单击**事件和操作 > 操作**。
- 2 执行下面的任何操作：

### 编辑操作

- a 选择一个操作，然后单击**编辑**。
- b 配置设置。
- c 单击**保存更改**。

### 删除操作

- a 选择一个或多个操作。
- b 单击**删除**，然后确认删除。

### 测试操作

- a 选择一个操作，然后单击**测试**。
- b 要检验测试结果，请查看任务日志。

#### 注意：

- 如需更多信息，请参阅[第 127 页上的“查看日志”](#)。
- 如果您测试电子邮件操作，请检验电子邮件是否被发送给收件人。

## 创建事件

您可以监视打印机群中的警报。创建一个事件，然后设置当发生指定警报时执行的操作。事件在安全打印机中不受支持。

- 1 从“打印机”菜单，单击**事件和操作 > 事件 > 创建**。
- 2 键入事件的唯一名称及其描述。
- 3 从“警报”部分，选择一个或多个警报。如需更多信息，请参阅[第 122 页上的“理解打印机警报”](#)。
- 4 从“操作”部分，选择一个或多个操作在选定警报活动时执行。

**注意：**如需更多信息，请参阅[第 119 页上的“创建操作”](#)。

- 5 让系统能够在打印机上清除警报时执行选定的操作。
- 6 设置在执行任何选定操作之前的宽限期。

**注意：**如果警报在宽限期内清除，那么不会执行该操作。

- 7 单击**创建事件**。

## 理解打印机警报

当打印机需要关注时触发警报。以下警报可以与 MVE 中的一个事件相关联：

- **自动文档传送器 (ADF) 卡纸**—纸张卡在 ADF 中，必须物理移除。
  - 扫描仪 ADF 出口卡纸
  - 扫描仪 ADF 进纸器卡纸
  - 扫描仪 ADF 反相器卡纸
  - 扫描仪 ADF 纸张已清理
  - 扫描仪 ADF 缺少纸张
  - 扫描仪 ADF 预对准卡纸
  - 扫描仪 ADF 对准卡纸
  - 扫描仪警报 - 如果重新启动作业，请放回所有原件
- **盖门或盖板打开**—打印机上的盖门打开，必须关闭。
  - 检查盖门/盖板 - 邮箱
  - 盖门打开
  - 盖板警报
  - 盖板关闭
  - 盖板打开
  - 盖板打开或缺少碳粉盒
  - 双面打印盖板打开
  - 扫描仪 ADF 盖板打开
  - 扫描仪卡纸通道盖板打开
- **不正确的介质尺寸或类型**—正在打印作业，要求在进纸匣中加载特定的纸张。
  - 不正确的信封尺寸
  - 不正确的手动进纸
  - 不正确的介质
  - 不正确的介质尺寸
  - 加载介质
- **内存已满或错误**—打印机内存不足，必须应用更改。
  - 复杂页面
  - 文件将被删除
  - 逐份打印内存不足
  - 整理闪存碎片内存不足
  - 传真内存不足
  - 内存不足
  - 内存不足 - 挂起作业可能丢失
  - 用于资源保存的内存不足
  - 内存已满
  - PS 内存不足
  - 扫描仪太多页面 - 扫描作业已取消
  - 分辨率降低

- **选件故障**—连接到打印机的选件处于错误状态。选件包括输入选件、输出选件、字体卡、用户闪存卡、硬盘和完成器。
  - 检查对齐/连接
  - 检查双面打印连接
  - 检查完成器/邮箱安装
  - 检查电源
  - 损坏的选件
  - 有故障的选件
  - 分离设备
  - 双面打印警报
  - 缺少双面打印进纸匣
  - 外部网络适配器丢失
  - 完成器警报
  - 完成器盖门或互锁打开
  - 完成器挡纸墙打开
  - 不兼容的双面打印设备
  - 不兼容的输入设备
  - 不兼容的输出设备
  - 不兼容的未知设备
  - 不正确的选件安装
  - 输入警报
  - 输入配置错误
  - 选件警报
  - 接纸架已满
  - 接纸架即将满
  - 输出配置错误
  - 选件已满
  - 缺少选件
  - 缺少进纸机构
  - 选件上的打印作业
  - 重新连接设备
  - 重新连接输出设备
  - 安装的输入太多
  - 安装的选件太多
  - 安装的输出太多
  - 缺少进纸匣
  - 在加电期间缺少进纸匣
  - 进纸匣检测错误
  - 未校准的输入
  - 未格式化的选件

- 不支持的选件
- 重新连接输入设备
- **卡纸**—纸张卡在打印机中，必须物理移除。
  - 内部卡纸
  - 卡纸警报
  - 卡纸
- **扫描仪错误**—扫描仪有问题。
  - 扫描仪背后电缆已拔出
  - 扫描仪支架已锁定
  - 扫描仪清洁平板玻璃/背衬条
  - 扫描仪已禁用
  - 扫描仪平板盖板打开
  - 扫描仪前部电缆已拔出
  - 扫描仪无效的扫描仪对准
- **耗材错误**—打印机耗材有问题。
  - 异常的耗材
  - 碳粉盒使用地区不匹配
  - 有故障的耗材
  - 缺少定影部件或涂覆辊
  - 无效或缺少的左侧碳粉盒
  - 无效或缺少的右侧碳粉盒
  - 无效的耗材
  - 调试失败
  - 耗材警报
  - 耗材卡纸
  - 缺少耗材
  - 碳粉盒弹出手柄已拉出
  - 碳粉盒安装不正确
  - 未校准的耗材
  - 未许可的耗材
  - 不支持的耗材
- **耗材或消耗品已空**—必须更换打印机耗材。
  - 输入已空
  - 使用寿命已耗尽
  - 打印机准备好维护
  - 预定维护
  - 耗材已空
  - 耗材已满
  - 耗材已满或缺少

**注意：**打印机将警报发送为错误和警告。如果其中一个警报被触发，那么它的关联操作会发生两次。

- **耗材或消耗品不足**—打印机耗材供应不足。

- 预警
- 第一个不足
- 输入不足
- 使用寿命警告
- 即将为空
- 即将不足
- 耗材不足
- 耗材即将满

- **未分类的警报或条件**

- 色彩校正失败
- 数据传输错误
- 引擎 **CRC** 失败
- 外部警报
- 传真连接丢失
- 风扇停转
- 十六进制活动
- 插入双面打印页并按“转到”
- 内部警报
- 内部网络适配器需要服务
- 逻辑单元警报
- 脱机
- 脱机警告提示
- 操作失败
- 操作者干预警报
- 页面错误
- 端口警报
- 端口通信失败
- 端口已禁用
- 省电模式
- 电源关闭
- **PS** 作业超时
- **PS** 手动超时
- 要求设置
- **SIMM** 校验和错误
- 耗材校准
- 碳粉补丁检测失败
- 未知的警报条件
- 未知的配置
- 未知的扫描仪警报条件

- 用户被锁定
- 警告警报

## 管理事件

- 1 从“打印机”菜单，单击**事件和操作 > 事件**。
- 2 请执行下面的任一操作：

### 编辑事件

- a 选择一个事件，然后单击**编辑**。
- b 配置设置。
- c 单击**保存更改**。

### 删除事件

- a 选择一个或多个事件。
- b 单击**删除**，然后确认删除。

## 查看任务状态和记录

### 概述

任务是在 MVE 中执行的任何打印机管理活动，如打印机发现、审核和配置执行。状态页显示当前正在运行的所有任务的状态以及在过去 72 小时内运行的任务。当前正在运行的任务的信息会被输入到日志中。超过 72 小时的任务只能在日志页面中查看单独的日志输入项，并且可以使用任务 ID 进行搜索。

### 查看任务状态

从“任务”菜单，单击**状态**。

**注意：**任务状态会实时更新。

### 停止任务

- 1 从“任务”菜单，单击**状态**。
- 2 从“当前运行的任务”部分，选择一个或多个任务。
- 3 单击**停止**。

### 查看日志

- 1 从“任务”菜单，单击**日志**。
- 2 选择任务类别、任务类型或时间段。

**注意：**

- 使用搜索字段来搜索多个任务 ID。使用逗号来分隔多个任务 ID 或使用连字符来指示范围。例如：**11、23、30-35**。
- 要导出搜索结果，请单击**导出到 CSV**。

### 清除日志

- 1 从“任务”菜单，单击**日志**。
- 2 单击**清除日志**，然后选择一个日期。
- 3 单击**清除日志**。

### 导出日志

- 1 从任务菜单，单击**日志**。
- 2 选择任务类别、任务类型或时间段。
- 3 单击**导出到 CSV**。

# 调度任务

## 创建时间表

- 1 从任务菜单，单击**时间表 > 创建**。
- 2 从常规部分，键入预定任务的唯一名称及其描述。
- 3 从任务部分，执行以下操作之一：

### 预定审核

- a 选择**审核**。
- b 选择一个保存搜索。

### 预定一致性检查

- a 选择**一致性**。
- b 选择一个保存搜索。

### 预定打印机状态检查

- a 选择**当前状态**。
- b 选择一个保存搜索。
- c 选择一个操作。

### 预定配置部署

- a 选择**部署文件**。
- b 选择一个保存搜索。
- c 浏览文件，然后选择文件类型。
- d 如果需要，请选择部署方法或协议。

### 调度发现

- a 选择**发现**。
- b 选择一个发现配置文件。

### 预定配置执行

- a 选择**执行**。
- b 选择一个保存搜索。

### 预定证书验证

选择**验证证书**。

**注意：**在验证期间，MVE 与 CA 服务器通信以下载证书链和证书吊销列表 (CRL)。还生成注册代理证书。此证书使 CA 服务器能够信任 MVE。



## 预定视图导出

- a** 选择视图导出。
  - b** 选择一个保存搜索。
  - c** 选择一个视图模板。
  - d** 键入导出文件所发送到的电子邮件地址列表。
- 4** 从时间表部分，设置任务的日期、时间和频率。
- 5** 单击**创建预定任务**。

## 管理预定任务

- 1** 从任务菜单，单击**时间表**。
- 2** 请执行下面的任一操作：

### 编辑预定任务

- a** 选择一个任务，然后单击**编辑**。
- b** 配置设置。
- c** 单击**编辑预定任务**。

**注意：**在编辑预定任务时会移除“上次运行”信息。

### 删除预定任务

- a** 选择一个任务，然后单击**删除**。
- b** 单击**删除预定任务**。

## 执行其他管理任务

### 配置常规设置

1 在页面的右上角，单击 .

2 单击**常规**，然后选择一个主机名来源。

- **打印机**—系统从打印机检索主机名。
- **反向 DNS 查询**—系统使用 IP 地址从 DNS 表格检索主机名。

3 设置警报重新注册频率。

**注意：**在进行更改（如重新启动或更新固件）时，打印机可能会丢失警报注册状态。MVE 会在警报重新注册频率中设定的下一个间隔尝试自动恢复状态。

4 单击**保存更改**。

### 配置电子邮件设置

启用 SMTP 配置以让 MVE 通过电子邮件发送数据导出文件和事件通知。

1 单击页面右上角的 .

2 单击**电子邮件**，然后选择**启用电子邮件 SMTP 配置**。

3 键入 SMTP 邮件服务器和端口。

4 选择适当的加密。

**注意：**

- 对于 SSL 加密，请选择端口 465。
- 对于 TLS/STARTTLS 加密，请选择端口 587。

5 键入发件人的电子邮件地址。

6 如果用户必须在发送电子邮件之前登录，请选择**需要登录**，然后键入用户凭证。

7 单击**保存更改**。

### 添加登录免责声明

您可以配置登录免责声明在用户使用新会话登录时显示。用户在访问 MVE 之前必须接受免责声明。

1 在页面的右上角，单击 .

2 单击**免责声明**，然后选择**在登录之前启用免责声明**。

3 键入免责声明文本。

4 单击**保存更改**。

## 签署 MVE 证书

“安全套接字层 (SSL)”或“传输层安全性 (TLS)”是一种安全协议，使用数据加密和证书验证来保护服务器-客户端通信。在 MVE 中，TLS 用于保护 MVE 服务器和 Web 浏览器之间共享的敏感信息。受保护的信息可以是打印机密码、安全策略、MVE 用户凭证或打印机验证信息（如 LDAP 或 Kerberos）。

TLS 使 MVE 服务器和 Web 浏览器能够在发送数据之前对其进行加密，然后在收到数据后将其解密。SSL 还要求服务器向 Web 浏览器展示证书，证明服务器是它声称的对象。此证书是自签名的或使用受信任的第三方 CA 签名。默认情况下，MVE 配置为使用自签名证书。

### 1 下载证书签名请求。

- a 在页面的右上角单击 .
- b 单击 **TLS > 下载**。
- c 选择**证书签名请求**。

**注意：**证书签名请求包括“主题备用名称 (SAN)”。

### 2 使用受信任的 CA 签署证书签名请求。

### 3 安装 CA 签名证书。

- a 在页面的右上角单击 .
- b 单击 **TLS > 安装签名证书**。
- c 上载 CA 签名证书，然后单击**安装证书**。
- d 单击**重新启动 MVE 服务**。

**注意：**重新启动 MVE 服务会重新启动系统，服务器可能在接下来的几分钟内无法使用。在重新启动服务之前，确保没有当前正在运行的任务。

## 移除用户信息和引用

MVE 符合“一般数据保护条例 (GDPR)”下的数据保护规则。MVE 可以配置为应用被遗忘的权限并从系统中移除私人用户信息。

### 移除用户

- 1 在页面的右上角单击 .
- 2 单击**用户**，然后选择一个或多个用户。
- 3 单击**删除 > 删除用户**。

### 移除 LDAP 中的用户引用

- 1 在页面的右上角单击 .
- 2 单击 **LDAP**。
- 3 移除搜索过滤器和绑定设置中的任何用户相关信息。

## 移除电子邮件服务器中的用户引用

- 1 在页面的右上角单击 。
- 2 单击**电子邮件**。
- 3 移除用于通过电子邮件服务器进行身份验证的任何用户相关信息，如用户凭证。

## 移除任务日志中的用户引用

如需更多信息，请参阅[第 127 页上的“清除日志”](#)。

## 移除配置中的用户引用

- 1 从配置菜单，单击**所有配置**。
- 2 单击配置名称。
- 3 从基本选项卡，移除打印机设置中任何与用户相关的值，如联系人名称和联系人位置。

## 移除高级安全组件中的用户引用

- 1 从配置菜单，单击**所有高级安全组件**。
- 2 单击组件名称。
- 3 从高级安全设置部分，移除任何与用户相关的值。

## 移除保存搜索中的用户引用

- 1 从打印机菜单，单击**保存搜索**。
- 2 单击一个保存搜索。
- 3 移除使用任何用户相关值的任何搜索规则，如联系人名称和联系人位置。

## 移除关键字中的用户引用

- 1 从打印机菜单，单击**打印机列表**。
- 2 从打印机取消用户相关关键字的分配。
- 3 从打印机菜单，单击**关键字**。
- 4 移除使用用户相关信息的任何关键字。

## 移除事件和操作中的用户引用

- 1 从打印机菜单，单击**事件和操作**。
- 2 移除包含对用户的电子邮件引用的任何操作。

## 常见问题解答

### Markvision Enterprise 常见问题解答

#### 为什么我不能在创建配置时在支持的型号列表中选择多台打印机？

打印机型号之间的配置设置和命令有所不同。

#### 其他用户能够访问我的保存搜索吗？

是的。所有用户都可以访问保存搜索。

#### 我可以在哪里找到日志文件？

您可以在安装 MVE 的用户的隐藏目录中找到安装日志文件。例如：**C:\Users\Administrator\AppData\Local\Temp\mveLexmark-install.log**。

您可以在 **installation\_dir\Lexmark\Markvision Enterprise\tomcat\logs** 文件夹中查找 \*.log 应用程序日志文件，其中 **installation\_dir** 是 MVE 的安装文件夹。

#### 主机名和反向 DNS 查询之间的区别是什么？

主机名是分配给网络上的打印机的唯一名称。每一个主机名对应于一个 IP 地址。“反向 DNS 查询”被用于确定给定 IP 地址的指定用户名和域名。

#### 在 MVE 中，哪里可以找到“反向 DNS 查询”？

可以在常规设置中找到“反向 DNS 查询”。如需更多信息，请参阅[第 130 页上的“配置常规设置”](#)。

#### 如何将规则手动添加到 Windows 防火墙？

以管理员身份运行命令提示符，然后键入以下内容：

```
firewall add allowedprogram "installation_dir/Lexmark/Markvision  
Enterprise/tomcat/bin/tomcat9.exe" "Markvision Enterprise Tomcat"  
firewall add portopening UDP 9187 "Markvision Enterprise NPA UDP"  
firewall add portopening UDP 6100 "Markvision Enterprise LST UDP"
```

其中 **installation\_dir** 是 MVE 的安装文件夹。

#### 如何设置 MVE 以使用端口 443 以外的端口？

1 停止 Markvision Enterprise 服务。

a 打开运行对话框，然后键入 **services.msc**。

b 用鼠标右键单击 **Markvision Enterprise**，然后单击**停止**。

2 打开 **installation\_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml** 文件。

其中 **installation\_dir** 是 MVE 的安装文件夹。

### 3 将连接器端口值更改为另一个未使用的端口。

```
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
compression="on" compressableMimeType="text/html,text/xml,text/plain,text/css,
text/javascript,application/javascript,application/json" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" enableLookups="false"
acceptCount="100" connectionTimeout="120000" disableUploadTimeout="true"
URIEncoding="UTF-8" server="Apache" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLS" keystoreFile="C:/Program Files/Lexmark/Markvision Enterprise/
../mve_truststore.p12" keystorePass="markvision" keyAlias="mve" keyPass="markvision"
keystoreType="PKCS12" ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA"/>
```

### 4 将 **redirectPort** 值更改为与连接器端口使用相同的端口号。

```
<Connector port="9788" maxHttpHeaderSize="16384" maxThreads="150" minSpareThreads="25"
enableLookups="false" redirectPort="443" acceptCount="100" connectionTimeout="120000"
disableUploadTimeout="true" compression="on" compressableMimeType="text/html,text/xml,
text/plain,text/css,text/javascript,application/javascript,application/json"
URIEncoding="UTF-8" server="Apache"/>
```

### 5 重新启动 Markvision Enterprise 服务。

- a 打开运行对话框，然后键入 **services.msc**。
- b 用鼠标右键单击 **Markvision Enterprise**，然后单击**重新启动**。

### 6 使用新端口访问 MVE。

例如，打开 Web 浏览器，然后键入 **https://MVE\_SERVER:port/mve**。

其中 **MVE\_SERVER** 是托管 MVE 的服务器的主机名或 IP 地址，而 **port** 是连接器端口号。

## 如何定制 MVE 使用的密码和 TLS 版本？

### 1 停止 Markvision Enterprise 服务。

- a 打开运行对话框，然后键入 **services.msc**。
- b 用鼠标右键单击 **Markvision Enterprise**，然后单击**停止**。

### 2 打开 **installation\_dir\Lexmark\Markvision Enterprise\tomcat\conf\server.xml** 文件。

其中 **installation\_dir** 是 MVE 的安装文件夹。

### 3 配置密码和 TLS 版本。

如需有关配置的更多信息，请参阅 [Apache Tomcat SSL/TLS configuration instructions](#)。

如需有关协议和密码值的更多信息，请参阅

[Apache Tomcat SSL support information documentation](#)。

### 4 重新启动 Markvision Enterprise 服务。

- a 打开运行对话框，然后键入 **services.msc**。
- b 用鼠标右键单击 **Markvision Enterprise**，然后单击**重新启动**。

## 使用 Microsoft CA 企业版时如何管理 CRL 文件？

### 1 从 CA 服务器获取 CRL 文件。

注意：

- 对于 Microsoft CA 企业版，CRL 不会自动通过 SCEP 下载。

- 如需更多信息，请参阅 *Microsoft 证书颁发机构配置指南*。

**2** 将 CRL 文件保存在 `installation_dir\Lexmark\Markvision Enterprise\apps\library\crl` 文件夹中，其中 `installation_dir` 是 MVE 的安装文件夹。

**3** 在 MVE 中配置证书颁发机构。

**注意：**此过程仅适用于使用的 SCEP 协议。

## 疑难解答

### 用户已经忘记密码

#### 重置用户密码

您需要管理权限才能重置密码。

- 1 在页面的右上角，单击 。
- 2 单击**用户**，然后选择一个用户。
- 3 单击**编辑**，然后更改密码。
- 4 单击**保存更改**。

如果您忘记了自己的密码，请执行下面的任一操作：

- 联系另一个管理员用户来重置密码。
- 联系 Lexmark 客户支持中心。

### 管理员用户已经忘记密码

#### 创建另一个管理员用户，然后删除以前的帐户

您可以使用“Markvision Enterprise 密码实用程序”创建另一个管理员用户。

- 1 浏览安装 Markvision Enterprise 的文件夹。  
例如：**C:\Program Files\**
- 2 启动 Lexmark\Markvision Enterprise\ 目录中的 **mvepwdutility-windows.exe** 文件。
- 3 选择语言，然后单击**确定** > 下一步。
- 4 选择添加用户帐户 > 下一步。
- 5 输入用户凭证。
- 6 单击下一步。
- 7 访问 MVE，然后删除以前的管理员用户。

**注意：**如需更多信息，请参阅[第 28 页上的“管理用户”](#)。



## 页面未加载

如果您在未注销的情况下关闭了 Web 浏览器，可能会出现此问题。

请尝试下列办法中的一个或多个：

清除缓存，并删除 Web 浏览器中的 cookie

访问 MVE 登录页面，然后使用您的凭证登录

打开 Web 浏览器，然后键入 **https://MVE\_SERVER/mve/login**，其中 **MVE\_SERVER** 是托管 MVE 的服务器的主机名或 IP 地址。

## 不能发现网络打印机

请尝试下列办法中的一个或多个：

确认打印机的电源已经打开

确认电源线牢固地插入打印机和正确接地的电源插座中

确认打印机已连接到网络

重新启动打印机

确认在您的打印机上启用 TCP/IP

确认 MVE 使用的端口已打开，并且 SNMP 和 mDNS 已启用

如需更多信息，请参阅[第 141 页上的“理解端口和协议”](#)。

联系 Lexmark 代表

## 不正确的打印机信息

执行审核

如需更多信息，请参阅[第 56 页上的“审核打印机”](#)。

## MVE 没有将打印机识别为安全打印机

确保打印机是安全的

如需有关保护打印机的更多信息，请参阅 *Markvision Enterprise* 和 *打印机安全性* 文档。

确保 mDNS 已打开且未被阻止

删除打印机，然后重新运行打印机发现

如需更多信息，请参阅[第 31 页上的“发现打印机”](#)。

## 对多个应用程序执行配置在第一次尝试中失败，但在随后的尝试中成功

### 增加超时

- 1 浏览安装 Markvision Enterprise 的文件夹。

例如: **C:\Program Files\**

- 2 导航至 Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes 文件夹。

- 3 使用文本编辑器，打开 *platform.properties* 文件。

- 4 编辑 **cdcl.ws.readTimeout** 值。

**注意：**该值以毫秒为单位。例如，90000 毫秒等于 90 秒。

- 5 使用文本编辑器，打开 *devCom.properties* 文件。

- 6 编辑 **lst.responseTimeoutsRetries** 值。

**注意：**该值以毫秒为单位。例如，10000 毫秒等于 10 秒。

例如: **lst.responseTimeoutsRetries=10000 15000 20000**。第一次连接重试在 10 秒之后，第二次连接重试在 15 秒之后，第三次连接重试在 20 秒之后。

- 7 如果需要，当您使用 LDAP GSSAPI 时，请创建 *parameters.properties* 文件。

添加以下设置: **lst.negotiation.timeout=400**

**注意：**该值以秒为单位。

- 8 保存更改。

## 使用打印机证书执行配置失败

有时，在执行期间不颁发新证书。

### 增加注册重试次数

在 **platform.properties** 文件中添加以下主键:

```
enrol.maxEnrolmentRetry=10
```

重试值必须大于 5。

# OpenXPki 证书颁发机构

## 使用 OpenXPki CA 服务器颁发证书失败

确保 MVE 中的“代表签名者”密钥与 CA 服务器中的授权签名者密钥匹配

例如：

如果以下是 MVE 中 **platform.properties** 文件中的 **ca.onBehalf.cn** 密钥，

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

那么以下必须是 CA 服务器中 **generic.yaml** 文件中的 **authorized\_signer** 密钥。

```
rule1:
    # Full DN
    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

如需有关配置 OpenXPki CA 服务器的更多信息，请参阅 *OpenXPki 证书颁发机构配置指南*。

## 发生内部服务器错误

安装 **en\_US.utf8** 区域设置

- 1 运行 **dpkg-reconfigure locales** 命令。
- 2 安装 **en\_US.utf8** (locale -a | grep en\_US) 区域设置。

## 登录提示没有出现

当访问 **http://yourhost/openxpki/** 时，您只会获得 Open Source Trustcenter 横幅，而没有登录提示。

启用 **fcgid**

运行以下命令：

- 1 **a2enmod fcgid**
- 2 **service apache2 restart**

## 发生没有类的嵌套连接器错误

在 **/usr/share/perl5/Connector/Multi.pm** 第 201 行上出现 **EXCEPTION: Nested connector without class (scep.scep-server-1.connector.initial)** 错误。

更新 **scep.scep-server-1**

在 **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml** 中，将 **scep.scep-server-1** 替换为 **scep.generic**。

**注意：**使用您的领域的名称替换 **REALM**。例如，当使用默认领域时，请使用 **ca-one**。

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## 无法手动批准证书

当手动批准证书时，手动批准按钮不会出现。

### 更新 **scep.scep-server-1**

在 `/etc/openxpki/config.d/realm/REALM/scep/generic.yaml` 中，将 **scep.scep-server-1** 替换为 **scep.generic**。

**注意：**使用您的领域的名称替换 **REALM**。例如，当使用默认领域时，请使用 **ca-one**。

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## 当批准注册请求时发生 Perl 错误

### 更新 **scep.scep-server-1**

在 `/etc/openxpki/config.d/realm/REALM/scep/generic.yaml` 中，将 **scep.scep-server-1** 替换为 **scep.generic**。

**注意：**使用您的领域的名称替换 **REALM**。例如，当使用默认领域时，请使用 **ca-one**。

```
eligible:
  initial:
    value@: connector:scep.generic.connector.initial
```

## **ca-signer-1** 和 **vault-1** 令牌脱机

系统状态页显示 **ca-signer-1** 和 **vault-1** 令牌脱机。

请尝试下列办法中的一个或多个：

### 更改证书密钥密码

在 `/etc/openxpki/config.d/realm/ca-one/crypto.yaml` 中更改证书密钥密码。

### 创建正确的符号链接并复制密钥文件

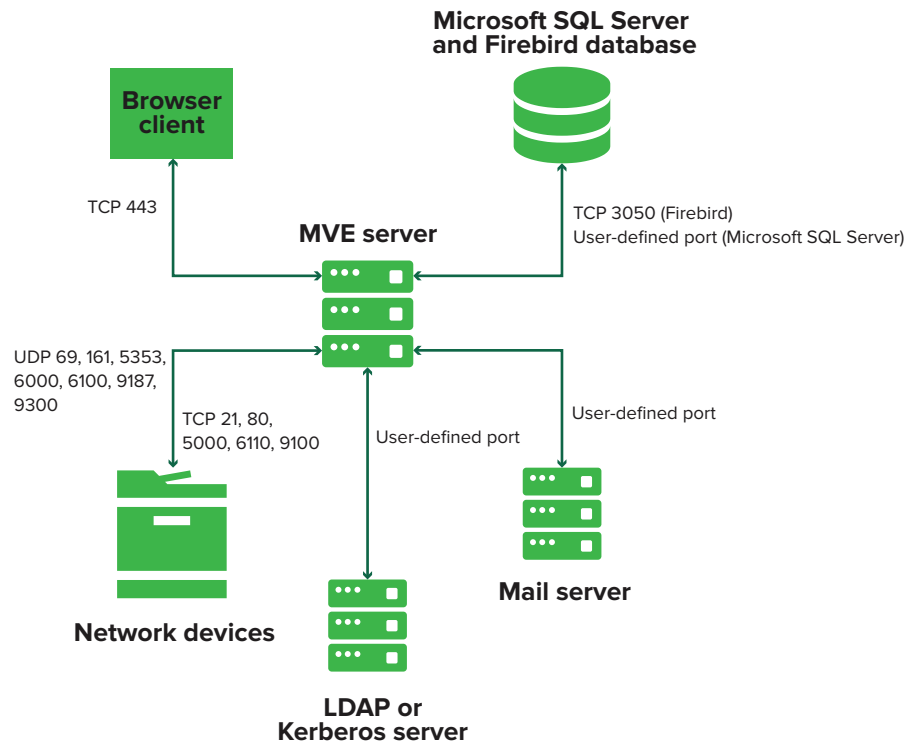
如需更多信息，请参阅[第 96 页上的“复制密钥文件并创建符号链接”](#)。

### 确保密钥文件由 OpenXPki 可读

# 附录

## 理解端口和协议

MVE 将不同的端口和协议用于几种类型的网络通信，如下图中所示：



注意：

- 端口是双向的，并且必须打开或活动才能让 MVE 正常运行。确认所有打印机端口都已启用。
- 一些通信需要临时端口，这是服务器上分配的可用端口范围。当客户端请求临时通信会话时，服务器会分配一个动态端口给客户端。该端口仅在短时间内有效，当之前的会话到期时它可以变为可用以便重新使用。

## 服务器到打印机通信

在从 MVE 服务器到网络打印机的通信期间使用的端口和协议

| 协议                 | MVE 服务器                                  | 打印机                          | 用于                     |
|--------------------|------------------------------------------|------------------------------|------------------------|
| 网络打印联盟协议 (NPAP)    | UDP 9187                                 | UDP 9300                     | 与 Lexmark 网络打印机通信。     |
| XML 网络传输 (XMLNT)   | UDP 9187                                 | UDP 6000                     | 与一些 Lexmark 网络打印机通信。   |
| Lexmark 安全传输 (LST) | UDP 6100<br>临时传输控制协议 (TCP)<br>端口<br>(握手) | UDP 6100<br>TCP 6110<br>(握手) | 与一些 Lexmark 网络打印机安全通信。 |

| 协议                      | MVE 服务器            | 打印机                | 用于                                                                 |
|-------------------------|--------------------|--------------------|--------------------------------------------------------------------|
| 多点传送域名系统 (mDNS)         | 临时用户数据报协议 (UDP) 端口 | UDP 5353           | 发现 Lexmark 网络打印机并确定打印机的安全性能。<br><b>注意：</b> 需要这个端口来允许 MVE 与安全打印机通信。 |
| 简单网络管理协议 (SNMP)         | 临时 UDP 端口          | UDP 161            | 发现并与 Lexmark 和第三方网络打印机通信。                                          |
| 文件传输协议 (FTP)            | 临时 TCP 端口          | TCP 21<br>TCP 20   | 部署文件。                                                              |
| 超文本传输协议 (HTTP)          | 临时 TCP 端口          | TCP 80             | 部署文件或执行配置。                                                         |
|                         |                    | TCP 443            | 部署文件或执行配置。                                                         |
| 通过 SSL 的超文本传输协议 (HTTPS) | 临时 TCP 端口          | TCP 161<br>TCP 443 | 部署文件或执行配置。                                                         |
| RAW                     | 临时 TCP 端口          | TCP 9100           | 部署文件或执行配置。                                                         |

## 打印机到服务器通信

在从网络打印机到 MVE 服务器的通信期间使用的端口和协议

| 协议   | 打印机      | MVE 服务器  | 用于      |
|------|----------|----------|---------|
| NPAP | UDP 9300 | UDP 9187 | 生成和接收警报 |

## 服务器到数据库通信

在从 MVE 服务器到数据库的通信期间使用的端口

| MVE 服务器   | 数据库                     | 用于                  |
|-----------|-------------------------|---------------------|
| 临时 TCP 端口 | 用户定义的端口。默认端口是 TCP 1433。 | 与 SQL Server 数据库通信。 |
| 临时 TCP 端口 | TCP 3050                | 与 Firebird 数据库通信。   |

## 客户端到服务器通信

在从浏览器客户端到 MVE 服务器的通信期间使用的端口和协议

| 协议                      | 浏览器客户端 | MVE 服务器 |
|-------------------------|--------|---------|
| 通过 SSL 的超文本传输协议 (HTTPS) | TCP 端口 | TCP 443 |

## 服务器到邮件服务器通信

在从 MVE 服务器到邮件服务器的通信期间使用的端口和协议

| 协议              | MVE 服务器   | SMTP 服务器              | 用于                   |
|-----------------|-----------|-----------------------|----------------------|
| 简单邮件传输协议 (SMTP) | 临时 TCP 端口 | 用户定义的端口。默认端口是 TCP 25。 | 提供电子邮件功能，用于从打印机接收警报。 |

# 服务器到 LDAP 服务器通信

在从 MVE 服务器到 LDAP 服务器的涉及用户组和验证功能的通信期间使用的端口和协议

| 协议                    | MVE 服务器   | LDAP 服务器               | 用于                           |
|-----------------------|-----------|------------------------|------------------------------|
| 轻量级目录访问协议 (LDAP)      | 临时 TCP 端口 | 用户定义的端口。默认端口是 TCP 389。 | 使用 LDAP 服务器验证 MVE 用户。        |
| TLS 轻量级目录访问协议 (LDAPS) | 临时 TCP 端口 | 用户定义的端口。默认端口是 TCP 636。 | 使用 LDAP 服务器通过 TLS 验证 MVE 用户。 |
| Kerberos              | 临时 UDP 端口 | 用户定义的端口。默认端口是 UDP 88。  | 使用 Kerberos 验证 MVE 用户。       |

# 在 Microsoft CA 中启用证书请求的自动批准

默认情况下，所有 CA 服务器都处于挂起模式，您必须手动批准每个签名证书请求。由于此方法对于批量请求不可行，因此启用签名证书的自动批准。

- 1 从“服务器管理器”，单击工具 > 证书颁发机构。
- 2 从左侧面板，用鼠标右键单击 CA，然后单击属性 > 策略模块。
- 3 从证书处理选项卡，单击如果适用，遵循证书模板中的设置，然后单击确定。

**注意：**如果选择将证书请求状态设置为挂起，则必须手动批准证书。

- 4 重新启动 CA 服务。

# 吊销证书

**注意：**在开始之前，请确保为 CRL 配置了 CA 服务器并且它们可用。

- 1 从 CA 服务器，打开证书颁发机构。
- 2 从左侧面板，展开 CA，然后单击已发布证书。
- 3 用鼠标右键单击要吊销的证书，然后单击所有任务 > 吊销证书。
- 4 选择原因代码以及吊销的日期和时间，然后单击是。
- 5 从左侧面板，用鼠标右键单击已吊销证书，然后单击所有任务 > 发布。

**注意：**确保您吊销的证书在已吊销证书中。

您可以在 CRL 中看到已吊销证书的序列号。

## 注意事项

### 版本注意事项

2022 年 9 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，请转到 <http://support.lexmark.com>。

如需有关管理本产品使用的 Lexmark 隐私策略的信息，请转到 [www.lexmark.com/privacy](http://www.lexmark.com/privacy)。

如需有关耗材和下载资源的信息，请转到 [www.lexmark.com](http://www.lexmark.com)。

© 2017 Lexmark International, Inc.

保留所有权利。

### 商标

Lexmark、Lexmark 徽标和 Markvision 是 Lexmark International, Inc. 在美国和/或其他国家的商标或注册商标。

Windows、Microsoft、Microsoft Edge、PowerShell、SQL Server 和 Windows Server 是微软集团公司的商标。

Firebird 是 Firebird Foundation 的注册商标。

Google Chrome 是 Google LLC 的商标。

Apple 和 Safari 是 Apple Inc 的注册商标。

Java 是 Oracle 和/或其关联机构的注册商标。

所有其他商标的所有权属于它们各自的所有者。

## GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.



## JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

\*\* JmDNS

## 许可注意事项

所有与此产品关联的许可注意事项可以从程序文件夹查看。

# 术语表

|        |                                                                               |
|--------|-------------------------------------------------------------------------------|
| 操作     | 电子邮件通知或命令行操作。当出现打印机警报时触发分配给事件的操作。                                             |
| 审核     | 收集打印机数据，如打印机状态、耗材和功能的任务。                                                      |
| 配置     | 设置的集合，可以被分配并执行到一台打印机或一组打印机型号。在配置中，您可以修改打印机设置并部署应用程序、许可证、固件和 <b>CA</b> 证书到打印机。 |
| 发现配置文件 | 包含一组参数，用于在网络上查找打印机的配置文件。它可能还包含预定义的配置，可以在发现过程中自动分配并执行到打印机。                     |
| 事件     | 定义在特定警报活动时执行哪些操作。                                                             |
| 关键字    | 分配给打印机的自定义文本，您可以用于在系统中搜索这些打印机。使用关键字筛选搜索时，将仅显示以该关键字标记的打印机。                     |
| 安全打印机  | 配置为通过加密通道通信，并要求验证才能访问其功能或应用程序的打印机。                                            |
| 令牌     | 在配置中代表变量设置的打印机数据值的标识符。                                                        |
| 变量设置   | 一组打印机设置，包含的动态值可以集成到配置中。                                                       |

# 索引

## A

- 访问 MVE 22
- 操作
  - 占位符 120
- 操作占位符
  - 理解 120
- 操作
  - 创建 119
  - 删除 121
  - 编辑 121
  - 管理 121
  - 测试 121
- 添加登录免责声明 130
- 在证书中添加客户端身份验证 EKU 103
- 管理员用户已经忘记密码 136
- 高级安全组件
  - 创建 65
- AES256 加密
  - 配置 133
- AIA
  - 配置 76
- 应用程序日志文件
  - 定位 133
- 应用程序
  - 卸载 59
- 应用程序软件包
  - 创建 67
- 分配关键字 60
- 分配配置到打印机 57
- 分配事件到打印机 59
- 审核打印机 56
- 验证
  - 客户端证书 82
  - 用户名和密码 82
  - Windows 集成 82
- 验证方法 82
- 颁发机构信息访问
  - 配置 76
- 自动证书管理
  - 配置 71
- 自动证书管理特性 69
- 证书请求的自动批准
  - 在 Microsoft CA 中启用 143
  - 在 OpenXPKI CA 中启用 99, 113

## B

- 备份和还原数据库 23
- 基本身份验证
  - 启用 117
- 最佳实践 12

## C

- ca-signer-1 脱机
  - 疑难解答 140
- 无法发现网络打印机 137
- 无法手动批准证书 140
- CA 证书下载
  - 更改详细信息以启用 114
- CDP
  - 配置 76
- CEP
  - 配置 84, 85, 88
  - 安装 84
- CEP 和 CES 服务器
  - 创建 SSL 证书 81
- 使用 OpenXPKI CA 服务器颁发证书失败 139
- 证书密钥密码
  - 使之可用于 openXPKI 111
- 证书密钥
  - 创建密码文件 94, 109, 115
- 证书管理 69
- Microsoft CA 中的证书请求
  - 自动批准 143
- OpenXPKI CA 中的证书请求
  - 自动批准 99, 113
- 不带质询密码的证书请求
  - 在 OpenXPKI CA 中拒绝 103
- 证书模板 81
  - 创建 78
- NDES 的证书模板
  - 设置 78
- 证书
  - 创建 100, 115
  - 导入 96
  - 吊销 104, 143
  - 具有相同主题的证书
    - 启用 116
  - 证书分发点
    - 配置 76
- CES
  - 配置 85, 86, 89
  - 安装 84
- 质询密码
  - 在 Microsoft CA 服务器中禁用 79
- 修改记录 7
- 安装后更改安装程序设置 26
- 更改语言 22
- 更改打印机列表视图 43
- 更改密码 22
- 检查打印机与配置的一致性 58
- 密码
  - 定制 133
- 清除日志 127
- 客户端身份验证 EKU
  - 在证书中添加 103
- 客户端证书 87
- 客户端证书身份验证 82
- 克隆配置
  - 示例场景 65
- 彩色打印权限
  - 配置 66
- 配置
  - 一致性 58
  - 创建 62, 64
  - 导出 68
  - 导入 68
- 配置设置
  - 可打印版本 66
- 配置
  - 分配 57
  - 执行 57
  - 管理 62
  - 取消分配 57
- 配置颁发机构信息访问设置 76
- 配置 CEP 84, 85, 88
- 配置证书分发点设置 76
- 配置 CES 85, 86, 89
- 配置 CRL 可访问性 77, 98
- 为多个领域配置 EST 端点 114
- 配置电子邮件设置 130
- 配置常规设置 130
- 使用 NDES 配置 Microsoft 企业 CA
  - 概述 72, 74
- 为自动证书管理配置 MVE 71
- 配置 NDES 服务器 77
- 配置网络设备注册服务服务器 77
- 手动配置 OpenXPKI CA 93, 108

- 使用默认脚本配置 OpenXPKI CA 92, 107
- 手动配置打印机证书 60
- 配置打印机安全性 54
- 配置根 CA 服务器概述 73
- 为多个领域配置 SCEP 端点 102
- 配置从属 CA 服务器概述 75
- 配置彩色打印权限 66
- 一致性
  - 检查 58
- 连接性要求 80
- 复制目录 100
- 复制发现配置文件 33
- 复制密钥文件 96
- 复制保存搜索 49
- 复制目录 114
- 复制视图 41
- 创建配置 62
- 从打印机创建配置 64
- 创建自定义保存搜索 45
- 创建发现配置文件 31
- 创建时间表 128
- 创建操作 119
- 从打印机创建高级安全组件 65
- 创建应用程序软件包 67
- 创建事件 121
- 创建证书模板 78, 81
- 创建证书 100
- 创建客户端证书 87
- 创建关键字 43
- 创建 OpenSSL 配置文件 93
- 为证书密钥创建密码文件 94, 115
- 创建根 CA 证书 94
- 创建 SCEP 证书 95
- 创建签名者证书 94
- 创建 SSL 证书
  - CEP 和 CES 服务器 81
- 创建符号链接 96
- 创建保管库证书 95
- 凭证
  - 输入 60
- CRL
  - 发布 104
- CRL 可访问性
  - 配置 77, 98
- CRL 信息
  - 生成 97, 112
  - 发布 113
- CSV
  - 变量设置 66

- 自定义保存搜索
  - 创建 45

## D

- 仪表板
  - 访问 35
- 数据库
  - 备份 23
  - 要求 14
  - 还原 23
  - 设置 18
- 数据库要求 14
- 默认配置 51
- 默认端口号
  - 为 OpenXPKI CA 更改 116
  - 为 OpenXPKI CA 设置 103
- OpenXPKI CA 的默认端口号
  - 更改 116
- 委派
  - 启用 83
  - 要求 83
- 委派要求 83
- 删除操作 121
- 删除发现配置文件 33
- 删除关键字 43
- 删除保存搜索 49
- 删除时间表 129
- 删除视图 41
- 部署文件到打印机 58
- 设备一致性检查
  - 管理 35
- 设备安全信息
  - 管理 35
- 目录
  - 复制和设置 114
- 在 Microsoft CA 服务器中禁用质询密码 79
- 发现打印机 33
- 发现配置文件
  - 创建 31
- 发现配置文件
  - 复制 33
  - 删除 33
  - 编辑 33
  - 管理 33
  - 运行 33
- 动态设置
  - 理解 66

## E

- 编辑操作 121

- 编辑发现配置文件 33
- 编辑关键字 43
- 编辑保存搜索 49
- 编辑时间表 129
- 编辑视图 41
- 嵌入式 Web 服务器
  - 查看 56
- 在 Microsoft CA 中启用证书请求的自动批准 143
- 在 OpenXPKI CA 中启用证书请求的自动批准 99
- 启用基本身份验证 117
- 启用 LDAP 服务器验证 28
- 启用多个活动证书
  - 相同主题 102
- 启用 SCEP 服务 98
- 启用签名者代表证书 99
- 对多个应用程序执行配置在第一次尝试中失败，但在随后的尝试中成功 138
- 使用打印机证书执行配置失败 138
- 执行配置 57
- 将凭证输入到安全打印机 60
- EST 端点
  - 为多个领域配置 114
- 事件
  - 创建 121
- 事件
  - 分配 59
  - 删除 126
  - 编辑 126
  - 管理 126
- 导出 CSV
  - 变量设置 66
- 导出日志 127
- 导出打印机数据 40
- 电子邮件操作 119
- 电子邮件设置
  - 配置 130

## F

- FAQ 118
- 文件
  - 部署 58
- 使用搜索栏筛选打印机 43
- Firebird 数据库 18
- 常见问题解答 118
- 完整的证书科目
  - 通过 SCEP 请求 103
- 功能访问控制
  - 理解 53

**G**

常规设置  
  配置 130  
生成 CRL 信息 97  
当通过 SCEP 请求时获得完整的  
证书科目 103

**H**

主机名查询  
  反向查询 133

**I**

导入证书 96  
导入 CSV  
  变量设置 66  
将文件导入资源库 68  
将文件导入资源库 68  
导入或导出配置 68  
不正确的打印机信息 137  
安装日志文件  
  定位 133  
安装程序设置  
  更改 26  
安装 LDAP 服务器证书 30  
安装 MVE 19  
无提示安装 MVE 19  
安装 OpenXPKI CA 90, 105  
安装根 CA 服务器 73  
安装从属 CA 服务器 75  
内部服务器错误 139

**K**

密钥文件  
  复制 96  
关键字  
  分配 60  
关键字  
  创建 43  
  删除 43  
  编辑 43  
  管理 43

**L**

语言  
  更改 22  
语言  
  支持的 15  
LDAP 服务器  
  启用验证 28

**LDAP 服务器证书**

  安装 30  
  日志事件操作 119  
  日志文件  
    定位 133  
  登录免责声明  
    添加 130  
  登录提示没有出现 139  
  日志  
    清除 127  
    导出 127  
    查看 127

**M**

管理操作 121  
管理配置 62  
管理发现配置文件 33  
管理事件 126  
管理关键字 43  
管理打印机警报概述 119  
管理保存搜索 49  
管理时间表 129  
管理用户 28  
管理视图 41  
Markvision Enterprise  
  理解 11  
Microsoft 企业 CA  
  配置 133  
Microsoft 企业 CA, 使用 NDES  
  配置 72, 74  
Microsoft SQL Server 18  
监控打印机 49  
具有相同主题的多个活动证书  
  启用 116  
MVE  
  访问 22  
  安装 19  
  升级 23  
MVE 证书  
  签名 131  
MVE 没有将打印机识别为安全打  
  印机 137  
MVE 无提示安装 19

**N**

NDES 服务器  
  配置 77  
没有类的嵌套连接器错误 139  
网络连接性要求 80  
网络设备注册服务服务器  
  配置 77

**O**

OpenSSL 配置文件  
  创建 93, 108  
OpenXPKI  
  启动 97, 111  
OpenXPKI CA  
  手动配置 93, 108  
  使用默认脚本配置 92, 107  
  安装 90, 105  
OpenXPKI CA 默认端口号  
  更改 116  
概述  
  配置根 CA 服务器 73  
  配置从属 CA 服务器 75  
  管理配置 62  
  管理打印机警报 119  
Markvision Enterprise 11  
  安全仪表板 35  
  设置用户访问 27  
  查看任务状态和记录 127

**P**

页面正在无限加载 137  
密码  
  更改 22  
  重置 136  
证书密钥的密码文件  
  创建 94, 109, 115  
Perl 错误 140  
权限  
  理解 53  
占位符 119  
端口  
  配置 133  
  理解 141  
打印机  
  一致性 58  
  重新启动 56  
打印机警报  
  理解 122  
打印机证书  
  手动配置 60  
打印机通信  
  保护 55  
打印机数据  
  导出 40  
打印机固件  
  更新 59  
打印机信息  
  查看 40

## 打印机生命周期状态

- 理解 43
- 打印机列表
  - 查看 37
- 打印机列表视图
  - 更改 43
- 打印机安全性
  - 配置 54
- 打印机安全状态
  - 理解 51
- 打印机状态
  - 设置 56
- 打印机状态
  - 更新 56
- 打印机
  - 审核 56
  - 部署文件 58
  - 发现 33
  - 事件 59
  - 筛选 43
  - 移除 61
  - 保护 51, 55
- 协议
  - 理解 141
- 发布 CRL 104

**R**

- 在 OpenXPKI CA 中拒绝不带质询密码的证书请求 103
- 移除打印机 61
- 移除用户信息和引用 131
- 要求
  - 网络连接性 80
  - 系统 80
- 资源库
  - 导入文件到 68
- 重新启动打印机 56
- 反向 DNS 查询 133
- 吊销证书 104, 143
- 根 CA 证书
  - 创建 94, 109
- 根 CA 服务器
  - 安装 73
- run-as 用户
  - 设置 18
- 运行保存搜索 45
- 运行发现配置文件 33

**S**

- 克隆配置的示例场景 65

## 保存搜索

- 访问 133
- 复制 49
- 删除 49
- 编辑 49
- 管理 49
- 运行 45
- SCEP 证书
  - 创建 95
- SCEP 端点
  - 为多个领域配置 102
- SCEP 服务
  - 启用 98
- 时间表
  - 创建 128
- 时间表
  - 删除 129
  - 编辑 129
  - 管理 129
- 搜索栏
  - 筛选打印机 43
- 搜索规则
  - 运算符 46
  - 参数 46
- 搜索规则设置
  - 理解 46
- 安全打印机
  - 正在验证 60
- 保护设备群中的打印机通信 55
- 保护打印机 55
- 使用默认配置保护打印机 51
- 设置默认视图 41
- 为 NDES 设置证书模板 78
- 为 OpenXPKI CA 设置默认端口号 103
- 设置目录 100
- 设置目录 114
- 设置打印机状态 56
- 将 MVE 设置为 run-as 用户 18
- 设置数据库 18
- 设置用户访问概述 27
- 设置 Web 服务器 111
- 签名者证书
  - 创建 94, 109, 115
- 签名者代表证书
  - 启用 99
- 签署 MVE 证书 131
- 无提示安装
  - MVE 19
- 简单证书注册协议
  - 启用 98

## SSL 证书

- 创建 81
- 启动 OpenXPKI 97
- 停止任务 127
- 从属 CA 服务器
  - 安装 75
- 支持的数据库 14
- 支持的语言 15
- 支持的型号
  - 配置 133
- 支持的操作系统 14
- 支持的打印机型号 15
- 支持的服务器 14
- 支持的 Web 浏览器 14
- 符号链接
  - 创建 96
- 系统要求 80

**T**

- 任务状态
  - 查看 127
- 任务
  - 停止 127
- 测试操作 121
- TLS 版本
  - 定制 133
- 疑难解答
  - 管理员用户已经忘记密码 136
  - ca-signer-1 脱机 140
  - 无法发现网络打印机 137
  - 无法手动批准证书 140
  - 使用 OpenXPKI CA 服务器颁发证书失败 139
  - 对多个应用程序执行配置在第一次尝试中失败，但在随后的尝试中成功 138
  - 使用打印机证书执行配置失败 138
  - 不正确的打印机信息 137
  - 内部服务器错误 139
  - 登录提示没有出现 139
  - MVE 没有将打印机识别为安全打印机 137
  - 没有类的嵌套连接器错误 139
  - 页面正在无限加载 137
  - Perl 错误 140
  - 用户忘记了密码 136
  - vault-1 脱机 140

**U**

- 取消配置分配 57

- 理解操作占位符 120
- 理解打印机警报 122
- 理解打印机生命周期状态 43
- 理解用户角色 27
- 从打印机卸载应用程序 59
- 更新打印机状态 56
- 更新打印机固件 59
- 升级到 **MVE** 的最新版本 23
- 用户忘记了密码 136
- 用户信息
  - 移除 131
- 用户名和密码身份验证 82
- 用户角色
  - 理解 27
- 用户系统
  - 要求 14
- 用户系统要求 14
- 用户
  - 添加 28
  - 删除 28
  - 编辑 28
  - 管理 28

## V

- 变量设置
  - 理解 66
- 保管库证书
  - 创建 95, 110
- vault-1** 脱机
  - 疑难解答 140
- 查看日志 127
- 查看任务状态和记录概述 127
- 查看打印机“嵌入式 **Web** 服务器” 56
- 查看打印机信息 40
- 查看打印机列表 37
- 查看任务状态 127
- 视图
  - 复制 41
  - 删除 41
  - 编辑 41
  - 管理 41

## W

- Web** 证书
  - 创建 110
- Web** 服务器
  - 要求 14
- Web** 服务器要求 14
- Web** 服务器
  - 设置 111

- Windows** 防火墙
  - 添加规则 133
- Windows** 集成身份验证 82