Markvision Enterprise

Versão 4,2

Guia do administrador

Setembro de 2022 **www.lexmark.com**

Conteúdo

Histórico de alterações..... 8

Visão geral.....12

Noções básicas sobre o Markvision Enterprise.....12

Primeiros passos..... 13

Práticas recomendadas..... 13
Requisitos de sistema..... 15
Idiomas compatíveis.....16
Modelos de impressora suportados..... 16
Configuração do banco de dados.....19
Configuração de usuários "executar como"..... 20
Instalação do MVE..... 20
Instalação silenciosa do MVE.....21
Acessando o MVE..... 23
Alterando o idioma.....24
Alterando a sua senha..... 24

Manutenção do aplicativo..... 25

Atualização para o MVE 4.2..... 25
Backup e restauração do banco de dados..... 26
Atualizando as definições do instalador após a instalação..... 28

Configuração do acesso do usuário..... 29

Visão geral..... 29
Compreendendo funções de usuário.....29
Gerenciamento de usuários..... 30
Ativação da autenticação do servidor LDAP.....31
Instalando certificados de servidor LDAP.....33

Descoberta de impressoras..... 34

Criação de perfis de descoberta.....34
Gerenciando perfis de localização..... 36
Amostra de cenários: Descoberta de impressoras..... 37

Gerenciamento do painel de segurança..... 38

Visão geral..... 38
Acessar o painel de segurança..... 38
Gerenciamento de Informações de segurança do dispositivo..... 38
Gerenciamento da Verificação de conformidade do dispositivo..... 39

Exibição de impressoras..... 40

Visualização da lista de impressoras..... 40
Visualizando as informações da impressora..... 43
Exportando dados da impressora..... 44
Gerenciamento de exibições..... 44
Alterando a exibição de lista de impressoras..... 46
filtrando impressoras usando a barra de pesquisa..... 46
Gerenciamento de palavras-chave..... 47
Uso das pesquisas salvas..... 47
Compreendendo os estados do ciclo de vida útil da impressora..... 47
Como executar uma pesquisa salva..... 49
Criação de uma pesquisa salva..... 49
Noções básicas sobre as configurações de critérios de pesquisa..... 51
Gerenciando pesquisas salvas..... 53
Amostra de cenários: Monitoramento dos níveis de toner de sua frota..... 54

Proteção das comunicações da impressora..... 55

Noções básicas sobre os estados de segurança da impressora..... 55
Proteção das impressoras usando as configurações padrão..... 56
Compreensão dos controles de acesso a funções e permissões..... 58
Configurando a segurança da impressora..... 59
Proteção das comunicações da impressora no parque de impressão..... 59
Outras maneiras de proteger suas impressoras..... 60

Gerenciamento de impressoras..... 61

Reiniciando a impressora..... 61
Exibindo o Embedded Web Server da impressora..... 61
Auditando impressoras..... 61
Atualização do status da impressora..... 61
Configurando o estado da impressora..... 62
Como atribuir configurações a impressoras..... 62

Cancelando atribuições de configurações..... 62
Aplicando configurações..... 62
Verificando a conformidade da impressora com uma configuração..... 63
Implantando arquivos em impressoras..... 63
Atualizando o firmware da impressora..... 64
Desinstalação de aplicativos das impressoras..... 65
Atribuindo eventos a impressoras..... 65
Atribuindo palavras-chave a impressoras..... 65
Inserindo credenciais em impressoras protegidas..... 66
Configuração manual dos certificados da impressora padrão..... 66
Remoção de impressoras..... 67

Gerenciamento de configurações..... 68

Visão geral..... 68
Criação de configurações..... 68
Criando uma configuração a partir de uma impressora..... 71
Amostra de cenários: Clonagem de uma configuração..... 71
Criação de um componente de segurança avançada a partir de uma impressora..... 72
Geração de uma versão para impressão das definições de configuração..... 72
Noções básicas sobre configurações dinâmicas..... 72
Aprendendo sobre definições de variável..... 72
Configurando as permissões de impressão colorida..... 73
Criando um pacote de aplicativos..... 74
Importando ou exportando uma configuração..... 74
Importação de arquivos para a biblioteca de recursos..... 75

Gerenciamento de certificados..... 76

Configuração do MVE para o gerenciamento automático de certificados..... 76
Noções básicas sobre o recurso de gerenciamento automatizado de certificados..... 76
Configuração do MVE para gerenciamento automatizado de certificados..... 78
Configuração do Microsoft Enterprise CA com NDES..... 80
Gerenciamento de certificados usando a autoridade de certificações da Microsoft pelo SCEP..... 81
Visão geral..... 81
Instalação do servidor CA raiz..... 81
Configuração do Microsoft Enterprise CA com NDES..... 82
Configuração do servidor CA subordinado..... 83
Definição das configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade..... 84

Configuração da acessibilidade da CRL ... 85
Configuração do servidor do NDES ... 85
Configuração do NDES para MVE ... 86
Gerenciando certificados usando a autoridade de certificações da Microsoft pelo MSCEWS ... 88
Requisitos de sistema ... 88
Requisitos de conectividade de rede ... 88
Criando certificados SSL para servidores de CEP e CES ... 89
Criando modelos de certificado ... 90
Noções básicas sobre métodos de autenticação ... 90
Requisitos de delegação ... 91
Configuração da autenticação integrada do Windows ... 92
Configuração da autenticação do certificado do cliente ... 95
Configuração da autenticação de nome de usuário e senha ... 97
Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo SCEP ... 99
Configuração do OpenXPKI CA ... 99
Configuração manual do OpenXPKI CA ... 103
Geração de informações do CRL ... 108
Configuração da acessibilidade da CRL ... 108
Ativação do serviço SCEP ... 109
Ativação do certificado Signatário em nome de (agente de inscrição) ... 109
Ativação da aprovação automática de solicitações de certificado no OpenXPKI CA ... 110
Criação de um segundo realm ... 111
Ativando vários certificados ativos com a mesma entidade a estar presente por vez ... 114
Configuração do número de portas padrão para OpenXPKI CA ... 114
Rejeitando solicitações de certificado sem Senha de desafio na AC do OpenXPKI ... 114
Adição de EKU de autenticação de cliente em certificados ... 115
Obtenção de entidades de certificado completo ao solicitar pelo SCEP ... 115
Revogando certificados e publicando o CRL ... 116
Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo EST ... 117
Configuração do OpenXPKI CA ... 117
Configuração manual do OpenXPKI CA ... 120
Criação de um segundo realm ... 129

Gerenciamento de alertas da impressora ... 135

Visão geral ... 135
Como criar uma ação ... 135
Compreendendo espaços reservados de ação ... 136
Gerenciamento de ações ... 137
Criação de um evento ... 137
Compreendendo alertas da impressora ... 138

Gerenciando eventos....142

Exibição do status e do histórico das tarefas....143

Visão geral....143
Visualizando o status da tarefa....143
Interrupção de tarefas....143
Exibindo registros....143
Limpando registros....143
Exportando registros....144

Programação de tarefas....145

Como criar uma programação....145
Gerenciando tarefas programadas....146

Execução de outras tarefas administrativas....147

Configurando as definições gerais....147
Definição das configurações de e-mail....147
Adição de isenção de responsabilidade no login....148
Assinatura do certificado do MVE....148
Removendo informações e referências de usuário....149

Perguntas frequentes....151

Perguntas frequentes do Markvision Enterprise....151

Solução de problemas....154

O usuário esqueceu a senha....154
O usuário Administrador esqueceu a senha....154
A página não carrega....155
Não é possível detectar uma impressora de rede....155
Informações incorretas de impressora....155
O MVE não reconhece uma impressora como segura....156
A aplicação de configurações com vários aplicativos falha na primeira tentativa, mas é bem-sucedida nas tentativas seguintes....156
Falha na aplicação de configurações com certificado da impressora....157
Autoridade de certificações OpenXPKI....157

Apêndice....160

Avisos..... 164

Glossário..... 166

Índice..... 167

Histórico de alterações

Agosto de 2022

- Informações adicionadas sobre:
  - Protocolo EST (Enrollment over Secure Transport, inscrição em transporte seguro) conforme definido no RFC 7030
  - Painel de segurança
  - Atribuição automática de palavras-chave durante a descoberta
  - Suporte para e-mail sobre SSL/TLS
  - Suporte para Windows Server 2022
- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Gerenciamento de certificados usando a CA da Microsoft por meio do Serviço da Web de registro de certificado da Microsoft (MSCEWS)
  - Configuração do servidor de AC OpenXPKI
  - Gerenciamento de configurações do MVE

Março de 2022

- Informações atualizadas sobre os modelos de impressora suportados.
- Adição de informações sobre como criar um certificado do cliente.

Maio de 2021

- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Gerenciamento da autoridade de certificações (CA) da Microsoft
  - Configuração do Markvision™ Enterprise (MVE) para o gerenciamento automatizado de certificados
  - Configuração da CA (Certificate Authority, autoridade de certificações) corporativa da Microsoft usando o NDES (Network Device Enrollment Service, serviço de registro de dispositivo de rede) da Microsoft
- Informações adicionadas sobre:
  - Gerenciamento de certificados usando a CA da Microsoft por meio do Serviço da Web de registro de certificado da Microsoft (MSCEWS)
  - Criação do certificado SSL para os servidores de Serviço da Web de política de registro de certificado (CEP) e Serviço da Web de registro de certificado (CES)
  - Métodos de autenticação para CEP e CES
  - Certificado nomeado do dispositivo

Novembro de 2020

- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Bancos de dados suportados

- Informações adicionadas sobre:
  - Gerenciamento e implementação de configurações
  - Backup e restauração do banco de dados
  - Gerenciamento de certificados usando o OpenXPKI e a autoridade de certificação da Microsoft
- Suporte adicional para:
  - Gerenciamento e implementação de configurações em um grupo de modelos de impressora
  - Criação de nomes de banco de dados personalizados

Fevereiro de 2020

- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Servidores suportados
  - Bancos de dados suportados
  - Caminho de upgrade do MVE válido
- Informações adicionadas sobre:
  - Instruções para práticas recomendadas
  - Instruções sobre como gerenciar certificados automatizados
  - Componentes de segurança avançada padrão e suas configurações
  - Outras maneiras de proteger impressoras
  - Amostra de cenários

Junho de 2019

- Informações atualizadas sobre os seguintes itens:
  - Notas de rodapé adicionadas aos modelos de impressora que requerem certificados
  - Atribuição de direitos dbo ao configurar o banco de dados
  - Caminho de upgrade válido ao fazer upgrade para a versão 3.4
  - Arquivos necessários ao fazer backup e restaurar o banco de dados
  - Configurações de autenticação do servidor LDAP
  - Status de validade, datas e parâmetros de fuso horário do certificado são adicionados às configurações de critérios de pesquisa
  - Configuração dos controles de acesso a funções e permissões nas configurações de segurança da impressora
  - Seleção de um arquivo de firmware da biblioteca de recursos ao atualizar o firmware da impressora
  - Seleção da data de início, do horário de início e de pausa e dos dias da semana ao atualizar o firmware da impressora
  - Gerenciamento de configurações
- Informações adicionadas sobre:
  - Noções básicas sobre os estados de segurança da impressora
  - Configuração de componentes de segurança avançada
  - Criação de componentes de segurança avançada a partir de uma impressora
  - Geração de uma versão para impressão das definições de configuração
  - Upload de autoridade de certificação do parque de impressão

- Remoção de informações e referências do usuário
- Noções básicas sobre os controles de acesso a funções e permissões
- Etapas de solução de problemas ao aplicar configurações com várias falhas de aplicativos
- Etapas de solução de problemas quando um usuário Administrador tiver esquecido a senha

Agosto de 2018

- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Configuração do banco de dados
  - Upgrade para o MVE 3.3
  - Perguntas frequentes
  - Criação de ações
  - Criação de programações
- Informações adicionadas sobre:
  - Configuração de contas de usuário de domínio “executar como”
  - Exportação de registros
  - Etapas de solução de problemas quando o MVE não reconhece impressoras protegidas

Julho de 2018

- Informações atualizadas sobre upgrade para o MVE 3.2.

Abril de 2018

- Informações atualizadas sobre os seguintes itens:
  - Modelos de impressora suportados
  - Configuração do banco de dados
  - Backup e restauração de arquivos de banco de dados
  - O URL para acessar o MVE
  - Noções básicas sobre configurações de variáveis
- Informações adicionadas sobre:
  - Configuração de certificados da impressora
  - Interrupção de tarefas
  - Atualização do firmware da impressora

Setembro de 2017

- Informações atualizadas sobre os seguintes itens:
  - Requisitos de sistema
  - Comunicação entre o MVE e os modelos de Impressoras de Formulários Lexmark™ 2580, 2581, 2590 e 2591
  - Como arrastar manualmente bancos de dados do Microsoft SQL Server
  - Backup e restauração de arquivos de banco de dados

- Configurações de segurança obrigatórias para os controles de acesso a funções ao implantar arquivos de firmware e de soluções em impressoras
- Suporte para licenças durante a implantação de aplicativos
- Alertas da impressora e suas ações associadas
- Recuperação automática do estado da impressora
- Atribuições de eventos e palavras-chave

Junho de 2017

- Lançamento da documentação inicial do MVE 3.0.

Visão geral

Noções básicas sobre o Markvision Enterprise

Markvision Enterprise (MVE) é um software utilitário de gerenciamento de impressora baseado na web projetado para profissionais de TI.

Com o MVE, você pode gerenciar um grande parque de impressão em um ambiente empresarial, de forma eficiente, executando os procedimentos a seguir:

- Localizar, organizar e controlar um parque de impressão. Você pode auditar uma impressora para coletar dados dela, como status, configurações e suprimentos.
- Criar configurações e atribuí-las às impressoras.
- Implementar firmware, certificados de impressora, CA (Certificate Authority, autoridade de certificações) e aplicativos às impressoras.
- Monitorar eventos e alertas da impressora.

Este documento apresenta informações sobre como configurar e usar o aplicativo e solucionar eventuais problemas.

Este documento destina-se a administradores.

Primeiros passos

Práticas recomendadas

Este tópico descreve as etapas recomendadas para usar o MVE no gerenciamento eficaz de sua frota.

1. Instale o MVE em seu ambiente.
   a. Crie um servidor usando o ambiente mais recente do Windows Server.

      Conteúdo relacionado:
      - **Requisitos do servidor da Web**

   b. Crie uma conta de usuário de domínio que não tenha acesso de administrador.

      Conteúdo relacionado:
      - **Configuração de um usuário "executar como"**

   c. Crie um banco de dados do Microsoft SQL Server, configure a criptografia e, em seguida, dê acesso à nova conta de usuário aos bancos de dados.

      Conteúdo relacionado:
      - **Requisitos de banco de dados**
      - **Configuração do banco de dados**

   d. Instale o MVE usando a conta de usuário do domínio e o servidor SQL com Autenticação do Windows.

      Conteúdo relacionado:
      - **Instalação do MVE**

2. Configure o MVE e, em seguida, descubra e organize sua frota.
   a. Assine o certificado do servidor.

      Conteúdo relacionado:
      - **Assinatura do certificado do MVE**
      - **Configuração do MVE para gerenciar certificados automaticamente**

   b. Configure as definições de LDAP.

      Conteúdo relacionado:
      - **Ativação da autenticação do servidor LDAP**
      - **Instalação de certificados LDAP**

   c. Conecte-se a um servidor de e-mail.

      Conteúdo relacionado:
      - **Configuração das definições de e-mail**

   d. Descubra sua frota.

      Conteúdo relacionado:
      - **Descoberta de impressoras**

   e. Programe auditorias e atualizações de status.

      Conteúdo relacionado:
      - **Como auditar impressoras**
      - **Atualização do status da impressora**

f Configure as definições básicas, como nomes de contato, locais, etiquetas de ativos e fusos horários.

g Organize sua frota. Use palavras-chave, como locais, para categorizar as impressoras.

Conteúdo relacionado:

- **Atribuição de palavras-chave a impressoras**
- **Criação de uma pesquisa salva**

3 Proteja sua frota.

a Proteja o acesso à impressora usando os componentes de segurança avançada padrão.

Conteúdo relacionado:

- **Proteção de impressoras usando as configurações padrão**
- **Compreensão dos controles de acesso a funções e permissões**
- **Outras maneiras de proteger suas impressoras**

b Crie uma configuração segura que inclua certificados.

Conteúdo relacionado:

- **Como criar uma configuração**
- **Importação de arquivos para a biblioteca de recursos**

c Aplique a configuração em sua frota atual.

Conteúdo relacionado:

- **Como atribuir configurações a impressoras**
- **Aplicação de configurações**

d Programe aplicações e verificações de conformidade.

Conteúdo relacionado:

Como criar uma programação

e Adicione configurações aos perfis de descoberta para proteger novas impressoras.

Conteúdo relacionado:

Como criar um perfil de descoberta

f Assine certificados da impressora.

Conteúdo relacionado:

Assinatura do certificado do MVE

4 Mantenha o firmware atualizado.

Conteúdo relacionado:

Atualização do firmware da impressora

5 Instale e configure aplicativos.

Conteúdo relacionado:

- **Como criar uma configuração**
- **Importação de arquivos para a biblioteca de recursos**

6 Monitore sua frota.

Conteúdo relacionado:

Criação de uma pesquisa salva

Requisitos de sistema

O MVE é instalado como um servidor da Web e pode ser acessado de um navegador da Web em qualquer computador na rede. O MVE também usa um banco de dados para armazenar informações sobre o parque de impressão. As listas a seguir são os requisitos para o servidor da Web, o banco de dados e o sistema do usuário:

Requisitos do servidor da Web

Processador	No mínimo um processador dual core de 2 GHz que usa Tecnologia Hyper-Threading (HTT)
RAM	No mínimo 4 GB
Unidade de disco rígido	No mínimo 60GB

Nota: Não é possível executar o MVE, o Lexmark Document Distributor (LDD) e o Utilitário de Implantação de Dispositivos (DDU) ao mesmo tempo.

Servidores suportados

- Windows Server 2022 Standard Edition
- Windows Server 2019
- Windows Server 2016 Standard Edition
- Windows Server 2012 Standard Edition
- Windows Server 2012 R2

  Nota: O MVE oferece suporte à virtualização para os servidores suportados em um ambiente baseado no local.

Requisitos de banco de dados

Bancos de dados suportados

- Firebird® banco de dados (integrado)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

  Nota: O tamanho mínimo recomendado dos bancos de dados é de 60 GB para alocar 20 MB para o FRAMEWORK e 4,5 MB para MONITOR e QUARTZ. Para obter mais informações, consulte " Configuração do banco de dados" na página 19.

Requisitos do sistema do usuário

Navegadores da Web suportados

- Microsoft Edge
- Mozilla Firefox (versão mais recente)
- Google Chrome™ (versão mais recente)
- Apple Safari (versão mais recente)

Resolução da tela

Pelo menos 1280 x 768 pixels

Idiomas compatíveis

- Português (Brasil)
- Inglês
- French
- German
- Italian
- Chinês Simplificado
- Espanhol

Modelos de impressora suportados

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

- Lexmark CS943[2]
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX331[2]
- Lexmark CX421[2], CX522[2], CX622[2], CX625[2]
- Lexmark CX431[2]
- Lexmark CX532[2]
- Lexmark CX625[2]
- Lexmark CX635[2]
- Lexmark CX725[2]
- Lexmark CX728[2]
- Lexmark CX730[2]
- Lexmark CX735[2]
- Lexmark CX820[2], CX825[2], CX827[2], CX860[2]
- Lexmark CX920[2], CX921[2], CX922[2], CX923[2], CX924[2], CX927[2]
- Lexmark CX930[2], CX931[2]
- Lexmark CX942[2], CX943[2], CX944[2]
- Impressoras de formulários Lexmark 2580[4], 2581[4], 2590[4], 2591[4]
- Lexmark M1140, M1145, M3150
- Lexmark M1242[2], M1246[2], M3250[2], M5255[2], M5265[2], M5270[2]
- Lexmark M3350[2]
- Lexmark M5155, M5163, M5170
- Lexmark M5255[2], M5265[2], M5270[2]
- Lexmark MB2236[2]
- Lexmark MB2338[2], MB2442[2], MB2546[2], MB2650[2], MB2770[2]
- Lexmark MB3442[2]
- Lexmark MC2325[2], MC2425[2], MC2535[2], MC2640[2]
- Lexmark MC3224[2]
- Lexmark MC3326[2]
- Lexmark MC3426[2]
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321[2], MS421[2], MS521[2], MS621[2], MS622[2]
- Lexmark MS331[2], MS431[2]
- Lexmark MS531[2], MS631[2], MS632[2]
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725[2], MS821[2], MS822[2], MS823[2], MS824[2], MS825[2], MS826[2]
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611
- Lexmark MX317, MX417, MX517

- Lexmark MX321[2], MX421[2], MX521[2], MX522[2], MX622[2]
- Lexmark MX331[2], MX431[2]
- Lexmark MX432[2]
- Lexmark MX532[2], MX632[2]
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721[2], MX722[2], MX725[2], MX822[2], MX824[2], MX826[2]
- Lexmark MX910, MX911, MX912
- Lexmark MX931[2]
- Lexmark T650[1], T652[1], T654[1], T656[1]
- Lexmark X651[1], X652[1], X654[1], X656[1], X658[1], XS651[1], XS652[1], XS654[1], XS658[1]
- Lexmark X746, X748, X792
- Lexmark X850[1], X852[1], X854[1], X860[1], X862[1], X864[1], XS864[1]
- Lexmark X925, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235[2], XC2240[2], XC4240[2]
- Lexmark XC2335[2]
- Lexmark XC4140[2], XC4150[2], XC6152[2], XC8155[2], XC8160[2]
- Lexmark XC9225[2], XC9235[2], XC9245[2], XC9255[2], XC9265[2]
- Lexmark XC9325[2], XC9335[2]
- Lexmark XC9445[2], XC9455[2], XC9465[2]
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242[2], XM1246[2], XM3250[2]
- Lexmark XM3142[2]
- Lexmark XM3350[2]
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365[2], XM5370[2]
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355[2], MX7365[2], MX7370[2]
- Lexmark XM9145, XM9155, XM9165
- Lexmark XM9335[2]
- Lexmark XC2326
- Lexmark XC2326
- Lexmark XC4342[2], XC4352[2]

[1] É necessário atualizar o certificado da impressora. Nesta versão, a segurança da plataforma Java e a atualização de desempenho removem o suporte para alguns algoritmos de assinatura de certificado como MD5 e SHA1. Essa alteração evita que o MVE opere com algumas impressoras. Para obter mais informações, consulte a **documentação de informações de ajuda**.

[2] O suporte a SNMPv3 deve estar habilitado na impressora.

[3] Se uma senha de segurança avançada estiver configurada na impressora, o MVE não será compatível com a impressora.

[4] O MVE não consegue se comunicar com as Impressoras de Formulários Lexmark modelos 2580, 2581, 2590 e 2591 que estejam no estado Não pronta. A comunicação funciona apenas quando o MVE já tiver se comunicado com a impressora no estado Pronta anteriormente. A impressora pode ficar no estado Não pronta quando houver erros ou avisos, como suprimentos vazios. Para alterar o estado, solucione o erro ou aviso e, em seguida, pressione **Pronto**.

Configuração do banco de dados

Você pode utilizar tanto o Firebird como o Microsoft SQL Server como banco de dados de back-end. A tabela a seguir pode ajudar você a decidir qual banco de dados usar.

	Firebird	Microsoft SQL Server
Instalação do servidor	Deve ser instalado no mesmo servidor que o MVE.	Pode ser executado em qualquer servidor.
Comunicação	Bloqueado para apenas localhost (host local).	Comunica-se por uma porta estática ou por uma instância de nomeação dinâmica. A comunicação SSL/TLS com um servidor Microsoft SQL seguro é suportada.
Desempenho	Mostra problemas de desempenho em parques de impressão grandes.	Mostra o melhor desempenho para parques de impressão grandes.
Tamanho do banco de dados	Os tamanhos padrão dos bancos de dados são de 6 MB para FRAMEWORK e 1 MB para MONITOR e QUARTZ. A tabela de FRAMEWORK aumenta em 1 KB para cada registro de impressora adicionado.	Os tamanhos padrão dos bancos de dados são de 20 MB para FRAMEWORK e 4,5 MB para MONITOR e QUARTZ. A tabela de FRAMEWORK aumenta em 1 KB para cada registro de impressora adicionado.
Configuração	Configurado automaticamente durante a instalação.	Requer configuração na pré-instalação.

Se você estiver usando o Firebird, o instalador MVE instala e configura o Firebird sem nenhuma outra configuração necessária.

Se estiver usando o Microsoft SQL Server, antes de instalar o MVE, execute os procedimentos a seguir:

- Permita que o aplicativo seja executado automaticamente.
- Defina as bibliotecas de rede para que usem soquetes TCP/IP.
- Crie os seguintes bancos de dados:

  Nota: Os nomes de banco de dados a seguir são padrão. Você também pode fornecer nomes de bancos de dados personalizados.

  - ESTRUTURA
  - MONITOR
  - QUARTZ
- Se você estiver usando uma instância nomeada, defina o serviço do Microsoft SQL Server Browser para que seja iniciado automaticamente. Caso contrário, defina uma porta estática nos soquetes TCP/IP.

- Crie uma conta de usuário com direitos de dbowner para os três os bancos de dados que o MVE usa para se conectar e definir o banco de dados. Se o usuário for uma conta do Microsoft SQL Server, habilite o Microsoft SQL Server e os modos de autenticação do Windows no Microsoft SQL Server.

  Nota: A desinstalação do MVE configurado para o uso do Microsoft SQL Server não remove as tabelas ou bancos de dados criados. Depois da desinstalação, os bancos de dados FRAMEWORK, MONITOR e QUARTZ devem ser descartados manualmente.
- Atribua os direitos dbo ao usuário do banco de dados e, em seguida, defina o esquema dbo como esquema padrão.

Configuração de usuários "executar como"

Durante a instalação, você pode especificar o MVE para ser executado como uma conta do sistema local ou como uma conta de usuário do domínio. A execução do MVE como uma conta de usuário do domínio "executar como" fornece uma instalação mais segura. A conta de usuário do domínio tem privilégios limitados em comparação a uma conta do sistema local.

	Conta de usuário de domínio "executar como"	Sistema local "executar como"
Permissões de sistema local	• Acesso a todos os arquivos para o seguinte: – *$MVE_INSTALL*/tomcat/logs – *$MVE_INSTALL*/tomcat/temp – *$MVE_INSTALL*/tomcat/work – *$MVE_INSTALL*/apps/library – *$MVE_INSTALL*/apps/dm-mve/picture – *$MVE_INSTALL*/../mve_truststore* – *$MVE_INSTALL*/jre/lib/security/cacerts – *$MVE_INSTALL*/apps/dm-mve/WEB-INF/ldap – *$MVE_INSTALL*/apps/dm-mve/download Em que *$MVE_INSTALL* é o diretório de instalação. • Privilégio do Windows: LOGON_AS_A_SERVICE	Permissões de administrador
Autenticação de conexão com o banco	• Autenticação do Windows com o Microsoft SQL Server • Autenticação SQL	Autenticação SQL
Configuração	Um usuário de domínio deve ser configurado antes da instalação.	Configurado automaticamente durante a instalação

Se você configurar o MVE como uma conta de usuário do domínio "executar como", crie o usuário no mesmo domínio que o servidor MVE.

Instalação do MVE

1. Faça o download do arquivo executável em um caminho que não contenha espaços.
2. Execute o arquivo como um administrador e siga as instruções exibidas na tela do computador.

Notas:

- As senhas são criptografadas e armazenadas de forma segura. Certifique-se de lembrar-se das senhas, ou armazene-as em um local seguro, pois senhas não podem ser decodificadas depois de armazenadas.
- Se você estiver conectado ao Microsoft SQL Server usando a Autenticação do Windows, não ocorrerão verificações de conexão durante a instalação. Certifique-se de que o usuário designado para executar o serviço MVE do Windows tenha uma conta correspondente na instância do Microsoft SQL Server. O usuário designado deve possuir direitos de dbowner para os bancos de dados ESTRUTURA, QUARTZO e MONITOR.

Instalação silenciosa do MVE

Configurações do banco de dados para instalação silenciosa

Configuração	Descrição	Valor
--help	Mostra a lista de opções válidas.	
--version	Mostra as informações do produto.	
--unattendedmodeui <unattended-modeui>	A interface de usuário para o modo autônomo.	Padrão: **nenhum** Permitido: • **nenhum** • **mínimo** • **minimalWithDialogs**
--optionfile <optionfile>	O arquivo de opção de instalação.	Padrão:
--debuglevel <debuglevel>	O nível de detalhamento das informações de depuração.	Padrão: **2** Permitido: • **0** • **1** • **2** • **3** • **4**
--mode <mode>	O modo de instalação.	Padrão: **win32** Permitido: • **win32** • **unattended**
--debugtrace <debugtrace>	O nome do arquivo de depuração.	Padrão:

Configuração	Descrição	Valor
--installer-language <installer-language>	A seleção de idioma.	Padrão: **pt_BR** Permitido: • **en** • **es** • **de** • **fr** • **it** • **pt_BR** • **zh_CN**
--encryptionKey <encryptionKey>	A chave de criptografia.	Chave de criptografia: Padrão:
--prefix <prefix>	O diretório de instalação.	Padrão: **C:\Arquivos de Programas**
--mveLexmark_runas <mveLexmark_runas>	As opções de usuário executar como.	Padrão: **LOCAL_SYSTEM** Permitido: • **LOCAL_SYSTEM** • **SPECIFIC_USER**
--serviceRunAsUsername <serviceRunAsUsername>	O nome de usuário executar como.	Nome de usuário: Padrão:
--serviceRunAsPassword <serviceRunAsPassword>	A senha de usuário executar como.	Senha: Padrão:
--mveLexmark_database <mveLexmark_database>	O tipo de banco de dados.	Padrão: Permitido: • **FIREBIRD** • **SQL_SERVER**
--firebirdUsername <firebirdUsername>	O nome de usuário do banco de dados Firebird.	Nome de usuário: Padrão:
--firebirdPassword <firebirdPassword>	A senha do banco de dados Firebird.	Senha: Padrão:
--firebirdFWDbName <firebirdFWDbName>	O nome do banco de dados Firebird para FRAMEWORK.	Nomes dos bancos de dados: Padrão: **ESTRUTURA**
--firebirdMNDbName <firebirdMNDbName>	O nome do banco de dados Firebird para MONITOR.	Padrão: **MONITOR**
--firebirdQZDbName <firebirdQZDbName>	O nome do banco de dados Firebird para QUARTZ.	Padrão: **QUARTZ**
--databaseIPAddress <databaseIPAddress>	O endereço IP ou o nome de host do banco de dados.	Endereço IP ou nome do host: Padrão:
--databasePort <databasePort>	O número da porta do banco de dados.	Número da porta: Padrão:
--instanceName <instanceName>	O nome da instância.	Nome da instância: Padrão:

Configuração	Descrição	Valor
--instanceIdentifier <instanceIdentifier>	A instância.	Padrão: **databasePort** Permitido: • **databasePort** • **instanceName**
--databaseUsername <databaseUsername>	O nome de usuário do banco de dados.	Nome de usuário: Padrão:
--databasePassword <databasePassword>	A senha do banco de dados.	Senha: Padrão:
--sqlServerAuthenticationMethod <sqlServerAuthenticationMethod>	O método de autenticação do Microsoft SQL Server.	Padrão: **sqlServerDbAuthentication** Permitido: • **sqlServerDbAuthentication** • **sqlServerWindowsAuthentication**
--fWDbName <fWDbName>	O nome do banco de dados para FRAMEWORK.	Nomes dos bancos de dados: Padrão: **ESTRUTURA**
--mNDbName <mNDbName>	O nome do banco de dados para MONITOR.	Padrão: **MONITOR**
--qZDbName <qZDbName>	O nome do banco de dados para QUARTZ.	Padrão: **QUARTZ**
--mveAdminUsername <mveAdminUsername>	O nome de usuário do administrador.	Nome de usuário: Padrão: **admin**
--mveAdminPassword <mveAdminPassword>	A senha de administrador.	Senha: Padrão:

Acessando o MVE

Para acessar o MVE, use as credenciais de login que você criou durante a instalação. Você também pode configurar outros métodos de login, como LDAP, Kerberos ou outras contas locais. Para obter mais informações, consulte " Configuração do acesso do usuário" na página 29.

1. Abra um navegador da Web e digite **https://*MVE_SERVER*/mve/**, em que ***MVE_SERVER*** é o nome do host ou o endereço IP do servidor que hospeda o MVE.
2. Se necessário, aceite o aviso de isenção de responsabilidade.
3. Insira suas credenciais.
4. Clique em **Log in**.

Notas:

- Depois de conectar-se, certifique-se de mudar a senha padrão do administrador que foi usada durante a instalação. Para obter mais informações, consulte " Alterando a sua senha" na página 24.
- Se o MVE permanecer ocioso por mais de 30 minutos, o usuário será desconectado automaticamente.

Alterando o idioma

1. Abra um navegador da Web e digite **`https://MVE_SERVER/mve/`**, em que ***`MVE_SERVER`*** é o nome do host ou o endereço IP do servidor que hospeda o MVE.
2. Se necessário, aceite o aviso de isenção de responsabilidade.
3. No canto superior direito da página, selecione um idioma.

Alterando a sua senha

1. Abra um navegador da Web e digite **`https://MVE_SERVER/mve/`**, em que ***`MVE_SERVER`*** é o nome do host ou o endereço IP do servidor que hospeda o MVE.
2. Se necessário, aceite o aviso de isenção de responsabilidade.
3. Insira suas credenciais.
4. Clique em **Log in**.
5. No canto superior direito da página, clique no seu nome de usuário e clique em **Alterar a senha**.
6. Altere a senha.

Manutenção do aplicativo

Atualização para o MVE 4.2

Antes de começar o upgrade, faça o seguinte:

- Faça backup dos arquivos do banco de dados, dos arquivos do aplicativo e propriedades. Para obter mais informações, consulte " Backup e restauração do banco de dados" na página 26.
- Se necessário, forneça nomes de banco de dados personalizados.

Se estiver atualizando da versão 1.x, atualize primeiro para a versão 2.0 e, em seguida, respectivamente para a 3.3 e, finalmente, para a 4.0 antes de atualizar para a 4.2. O processo de migração de políticas é realizado apenas durante a atualização para o MVE 2.0.

Caminho de upgrade válido	**3.3** para **4.0** para **4.2**
Caminho de upgrade inválido	**1.6.x** para **4.2** **2.0** para **4.2**

1. Faça backup dos arquivos do banco de dados e dos arquivos do aplicativo. Qualquer upgrade ou desinstalação cria um risco de perda de dados irrecuperável. Você pode usar os arquivos de backup para restaurar o aplicativo ao seu estado anterior, caso o upgrade falhe.

   Aviso — Danos potenciais: Quando você faz upgrade do MVE, o banco de dados é alterado. Não restaure um backup de banco de dados criado a partir de uma versão anterior.

   Nota: Para obter mais informações, consulte " Backup e restauração do banco de dados" na página 26.

2. Faça download do arquivo executável em um local temporário.

3. Execute o instalador como administrador e siga as instruções exibidas na tela do computador.

   Notas:

   - Quando o upgrade para o MVE 2.0 é realizada, as políticas que são atribuídas às impressoras migram para uma configuração única em cada modelo de impressora. Por exemplo, se as políticas de envio de fax, cópia, papel e impressão forem atribuídas a uma impressora X792, essas políticas serão consolidadas em uma configuração da X792. Esse processo não se aplica às políticas que não são atribuídas às impressoras. O MVE gera um arquivo de registro confirmando que as políticas foram migradas para uma configuração com êxito. Para obter mais informações, consulte " Onde posso encontrar os arquivos de registro?" na página 151.
   - Após a atualização, certifique-se de limpar o cache do navegador antes de acessar o aplicativo novamente.
   - Ao fazer o upgrade do MVE para a versão 3.5 ou posterior, os componentes de segurança avançada são removidos das configurações em que estão. Se um ou mais componentes de segurança avançada forem os mesmos, eles serão combinados em um único componente. O componente de segurança avançada criado é adicionado automaticamente à biblioteca de componentes de segurança avançada.

Backup e restauração do banco de dados

Nota: Há possível perda de dados ao executar procedimentos de backup e restauração. Certifique-se de executar as etapas corretamente.

Backup dos arquivos do banco de dados e dos arquivos do aplicativo

Recomendamos que o backup de seus bancos de dados seja feito regularmente.

1. Encerre o serviço do Firebird e o serviço do Markvision Enterprise.
   a. Abra a caixa de diálogo Executar e digite **`services.msc`**.
   b. Clique com o botão direito em **Firebird Guardian - DefaultInstance** e, em seguida, clique em **Parar**.
   c. Clique com o botão direito em **Markvision Enterprise**e, em seguida, clique em **Parar**.
2. Navegue até a pasta em que Markvision Enterprise está instalado.

   Por exemplo, **`C:\Arquivos de Programas\`**
3. Faça backup dos arquivos do aplicativo e dos arquivos do banco de dados.

Backup dos arquivos do aplicativo

Copie os arquivos a seguir em um repositório seguro:

- 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

Nota: Verifique se esses arquivos estão armazenados corretamente. Sem as chaves de criptografia no arquivo mve_encryption.jceks, os dados armazenados em um formato criptografado no banco de dados e no sistema de arquivos não podem ser recuperados.

Backup dos arquivos do banco de dados

Execute uma das seguintes opções:

Nota: Os arquivos a seguir estão usando os nomes de banco de dados padrão. Essas instruções também se aplicam a nomes de bancos de dados personalizados.

- Se você estiver usando um banco de dados Firebird, copie os seguintes arquivos para um repositório seguro. É necessário fazer backup desses arquivos frequentemente para evitar a perda de dados.
  - Lexmark\Markvision Enterprise\firebird\security2.fdb

    Se você estiver usando nomes de banco de dados personalizados, atualize o seguinte:
    - 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
- Se você estiver usando o Microsoft SQL Server, crie um backup para FRAMEWORK, MONITOR e QUARTZ.

  Para obter mais informações, entre em contato com o administrador do Microsoft SQL Server.

4. Reinicie o serviço do Firebird e o serviço do Markvision Enterprise.
   a. Abra a caixa de diálogo Executar e digite **`services.msc`**.
   b. Clique com o botão direito em **Firebird Guardian - DefaultInstance** e, em seguida, clique em **Reiniciar**.
   c. Clique com o botão direito em **Markvision Enterprise** e, em seguida, clique em **Reiniciar**.

Restauração dos arquivos do banco de dados e os arquivos do aplicativo

Aviso — Danos potenciais: Quando você atualizar o MVE, o banco de dados pode ser alterado. Não restaure um backup de banco de dados criado a partir de uma versão anterior.

1. Encerre o serviço do Markvision Enterprise.

   Para obter mais informações, consulte etapa 1 de " Backup dos arquivos do banco de dados e dos arquivos do aplicativo" na página 26.

2. Navegue até a pasta em que Markvision Enterprise está instalado.

   Por exemplo, **`C:\Arquivos de Programas\`**

3. Restaure os arquivos do aplicativo.

   Substitua os arquivos a seguir pelos arquivos que você salvou durante o processo de backup:
   - 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

   Nota: É possível restaurar um backup de banco de dados em uma nova instalação do MVE somente se a nova instalação do MVE for da mesma versão.

4. Restaure os arquivos do banco de dados.

   Execute uma das seguintes opções:
   - Se estiver usando um banco de dados Firebird, substitua os seguintes arquivos salvos durante o processo de backup:

Nota: Os arquivos a seguir estão usando os nomes de banco de dados padrão. As instruções também se aplicam a nomes de bancos de dados personalizados.

- Lexmark\Markvision Enterprise\firebird\security2.fdb

  Se estiver usando nomes de banco de dados personalizados, os seguintes arquivos também serão restaurados:

  - 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

- Se estiver usando o Microsoft SQL Server, entre em contato com o administrador do Microsoft SQL Server.

5. Reinicie o serviço do Markvision Enterprise.

   Para obter mais informações, consulte etapa 4 de " Backup dos arquivos do banco de dados e dos arquivos do aplicativo" na página 26.

Atualizando as definições do instalador após a instalação

O Utilitário de senhas Markvision Enterprise permite que você atualize as definições do Microsoft SQL Server que foram configuradas durante a instalação sem precisar reinstalar o MVE. O utilitário também possibilita a atualização das credenciais de domínio do usuário executar como, tais como nome de usuário e senha. Você também pode usar o utilitário para criar outro usuário administrador se esquecer suas credenciais de usuário administrador anteriores.

1. Navegue até a pasta onde o Markvision Enterprise está instalado.

   Por exemplo, **`C:\Arquivos de Programas\`**

2. Inicie o arquivo **mvepwdutility-windows.exe** no diretório Lexmark\Markvision Enterprise\.

3. Selecione um idioma e clique em **OK** > **Avançar**.

4. Siga as instruções na tela do computador.

Configuração do acesso do usuário

Visão geral

O MVE permite que você adicione usuários internos diretamente ao servidor MVE ou use as contas de usuário registradas em um servidor LDAP. Para obter mais informações sobre como adicionar usuários internos, consulte " Gerenciamento de usuários" na página 30. Para obter mais informações sobre como usar contas de usuário LDAP, consulte " Ativação da autenticação do servidor LDAP" na página 31.

Ao adicionar usuários, é preciso atribuir funções. Para mais informações, consulte " Compreendendo funções de usuário" na página 29.

Durante a autenticação, o sistema verifica as credenciais dos usuários internos presentes no servidor MVE. Se o MVE não conseguir autenticar o usuário, ele tenta autenticar o usuário no servidor LDAP. Se o nome de usuário existir no servidor MVE e no servidor LDAP, a senha no servidor MVE será usada.

Compreendendo funções de usuário

Os usuários do MVE podem ser atribuídos a uma ou mais funções. Dependendo da função, os usuários podem executar as seguintes tarefas:

- **Admin**—acessar e executar tarefas em todos os menus. Eles também têm privilégios administrativos, como adicionar usuários ao sistema ou configurar as definições do sistema. Somente os usuários com função de Admin podem interromper a tarefa de execução independentemente do tipo de usuário que a iniciou.
- **Impressoras**
  - Gerenciar perfis de localização.
  - Definir os estados da impressora.
  - Realizar uma auditoria.
  - Gerenciar categorias e palavras-chave.
  - Programar uma auditoria, exportação de dados e localização de impressora.
- **Configurações**
  - Gerenciar configurações, incluindo importação e exportação de arquivos de configuração.
  - Carregar arquivos para a biblioteca de recursos.
  - Atribuir e aplicar configurações às impressoras.
  - Programar uma verificação de conformidade e aplicação de configurações.
  - Implantar arquivos para impressoras.
  - Atualize o firmware da impressora.
  - Gerar solicitações de assinatura do certificado da impressora.
  - Fazer download das solicitações de assinatura do certificado da impressora.
- **Gerente de eventos**
  - Gerenciar ações e eventos.
  - Atribuir eventos às impressoras.
  - Testar ações.

- **Serviço de help desk**
  - Atualizar o status da impressora.
  - Reiniciar impressoras.
  - Executar uma verificação de conformidade.
  - Aplicar configurações a impressoras.

Notas:

- Todos os usuários no MVE podem visualizar a página de informações da impressora e gerenciar pesquisas salvas e exibições.
- Para obter mais informações sobre como atribuir funções de usuário, consulte " Gerenciamento de usuários" na página 30.

Gerenciamento de usuários

1. Clique em no canto superior direito da página.
2. Clique em **Usuário** e faça uma das seguintes opções:

Adicionar um usuário

a. Clique em **Criar**.
b. Digite o nome de usuário, ID de usuário e senha.
c. Selecione as funções.

   Nota: Para obter mais informações, consulte " Compreendendo funções de usuário" na página 29.

d. Clique em **Criar usuário**.

Editar um usuário

a. Selecione um ID de usuário.
b. Configure as definições.
c. Clique em **Salvar alterações**.

Excluir usuários

a. Selecione um ou mais usuários.
b. Clique em **Excluir**e confirme a exclusão.

Nota: Uma conta de usuário é bloqueada depois de três falhas consecutivas em tentativas de login. Apenas um usuário Admin poderá reativar a conta do usuário. Se o usuário Admin for bloqueado, o sistema o reativará automaticamente após cinco minutos.

Ativação da autenticação do servidor LDAP

O LDAP é um protocolo extensível multiplataforma baseado em padrões, executado diretamente sobre o TCP/IP. Ele é usado para acessar bancos de dados especializados chamados diretórios.

Para evitar a manutenção de várias credenciais de usuário, você pode usar o servidor LDAP da empresa para autenticar IDs e senhas de usuários.

Como pré-requisito, o servidor LDAP deve conter grupos de usuários que correspondem às funções de usuário necessárias. Para obter mais informações, consulte " Compreendendo funções de usuário" na página 29.

1. Clique em no canto superior direito da página.
2. Clique em **LDAP** e selecione **Ativar LDAP para autenticação**.
3. No campo Nome do host do servidor LDAP, digite o endereço IP ou o nome do host do servidor LDAP no qual a autenticação ocorre.

   Nota: Se você quiser usar comunicação criptografada entre o servidor MVE e o servidor LDAP, use o nome de domínio totalmente qualificado (FQDN).
4. Especifique o número da porta do servidor de acordo com o protocolo de criptografia selecionado.
5. Selecione o protocolo de criptografia.
   - **Nenhuma**
   - **TLS** — Um protocolo de segurança que utiliza criptografia de dados e autenticação de certificado para proteger a comunicação entre o servidor e o cliente. Se essa opção for selecionada, um comando START_TLS será enviado para o servidor LDAP depois que a conexão tiver sido estabelecida. Use essa configuração se desejar uma comunicação segura pela porta 389.
   - **SSL/TLS** — Um protocolo de segurança que usa criptografia de chave pública para autenticar a comunicação entre um servidor e um cliente. Use essa opção se quiser uma comunicação segura desde o início do vínculo LDAP. Essa opção é normalmente usada para a porta 636 ou outras portas LDAP protegidas.
6. Selecione o tipo de vínculo.
   - **Simples** — O servidor MVE produz as credenciais específicas do servidor LDAP para usar o recurso de pesquisa do servidor LDAP.
     a. Digite seu nome de usuário de vínculo.
     b. Digite a senha de vínculo e confirme-a.
   - **Kerberos** — Para definir as configurações, faça o seguinte:
     a. Digite seu nome de usuário de vínculo.
     b. Digite a senha de vínculo e confirme-a.
     c. Clique em **Escolher arquivo** e navegue até o arquivo krb5.conf.
   - **SPNEGO** — Para definir as configurações, faça o seguinte:
     a. Digite o nome principal do serviço.
     b. Clique em **Escolher arquivo** e navegue até o arquivo krb5.conf.
     c. Clique em **Escolher arquivo** e navegue até o arquivo keytab do Kerberos.

     Essa opção é usada apenas para configurar o Mecanismo de negociação GSSAPI simples e protegido (SPNEGO) para suportar a funcionalidade de Logon único.

7 Na seção Opções avançadas, configure da seguinte forma:

- **Base de pesquisa** — O DN (nome diferenciado) base do nó raiz. Na hierarquia do servidor da comunidade LDAP, esse nó deve ser ancestral do nó do usuário e do nó do grupo. Por exemplo, **dc=mvetest,dc=com**.

  Nota: Ao especificar o DN raiz, certifique-se de que somente **dc** e **o** façam parte do DN raiz. Se **ou** ou **cn** for o ancestral dos nós de usuários e grupos, use **ou** ou **cn** nas bases de pesquisa de usuário e grupo.
- **Base de pesquisa do usuário** — O nó no servidor da comunidade LDAP onde está o objeto de usuário. Este nó está no DN raiz em que todos os nós de usuários estão listados. Por exemplo, **ou=people**.
- **Filtro de pesquisa do usuário** — O parâmetro para localizar um objeto de usuário no servidor da comunidade LDAP. Por exemplo, **(uid={0})**.

  ### Exemplos de condições múltiplas permitidas e expressões complexas

Faça login usando	No campo Filtro de pesquisa do usuário, digite
Nome comum	**(CN={0})**
Nome de login	**(sAMAccountName={0})**
Nome principal do usuário	**(userPrincipalName={0})**
Número de telefone	**(telephoneNumber={0})**
Nome de login ou nome comum	**(|(sAMAccountName={0})(CN={0}))**

  Nota: O único padrão válido é **{0}**, o que significa que o MVE procura o nome de login do usuário MVE.
- **Pesquisar objeto da base do usuário e toda a subárvore** — O sistema pesquisa todos os nós na base de pesquisa do usuário.
- **Base de pesquisa do grupo** — O nó no servidor da comunidade LDAP que contém os grupos de usuários correspondentes às funções do MVE. Esse nó está no DN raiz em que todos os nós de grupos estão listados. Por exemplo, **ou=group**.
- **Filtro de pesquisa do grupo** — O parâmetro para localizar um usuário em um grupo que corresponde a uma função no MVE.

  Nota: Somente os padrões **{0}** e **{1}** podem ser usados. Se **{0}** for usado, o MVE procura o DN do usuário LDAP. Se **{1}** for usado, o MVE procura o nome de login do usuário MVE.
- **Atributo de função do grupo** — Digite o atributo LDAP para obter o nome completo do grupo. Um atributo LDAP tem um significado específico e define um mapeamento entre o atributo e um nome de campo. Por exemplo, o atributo LDAP **cn** está associado ao campo Nome completo. O atributo LDAP **commonname** também é mapeado para o campo Nome completo. Geralmente, esse atributo deve ser deixado no valor padrão de **cn**.
- **Pesquisar objeto da base do usuário e toda a subárvore** — O sistema pesquisa todos os nós na base de pesquisa do grupo.

8 Na seção Grupos de LDAP para mapeamento de funções do MVE, insira os nomes dos grupos LDAP que correspondem às funções do MVE.

Notas:

- Para obter mais informações, consulte " Compreendendo funções de usuário" na página 29.
- Você pode atribuir um grupo LDAP a várias funções MVE. Você também pode digitar mais de um grupo LDAP em um campo de função usando o caractere de barra vertical (|) para separar diversos

grupos. Por exemplo, para incluir os grupos **admin** e **assets** na função Administrador, digite **admin|assets** no campo de função Grupos de LDAP para administrador.

- Se desejar usar apenas a função Administrador e não as outras funções MVE, deixe os campos em branco.

9 Clique em **Salvar alterações**.

Instalando certificados de servidor LDAP

Para estabelecer uma comunicação criptografada entre o servidor MVE e o servidor LDAP, é necessário que o MVE confie no certificado do servidor LDAP. Na arquitetura MVE, quando o MVE está autenticando com um servidor LDAP, o MVE é o cliente e o servidor LDAP é o par.

1 Clique em no canto superior direito da página.

2 Clique em **LDAP** e defina as configurações LDAP. Para obter mais informações, consulte " Ativação da autenticação do servidor LDAP" na página 31.

3 Clique em **Testar LDAP**.

4 Insira um nome de usuário e senha LDAP válidos quando solicitado e, em seguida, clique em **Iniciar teste**.

5 Examine o certificado quanto à validade e depois aceite-o.

Descoberta de impressoras

Criação de perfis de descoberta

Utilize um perfil de descoberta para encontrar impressoras na rede e adicioná-las ao sistema. Em um perfil de descoberta, siga um dos seguintes procedimentos para incluir ou excluir uma lista de endereços IP ou nomes do host:

- Adição de entradas uma a uma
- Importação de entradas usando um arquivo TXT ou CSV

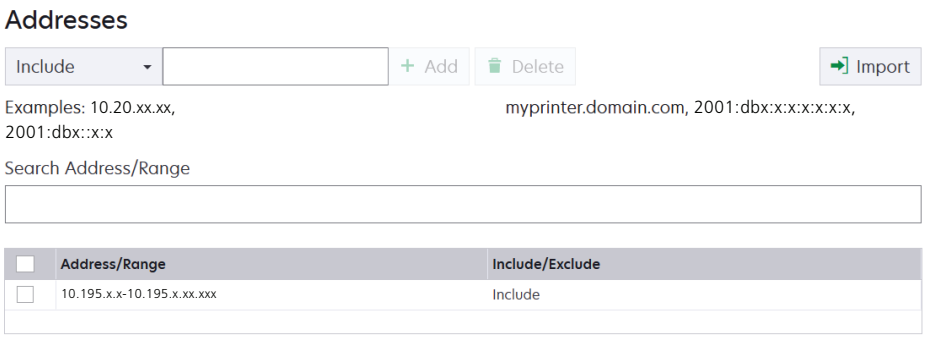
Também é possível atribuir e aplicar uma configuração automaticamente a um modelo de impressora compatível. Uma configuração deve conter definições, aplicativos, licenças, firmware e certificados CA da impressora que podem ser implantados nas impressoras.

1. No menu Impressoras, clique em **Perfis de descoberta** > **Criar**.
2. Na seção Geral, digite um nome exclusivo e uma descrição para o perfil de descoberta e configure as seguintes opções:
   - **Tempo limite** — O tempo que o sistema aguarda até a impressora responder.
   - **Tentativas** — O número de vezes que o sistema tenta se comunicar com a impressora.
   - **Gerenciar automaticamente as impressoras localizadas** — Impressoras descobertas recentemente são definidas automaticamente para o estado Gerenciado, e o estado Novo é ignorado durante a descoberta.
3. Na seção Endereços, execute um destes procedimentos:

Adicione os endereços

a. Selecione **Incluir** ou **Excluir**.

b. Digite o endereço IP, o nome do host, a sub-rede ou a faixa de endereços IP.



Adicione somente uma entrada por vez. Utilize os seguintes formatos para os endereços:

- **`10.195.10.1`** (endereço IPv4 único)
- **`myprinter.example.com`** (nome único do host)
- **`10.195.10.3-10.195.10.255`** (faixa de endereços IPv4)
- **`10.195.*.*`** (curingas)
- **`10.195.10.1/22`** (roteamento entre domínios sem classe IPv4 ou notação CIDR)

- **2001:db8:0:0:0:0:2:1** (endereço IPv6 completo)
- **2001:db8::2:1** (endereço IPv6 reduzido)

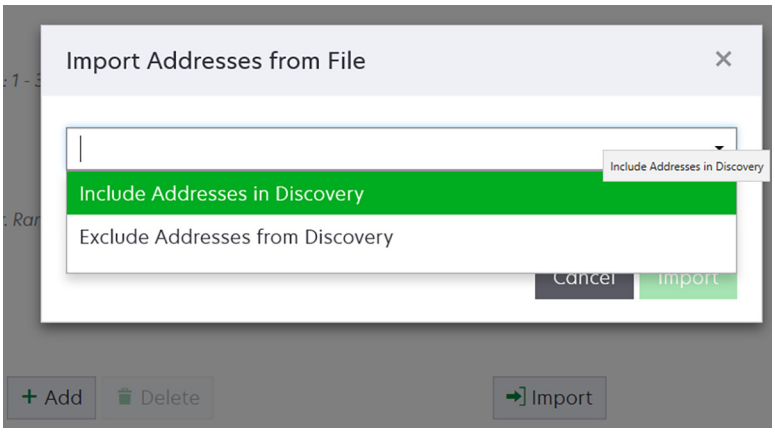
Nota: Caso perfis de descoberta separados sejam criados para os endereços IPv6 e IPv4 da mesma impressora, o último endereço descoberto será exibido. Por exemplo, se a impressora for descoberta usando IPv6 e for descoberta novamente usando IPv4, somente o endereço IPv4 será exibido na lista de impressoras.

c Clique em **Adicionar**.

Importar os endereços

a Clique em **Importar**.

b Selecione se deseja incluir ou excluir endereços IP durante a descoberta.



c Navegue até o arquivo de texto que contém uma lista de endereços. Cada entrada de endereço deve ser colocada em uma linha separada.

Arquivo de texto de amostra

```
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 Clique em **Importar**.

4 Na seção SNMP, selecione **Versão 1**, **Versão 2c** ou **Versão 3** e defina as permissões de acesso.

Nota: Para descobrir impressoras usando a versão 3 do SNMP, crie um nome de usuário e uma senha no Embedded Web Server da impressora e, em seguida, reinicie a impressora. Se não for possível estabelecer uma conexão, redescubra as impressoras. ‘Para obter mais informações, consulte o *Guia do Administrador do Embedded Web Server*.

5 Se necessário, na seção Inserir credenciais, selecione o método de autenticação que as impressoras estão usando e, em seguida, insira as credenciais.

Nota: Esse recurso permite estabelecer a comunicação com impressoras protegidas durante a descoberta. As credenciais corretas devem ser fornecidas para executar tarefas nas impressoras protegidas, como auditoria, atualização de status e atualização de firmware.

6 Se necessário, na seção Atribuir configurações, associe uma configuração a um modelo de impressora. Para obter mais informações sobre a criação de uma configuração, consulte " Criação de configurações" na página 68.

7 Se necessário, na seção Atribuir configurações, associe uma senha a um modelo de impressora durante a descoberta. Para obter informações sobre a atribuição de palavras-chave a impressoras, consulte " Atribuindo palavras-chave a impressoras" na página 65

Notas:

- Todas as impressoras descobertas por meio desse perfil são atribuídas com as novas palavras-chave.
- As novas palavras-chave são adicionadas à lista existente de palavras-chave que já estão atribuídas a uma impressora.

8 Clique em **Salvar perfil** ou **Salvar e executar perfil**.

Nota: É possível programar uma descoberta para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Gerenciando perfis de localização

1 No menu Impressoras, clique em **Perfis de localização**.

2 Tente um dos seguintes métodos:

Edite um perfil

a Selecione um perfil e clique em **Editar**.

b Configure as definições.

c Clique em **Salvar perfil** ou **Salvar e Executar perfil**.

Copiar um perfil

a Selecione um perfil e clique em **Copiar**.

b Configure as definições.

c Adicionar endereços IP. Para obter mais informações, consulte " Adicione os endereços" na página 34.

d Clique em **Salvar perfil** ou **Salvar e Executar perfil**.

Excluir um perfil

a Selecione um ou mais perfis.

b Clique em **Excluir**e confirme a exclusão.

Executar um perfil

a Selecione um ou mais perfis.

b Clique em **Executar**. Verifique o status de localização no menu Tarefas.

Amostra de cenários: Descoberta de impressoras

A companhia ABC é uma grande empresa de fabricação que ocupa um edifício de nove andares. A empresa acabou de comprar 30 novas impressoras Lexmark, distribuídas entre os nove andares. Como a equipe de TI, você precisa adicionar essas novas impressoras ao MVE. As impressoras já estão conectadas à rede, mas você não sabe todos os endereços IP.

Você deseja proteger as seguintes novas impressoras no departamento de contabilidade.

10.194.55.60
10.194.56.77
10.194.55.71
10.194.63.27
10.194.63.10

Exemplo de implementação

1. Crie um perfil de descoberta para as impressoras no departamento de contabilidade.
2. Adicione cinco endereços IP.
3. Crie uma configuração que proteja as impressoras especificadas.
4. Inclua as configurações no perfil de descoberta.
5. Salve e execute o perfil.
6. Crie outro perfil de descoberta para o restante das impressoras.
7. Inclua os endereços IP usando um curinga. Use o seguinte: **10.194.*.***
8. Exclua os cinco endereços IP da impressora no departamento de contabilidade.
9. Salve e execute o perfil.

Gerenciamento do painel de segurança

Visão geral

O painel Segurança permite exibir a integridade das configurações de segurança do dispositivo. É uma representação visual de várias configurações de segurança, como portas, protocolos, status de criptografia de disco, contas de administrador do dispositivo e status de certificado padrão. Ele fornece visibilidade da postura de segurança de sua frota, o que ajuda os administradores a identificar e corrigir as configurações que estão fora de conformidade.

Acessar o painel de segurança

1. No portal da Web MVE, clique em **Painel**.

   Nota: O painel de segurança é a página inicial padrão para usuários Admin.

2. Clique em um dos seguintes widgets:
   - **Informações de segurança do dispositivo**
   - **Verificação de conformidade do dispositivo**

Gerenciamento de Informações de segurança do dispositivo

Este widget resume a exibição de segurança da frota.

1. Clique em qualquer barra do gráfico para ir para a janela Informações de segurança do dispositivo.
2. Passe o mouse sobre as barras para exibir os seguintes detalhes:
   - Número da porta
   - Número de impressoras associadas
   - Se as configurações da impressora estão abertas/ativadas
3. Clique em **Imprimir** para obter um formato imprimível da visualização detalhada.

Notas:

- A janela informações de segurança do dispositivo fornece ao usuário um recurso de detalhamento.
- Clicar em qualquer item da barra no gráfico permite que o usuário navegue até uma exibição filtrada da página de listagem de impressoras. Para obter mais informações, consulte " Visualização da lista de impressoras" na página 40.

Gerenciamento da Verificação de conformidade do dispositivo

Este widget resume a visualização detalhada da verificação de conformidade da frota.

1. Clique em qualquer seção do gráfico de pizza para ir para a janela Verificação de conformidade do dispositivo.
2. No painel esquerdo, aplique o filtro Intervalo de datas.

   Nota: O intervalo padrão é de 7 dias.
3. Clique em **Imprimir** para obter um formato imprimível da visualização detalhada.

Notas:

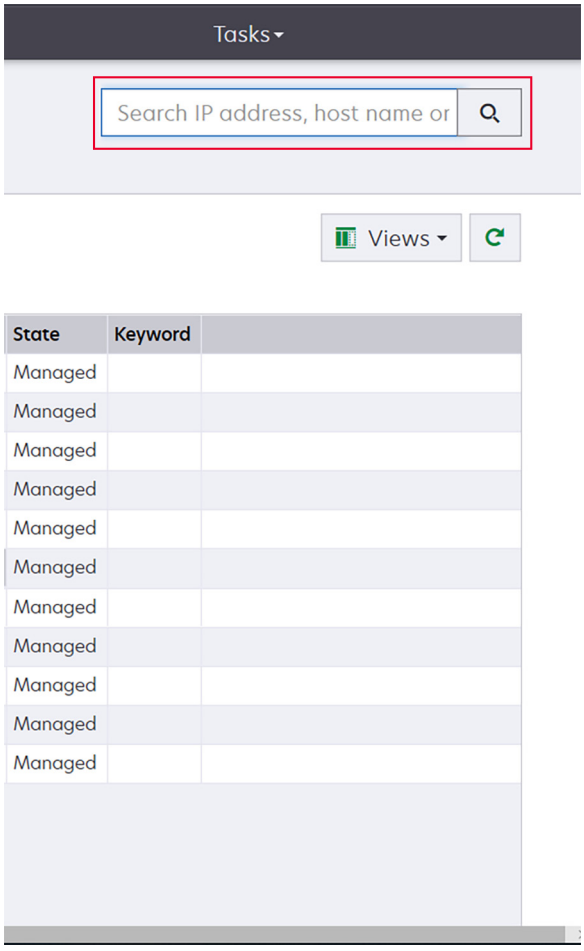
- A janela Verificação de conformidade do dispositivo fornece ao usuário um recurso de detalhamento.
- Clicar em qualquer seção do gráfico de pizza permite que o usuário navegue até uma exibição filtrada da página de listagem de impressoras. Para obter mais informações, consulte " Visualização da lista de impressoras" na página 40.

Exibição de impressoras

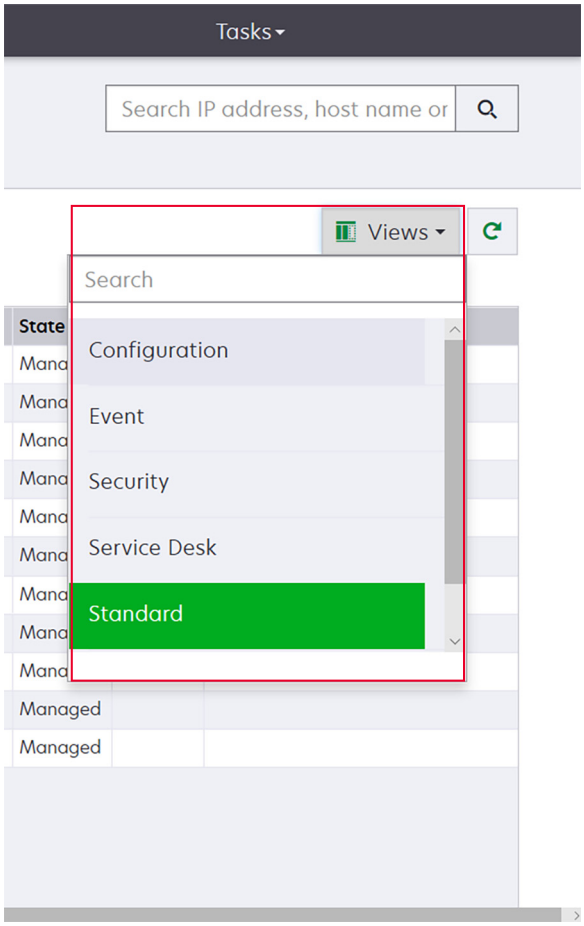
Visualização da lista de impressoras

A página Listagem de impressoras é a página inicial padrão quando você acessa o MVE. A tabela mostra a lista das impressoras adicionadas no MVE.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Na página de Listagem de impressoras, execute um dos seguintes procedimentos:
   - Para procurar impressoras específicas, siga um destes procedimentos:
     - Use a caixa de pesquisa para procurar um endereço IP, nome de host, nome de sistema ou número de série.

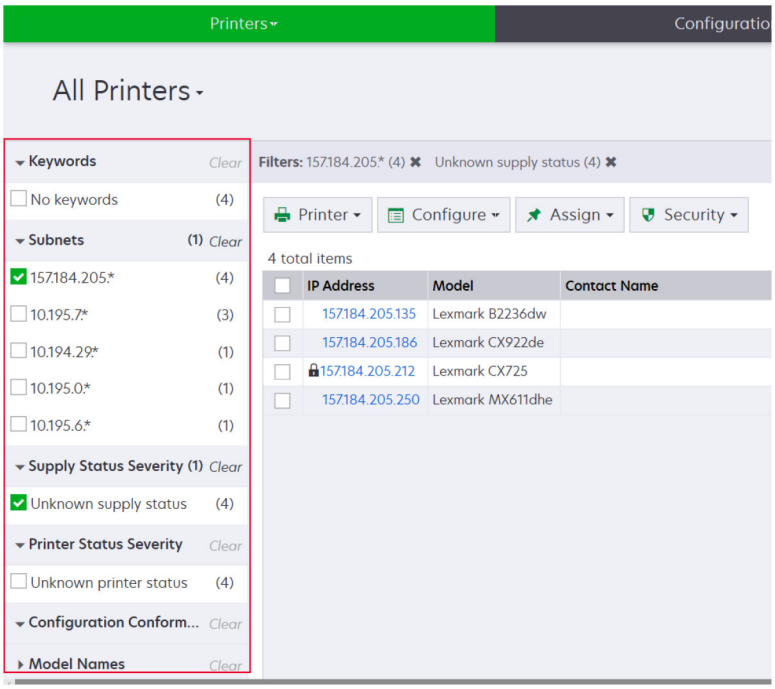


– Altere a exibição de listagem de impressoras. Para obter mais informações, consulte " Alterando a exibição de lista de impressoras" na página 46.

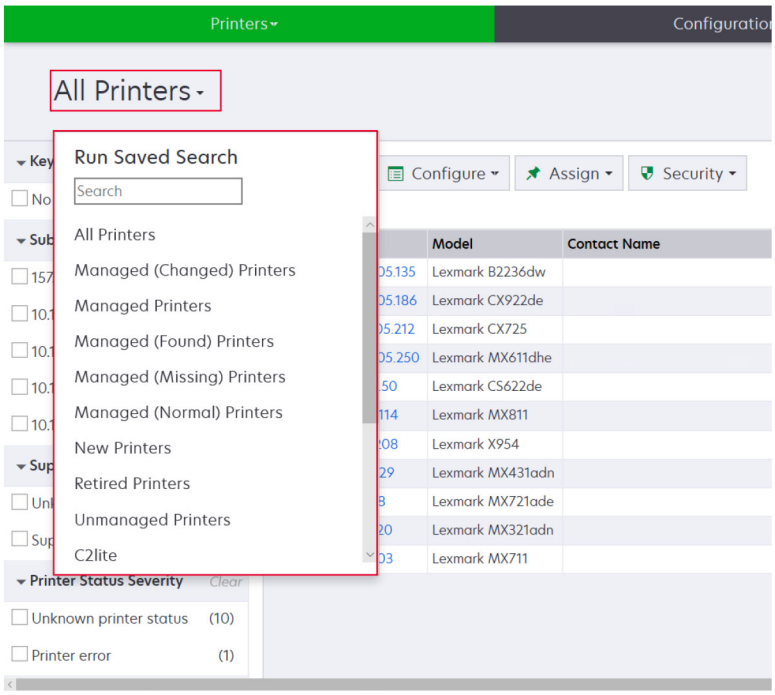


Nota: Se você estiver usando a caixa de pesquisa, o aplicativo procura todas as impressoras no sistema. Os filtros selecionados e as pesquisas salvas serão ignorados. Se você executar uma pesquisa salva, os critérios especificados na pesquisa salva serão usados. Os filtros selecionados e o endereço IP ou o nome do host digitados na caixa de pesquisa serão ignorados. Também é possível usar os filtros para restringir os resultados da pesquisa atual.

– Use os filtros.



– Execute uma pesquisa salva. Para obter mais informações, consulte " Como executar uma pesquisa salva" na página 49.



- Para classificar as impressoras, na tabela da lista de impressoras, clique em qualquer cabeçalho de coluna. As impressoras são classificadas de acordo com o cabeçalho da coluna selecionada.
- Para exibir mais informações sobre as impressoras, redimensione as colunas. Coloque o cursor sobre a borda vertical do cabeçalho da coluna e arraste a borda para a esquerda ou para a direita.

Visualizando as informações da impressora

Para ver a lista completa de informações, certifique-se de que uma auditoria seja executada na impressora. Para mais informações, consulte " Auditando impressoras" na página 61.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Clique no endereço IP da impressora.
3. Visualize as seguintes informações:
   - **Status** — O status da impressora.
   - **Suprimentos** — Os detalhes do suprimento e a porcentagem do suprimento restante.
   - **Identificação** — As informações de identificação da rede da impressora.

     Nota: As informações sobre o fuso horário estão disponíveis apenas em alguns modelos de impressora.
   - **Datas** — A data em que a impressora foi adicionada ao sistema, a data de descoberta e a data de auditoria mais recente.
   - **Firmware** — As propriedades do firmware da impressora e os níveis de código.
   - **Recursos** — Os recursos da impressora.
   - **Opções de memória** — O tamanho do disco rígido e o espaço livre de memória flash do usuário.
   - **Opções de entrada** — As definições das bandejas disponíveis.
   - **Opções de saída** — As definições das bandejas de saída disponíveis.
   - **Aplicativos eSF** — As informações sobre os aplicativos Framework de Soluções Embarcadas (eSF, Embedded Solutions Framework) instalados na impressora.
   - **Estatísticas da impressora** — Valores específicos para cada uma das propriedades da impressora.
   - **Detalhes de alterações** — As informações sobre as alterações na impressora.

     Nota: Essas informações estão disponíveis somente em impressoras no estado Gerenciada (Alterada). Para mais informações, consulte " Compreendendo os estados do ciclo de vida útil da impressora" na página 47.
   - **Credenciais da impressora** — As credenciais usadas na configuração atribuída à impressora.
   - **Certificado da impressora** — As propriedades dos seguintes certificados da impressora:
     - **Padrão**
     - **HTTPS**
     - **802.1x**
     - **IPSec**

     Notas:

     - Essa informação está disponível apenas em alguns modelos de impressora.
     - Um status de validade Expiração próxima indica a data de expiração, conforme definido na seção Autoridade de certificações em Configuração do sistema.
   - **Propriedades da configuração** — As propriedades da configuração atribuída à impressora.
   - **Alertas ativos** — Os alertas da impressora que aguardam resolução.
   - **Eventos atribuídos** — Os eventos atribuídos à impressora.

Exportando dados da impressora

O MVE permite exportar as informações da impressora que estão disponíveis na sua exibição atual.

1. Na pasta Impressoras menu, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Impressora** > **Exportar dados**.

   Notas:

   - Os dados exportados são salvos em um arquivo CSV.
   - A exportação dos dados pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Gerenciamento de exibições

O recurso Exibições possibilita a personalização das informações mostradas na página de listagem de impressoras.

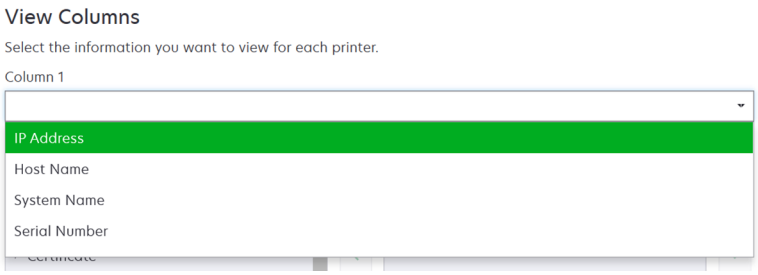
1. No menu Impressoras, clique em **Exibições**.
2. Execute um dos seguintes procedimentos:

Crie uma visualização

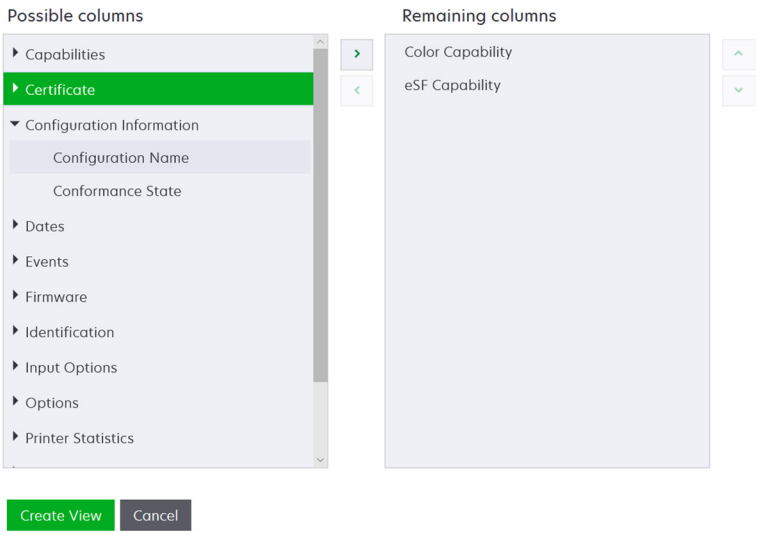
a. Clique em **Criar**.

b. Digite um nome exclusivo para a visualização e sua descrição.

c. Na seção Exibir colunas no menu Coluna 1, selecione a coluna do identificador.



d Na seção Colunas possíveis, expanda uma categoria, selecione a informação que deseja exibir como coluna e clique em **>**.



- **Recursos** — Mostra se os recursos selecionados são suportados na impressora.
- **Certificado** — Mostra a data de criação do certificado da impressora, o status da inscrição, a data de validade, a data de renovação, o número da revisão, o assunto do certificado, a validade e o status da assinatura.
- **Informações de configuração** — Mostra informações da configuração da impressora, como conformidade, nome da configuração e estado.
- **Datas** — Mostra a última auditoria, a última verificação de conformidade, a última descoberta e a data em que a impressora foi adicionada ao sistema.
- **Eventos** — Mostra informações de eventos da impressora.
- **Firmware** — Mostra informações de firmware, como a versão do firmware.
- **Identificação** — Mostra informações sobre a impressora, como o endereço IP, o nome do host e o número de série.
- **Opções de entrada** — Mostra informações sobre as opções de entrada, como o tamanho da bandeja e o tipo de mídia.
- **Opções** — Mostra informações sobre as opções da impressora, como disco rígido e unidade flash.
- **Estatísticas da impressora** — Mostra informações sobre o uso da impressora, como o número de páginas impressas ou digitalizadas e o número total de operações de fax.
- **Soluções** — Mostra os aplicativos eSF instalados na impressora e seus números de versão.
- **Status** — Mostra o status da impressora e dos suprimentos.
- **Suprimentos** — Mostra informações relacionadas a suprimentos.
- **Portas da impressora** — Mostra as informações relacionadas às portas.

  Nota: A opção **Desconhecido** no valor da porta significa que a porta não existe na impressora ou o MVE não pode recuperar a porta.
- **Opções de segurança da impressora** — Mostra as informações sobre o TLS e a cifra.

e Clique em **Criar exibição**.

Editar uma exibição

a Selecione uma exibição.

b Clique em **Editar** e edite as definições.

c Clique em **Salvar alterações**.

Copiar uma exibição

a Selecione uma exibição.

b Clique em **Copiar** e configure as definições.

c Clique em **Criar exibição**.

Excluir exibições

a Selecione uma ou mais exibições.

b Clique em **Excluir** e confirme a exclusão.

Definir uma exibição padrão

a Selecione uma exibição.

b Clique em **Definir como padrão**.

As seguintes exibições são geradas pelo sistema e não podem ser editadas ou excluídas:

- Configuração
- Lista de impressoras
- Evento
- Segurança
- Central de serviços
- Bandeja padrão

Alterando a exibição de lista de impressoras

Para obter mais informações, consulte " Gerenciamento de exibições" na página 44.

1 No menu Impressoras, clique em **Lista de impressoras**.

2 Clique em **Exibições** e, em seguida, selecione uma exibição.

filtrando impressoras usando a barra de pesquisa

Observe as seguintes instruções ao usar a barra de pesquisa para buscar impressoras.

- Para pesquisar um endereço IP, certifique-se de digitar o endereço completo ou intervalo do IP.

  Por exemplo:

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

- Se a string de pesquisa não for um endereço IP, as impressoras serão pesquisadas de acordo com o nome do host, nome do sistema ou o número de série.
- O caractere sublinhado (_) pode ser usado como curinga.

Gerenciamento de palavras-chave

As palavras-chave permitem que você crie marcas personalizadas e as atribua às impressoras.

1 No menu Impressoras, clique em **Palavras-chave**.

2 Execute uma das seguintes opções:
   - Adicionar, editar ou excluir uma categoria.

     Nota: As categorias agrupam as palavras-chave.
   - Adicionar, editar ou excluir uma palavra-chave.

Para obter informações sobre a atribuição de palavras-chave a impressoras, consulte " Atribuindo palavras-chave a impressoras" na página 65.

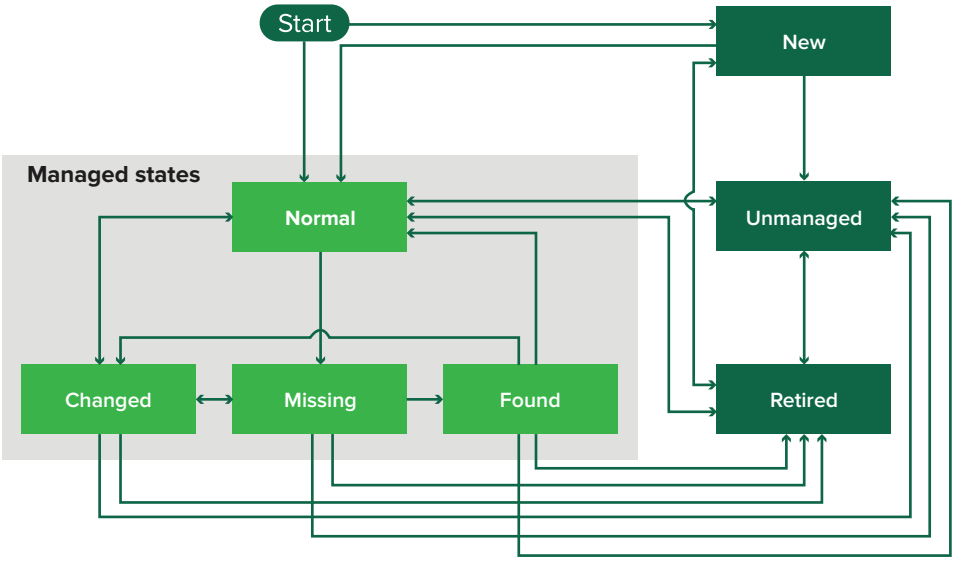
Uso das pesquisas salvas

Compreendendo os estados do ciclo de vida útil da impressora

As pesquisas salvas geradas pelo sistema exibem as impressoras nos seguintes estados do ciclo de vida útil da impressora:

- **Todas as impressoras** — Todas as impressoras no sistema.
- **Impressoras gerenciadas** — As impressoras exibidas podem estar em qualquer um dos seguintes estados:
  - Gerenciada (Normal)
  - Gerenciada (Alterada)
  - Gerenciada (Ausente)
  - Gerenciada (Encontrada)
- **Impressoras gerenciadas (alteradas)** — Impressoras no sistema cujas propriedades a seguir foram alteradas na última auditoria:
  - Marca de propriedade
  - Nome do host
  - Nome do contato
  - Localização do contato
  - Tamanho da memória
  - Duplex
  - Suprimentos (exceto níveis)
  - Opções de entrada
  - Opções de saída
  - Aplicativos eSF
  - Certificado padrão da impressora

- **Impressoras gerenciadas (encontradas)** — Impressoras que foram exibidas como ausentes, mas que agora foram encontradas.
- **Impressoras gerenciadas (ausentes)** — Impressoras com as quais o sistema não conseguiu se comunicar.
- **Impressoras gerenciadas (normais)** — Impressoras no sistema cujas propriedades permanecem as mesmas desde a última auditoria.
- **Novas impressoras** — Impressoras que foram localizadas recentemente e que não foram definidas para um estado Gerenciado automaticamente.
- **Impressoras desativadas** — Impressoras que não estão mais ativas no sistema.
- **Impressoras não gerenciadas** — Impressoras que foram marcadas para exclusão nas atividades executadas no sistema.



Estado inicial	Estado final	Transição
Iniciar	Normal	Descoberta.[1]
Iniciar	Nova	Descoberta.[2]
Qualquer	Normal, Não gerenciada ou Desativada	Manual (Ausente não será alterada para Normal).
Desativada	Normal	Descoberta.[1]
Desativada	Nova	Descoberta.[2]
Normal, Ausente ou Não encontrada	Alterada	Novo endereço ao ser localizada.
Normal	Alterada	As propriedades de auditoria não correspondam às propriedades do banco de dados.
Normal, Alterada ou Não encontrada	Ausente	Não encontrada no status auditar ou atualizar.
Alterada	Normal	As propriedades de auditoria correspondam às propriedades do banco de dados.

[1] A definição “Gerenciar automaticamente impressoras descobertas” está habilitada no perfil de descoberta.

[2] A definição "Gerenciar automaticamente impressoras descobertas" está desabilitada no perfil de descoberta.

Estado inicial	Estado final	Transição
Ausente	Encontrada	Status descoberta, auditar ou atualizar.
Encontrada	Normal	Status descoberta, auditar ou atualizar.

[1] A definição “Gerenciar automaticamente impressoras descobertas” está habilitada no perfil de descoberta.

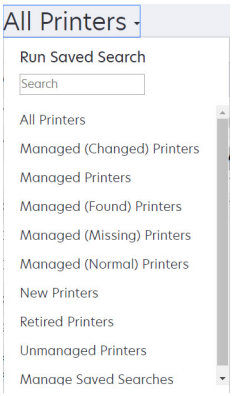
[2] A definição "Gerenciar automaticamente impressoras descobertas" está desabilitada no perfil de descoberta.

Como executar uma pesquisa salva

Uma pesquisa salva é um conjunto salvo de parâmetros que retorna as informações mais recentes da impressora que atendem aos parâmetros.

Você pode criar e executar uma pesquisa salva personalizada ou executar as pesquisas salvas geradas pelo sistema padrão. As pesquisas salvas geradas pelo sistema exibem as impressoras em seus estados do ciclo de vida. Para obter mais informações, consulte " Compreendendo os estados do ciclo de vida útil da impressora" na página 47.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. No menu suspenso, selecione uma pesquisa salva.



Criação de uma pesquisa salva

Utilização de filtros

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. No lado esquerdo da página, selecione os filtros.

   Nota: Os filtros selecionados estão listados acima do cabeçalho dos resultados da pesquisa.
3. Clique em **Salvar** e digite um nome exclusivo para a pesquisa salva e sua descrição.
4. Clique em **Criar pesquisa salva**.

Como usar a página da pesquisa salva

1. No menu Impressoras, clique em **Pesquisas salvas** > **Criar**.
2. Na seção Geral, digite um nome exclusivo para a pesquisa salva e sua descrição.

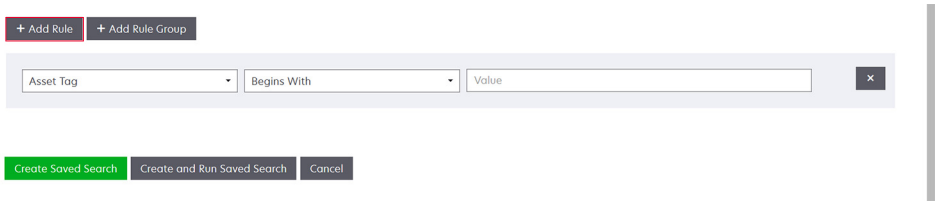
3 Na seção Regras e grupos de regras, no menu Correspondência, especifique se os resultados da pesquisa devem corresponder a qualquer regra ou a todas elas.

4 Execute uma das seguintes opções:

Adicionar uma regra

a Clique em **Adicionar regra**.

b Especifique o parâmetro, a operação e o valor para seus critérios de pesquisa. Para obter mais informações, consulte " Noções básicas sobre as configurações de critérios de pesquisa" na página 51.



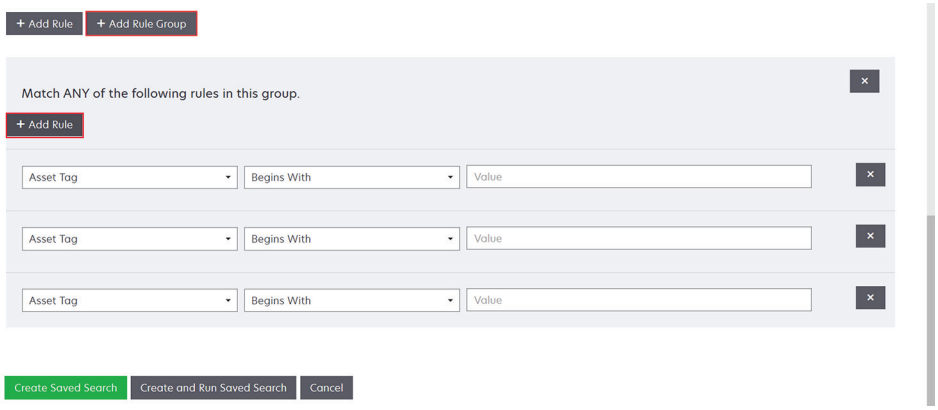
Adicionar um grupo de regras

Um grupo de regras pode conter uma combinação de regras. Se o menu Correspondência estiver definido como **QUAISQUER regras e grupos de regras**, o sistema procurará impressoras que correspondam a todas as regras no grupo de regras. Se o menu Correspondência estiver definido como **TODAS as regras e grupos de regras**, o sistema irá procurar por impressoras que correspondam a qualquer regra no grupo de regras.

a Clique em **Adicionar grupo de regras**.

b Especifique o parâmetro, a operação e o valor para seus critérios de pesquisa. Para obter mais informações, consulte " Noções básicas sobre as configurações de critérios de pesquisa" na página 51.

c Para adicionar outra regra, clique em **Adicionar regra**.



5 Clique em **Criar pesquisa salva** ou **Criar e executar pesquisa salva**.

Noções básicas sobre as configurações de critérios de pesquisa

Procure impressoras usando um ou mais dos seguintes parâmetros:

Parâmetro	Descrição
Etiqueta de ativo	O valor da configuração da etiqueta de ativo da impressora.
Data de criação do certificado[1]	A data em que o certificado foi criado.
Status do registro do certificado[1]	O status do registro do certificado.
Data de expiração do certificado[1]	A data em que o certificado expirou.
Data da renovação do certificado[1]	A data em que o certificado foi renovado.
Número da revisão do certificado[1]	O número da revisão do certificado.
Status da assinatura do certificado[1]	O status do certificado.
Status de validade do certificado[1]	A validade do certificado. **Nota:** O status Expiração próxima indica que o certificado expira em 30 dias.
Recurso Cor	A impressora imprime em preto e branco ou colorido.
Configuração	O nome da configuração atribuída à impressora.
Conformidade de configuração	O status de conformidade da impressora em relação à configuração atribuída.
Localização do contato	O valor da configuração de localização do contato da impressora.
Nome do contato	O valor da configuração de nome do contato da impressora.
Cópia	A impressora oferece suporte à função de cópia.
Data: Adicionado ao sistema	A data em que a impressora foi adicionada ao sistema.
Data: Auditada pela última vez	A data e a hora em que a impressora foi auditada pela última vez.
Data: Última verificação de conformidade	A data em que a conformidade de configuração da impressora foi verificada pela última vez.
Data: Descoberto pela última vez	A data em que a impressora foi descoberta pela última vez.
Criptografia de disco	A impressora está configurada para criptografia de disco.
Limpeza de disco	A impressora está configurada para limpeza de disco.
Frente e verso	A impressora oferece suporte à impressão em frente e verso.
Recurso eSF	A impressora suporta o gerenciamento de aplicativos eSF.
Informações sobre eSF	As informações sobre o aplicativo eSF instalado na impressora, como nome, estado e versão.
Nome do evento	O nome dos eventos atribuídos.
Nome do fax	O valor da configuração de nome do fax da impressora.
Número do fax	O valor da configuração de número do fax da impressora.
Recebimento de fax	A impressora oferece suporte ao recebimento de fax.

Parâmetro	Descrição
Informações de firmware	As informações sobre o firmware instalado na impressora. • **Nome**—O nome do firmware. Por exemplo, **Base** ou **Kernel**. • **Versão**—A versão do firmware da impressora.
Nome do host	O nome do host da impressora.
Endereço IP	O endereço IP da impressora. **Nota:** Você pode usar um asterisco nos últimos três octetos para procurar várias entradas. Por exemplo, **123.123.123.***, **123.123.*.***, **123.*.*.***, **2001:db8::2:1**, e **2001:db8:0:0:0:0:2:1**.
Palavra-chave	As palavras-chave atribuídas.
Total de páginas já impressas	O valor do total de páginas já impressas da impressora.
Endereço MAC	O endereço MAC da impressora.
Contador de manutenção	O valor do contador de manutenção da impressora.
Fabricante	O nome do fabricante da impressora.
Tecnologia de marcação	A tecnologia de marcação que a impressora suporta.
Recurso MFP	A impressora é um produto multifuncional (MFP).
Modelo	O nome do modelo da impressora.
Número de série modular	O número de série modular.
Status da impressora	O status da impressora. Por exemplo, **Pronto**, **Papel Preso**, **Bandeja 1 ausente**.
Gravidade do status da impressora	O valor do status mais grave presente na impressora. Por exemplo, **Desconhecido**, **Pronto**, **Aviso** ou **Erro**.
Perfil	A impressora suporta perfis.
Digitalizar para e-mail	A impressora suporta digitalização para e-mail.
Digitalizar para fax	A impressora suporta digitalização para fax.
Digitalização para rede	A impressora suporta digitalização para rede.
Estado de comunicação segura	O estado de segurança ou autenticação da impressora.
Número de série	O número de série da impressora.
Estado	O estado atual da impressora no banco de dados.
Status dos suprimentos	O status dos suprimentos da impressora.
Gravidade do status dos suprimentos	O valor do status dos suprimentos mais grave presente na impressora. Por exemplo, **Desconhecido**, **OK**, **Aviso** ou **Erro**.
Nome do sistema	O nome do sistema da impressora.
Fuso horário	O fuso horário da região onde a impressora está localizada.
TLI	O valor da configuração de TLI da impressora.

[1]Os parâmetros relacionados ao certificado são aplicáveis aos seguintes certificados de dispositivo:

- **Padrão**
- **HTTPS**

- **802.1x**
- **IPSec**

Use os seguintes operadores ao procurar impressoras:

- **Corresponde exatamente a** — Um parâmetro é equivalente a um valor especificado.
- **Não é** — Um parâmetro não é equivalente a um valor especificado.
- **Contém** — um parâmetro contém um valor especificado.
- **Não contém** — Um parâmetro não contém um valor especificado.
- **Começa com** — Um parâmetro começa com um valor especificado.
- **Termina com** — Um parâmetro termina com um valor especificado.
- **Data**
  - **Mais antigo que** — Um parâmetro para pesquisar dias antes dos dias especificados.
  - **Nos últimos** — Um parâmetro para pesquisar dentro dos dias especificados antes de hoje.
  - **Nos próximos** — Um parâmetro para pesquisar dentre os dias especificados depois de hoje.

Nota: Para pesquisar impressoras que têm parâmetros com valores vazios, use **_EMPTY_OR_NULL_**. Por exemplo, para procurar impressoras que têm Nome do fax vazio no campo Valor, digite **_EMPTY_OR_NULL_**.

Gerenciando pesquisas salvas

1. No menu Impressoras, clique em **Pesquisas salvas**.
2. Tente um dos seguintes métodos:

Editar uma pesquisa salva

a. Selecione uma pesquisa salva e clique em **Editar**.

Nota: As pesquisas salvas geradas pelo sistema não podem ser editadas. Para obter mais informações, consulte " Compreendendo os estados do ciclo de vida útil da impressora" na página 47.

b. Configure as definições.

c. Clique em **Salvar alterações** ou **Salvar e Executar**.

Copiar uma pesquisa salva

a. Selecione uma pesquisa salva e clique em **Copiar**.

b. Configure as definições.

c. Clique em **Criar pesquisa salva** ou **Criar e Executar pesquisa salva**.

Excluir pesquisas salvas

a. Selecione uma ou mais pesquisas salvas.

Nota: As pesquisas salvas geradas pelo sistema não podem ser excluídas. Para obter mais informações, consulte " Compreendendo os estados do ciclo de vida útil da impressora" na página 47.

b. Clique em **Excluir** e confirme a exclusão.

Amostra de cenários: Monitoramento dos níveis de toner de sua frota

Como equipe de TI da Empresa ABC, você deve organizar a frota de impressoras para monitorá-las facilmente. Você deseja monitorar o uso de toner das impressoras para determinar se os suprimentos precisam de substituição.

Exemplo de implementação

1. Crie uma pesquisa salva que recupera as impressoras cujos suprimentos têm erros ou avisos.

   Regra de amostra para sua pesquisa salva

   Parâmetro: **`Gravidade do status dos suprimentos`**

   Operação: **`Não é`**

   Valor: **`Suprimentos OK`**

2. Crie uma exibição que mostre o status, a capacidade e o nível dos suprimentos para cada impressora.

   Colunas de amostras a serem mostradas na exibição de suprimentos

   `Status dos suprimentos`
   `Capacidade do cartucho preto`
   `Nível do cartucho preto`
   `Capacidade do cartucho ciano`
   `Nível do cartucho ciano`
   `Capacidade do cartucho magenta`
   `Nível do cartucho magenta`
   `Capacidade do cartucho amarelo`
   `Nível do cartucho amarelo`

3. Execute a pesquisa salva enquanto usa a exibição.

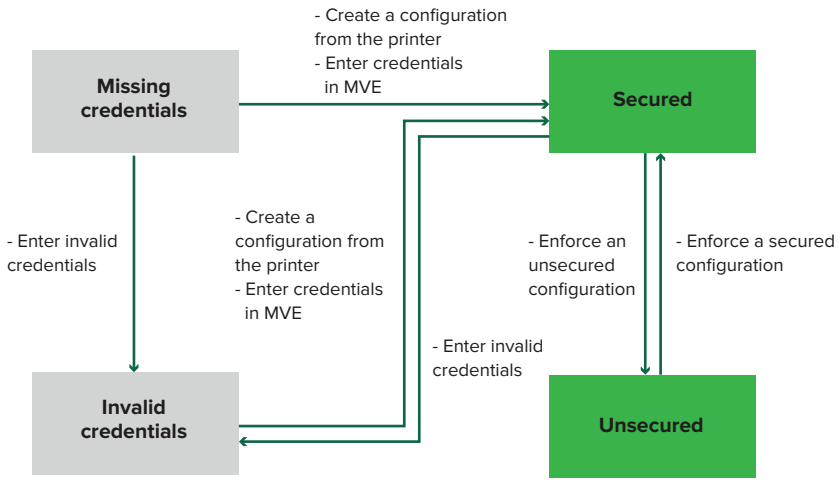
   Nota: As informações mostradas na exibição da listagem de impressoras são baseadas na última auditoria. Execute uma auditoria e uma atualização de status para obter o status atual da impressora.

Proteção das comunicações da impressora

Noções básicas sobre os estados de segurança da impressora

Durante a descoberta, a impressora pode estar em qualquer um dos seguintes estados de segurança:

- **Desprotegido** — O MVE não precisa de credenciais para se comunicar com o dispositivo.
- **Protegido** — O MVE precisa de credenciais e elas foram fornecidas.
- **Faltam credenciais** — O MVE precisa de credenciais, mas elas não foram fornecidas.
- **Credenciais inválidas** — O MVE precisa de credenciais, mas foram fornecidas credenciais incorretas.



Uma impressora está no estado Credenciais inválidas quando as credenciais são consideradas inválidas durante a descoberta, auditoria, atualização de status, verificação de conformidade ou aplicação da configuração.

A impressora está no estado Desprotegido somente quando não precisa de credenciais durante a descoberta.

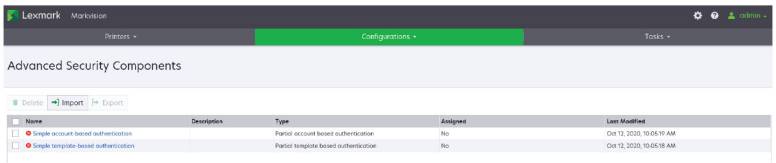
Para alterar o status Desprotegido para Protegido, aplique uma configuração segura.

Para mover uma impressora dos estados Faltam credenciais ou Credenciais inválidas, insira as credenciais no MVE manualmente ou crie uma configuração a partir da impressora.

Proteção das impressoras usando as configurações padrão

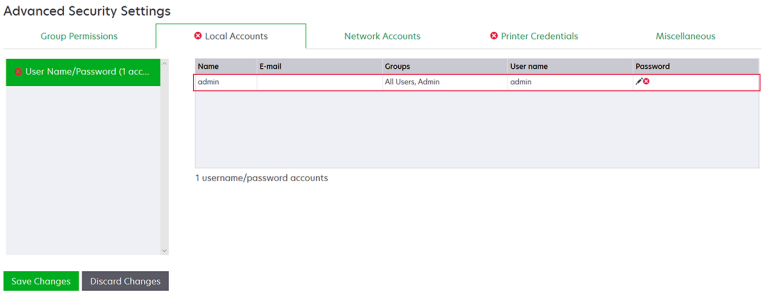
Em alguns modelos de impressora, não há usuário administrador padrão. O usuário Convidado tem acesso aberto e não está conectado. Essa configuração concede ao usuário acesso a todas as permissões e controles de acesso da impressora. O MVE lida com esse risco por meio de configurações padrão. Após uma nova instalação, dois componentes de segurança avançada são criados automaticamente. Cada componente contém as configurações de segurança padrão e a conta de administrador local pré-configurada. Você pode usar esses componentes de segurança ao criar uma configuração e, em seguida, implantar e aplicar a configuração às novas impressoras.

No menu Configurações, clique em **Todos os componentes de segurança avançada**.

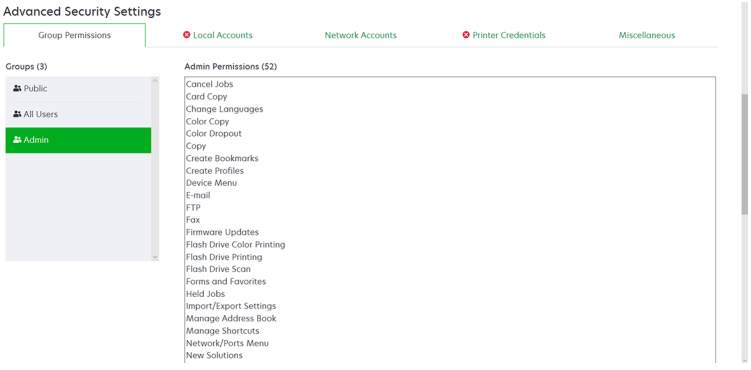


Autenticação simples baseada em conta

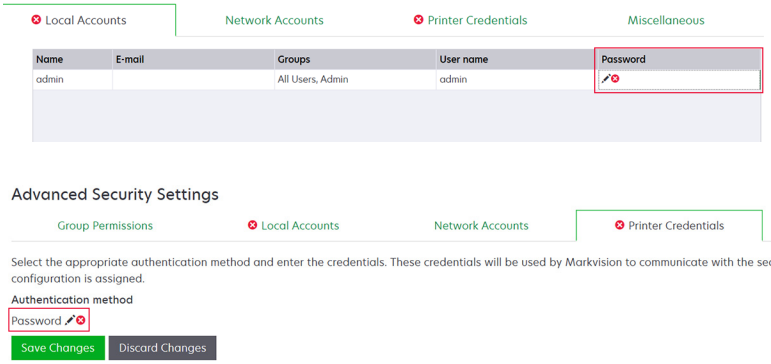
Esse componente de segurança contém uma Conta local com nome de usuário/senha chamada **Administrador**.



A conta **admin** é membro do grupo Admin, cujas permissões incluem controles e permissões de acesso a funções para proteger a impressora e restringir o acesso público. Para mais informações, consulte " Compreensão dos controles de acesso a funções e permissões" na página 58.

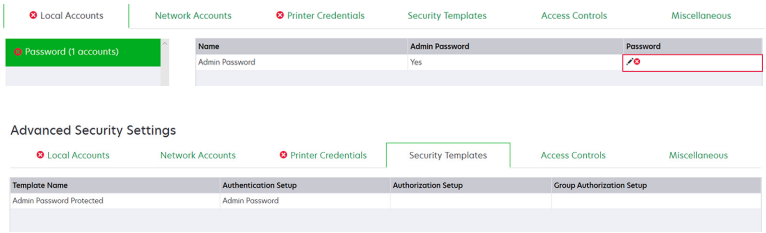


Antes de adicionar esse componente a uma configuração, certifique-se de definir a senha de **admin** e as credenciais da impressora.



Autenticação simples baseada em modelo

Esse componente de segurança contém um modelo de segurança chamado Protegido com senha de administrador que é configurado com uma Conta local com senha.

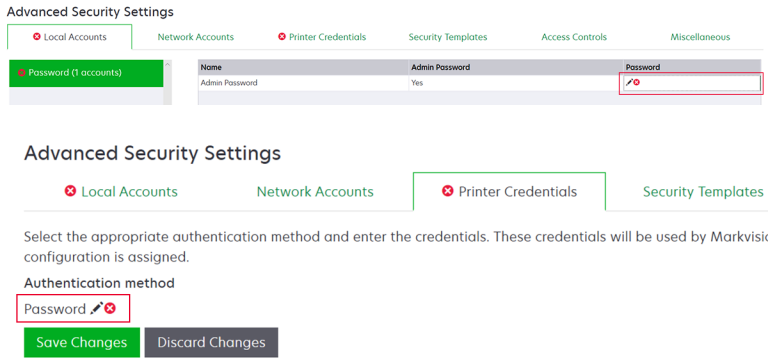


Esse modelo de segurança é aplicado aos seguintes controles de acesso:

- Atualizações de firmware
- Gerenciamento remoto
- Menu Segurança remoto

Os controles de acesso restantes são definidos como **Sem segurança**. No entanto, você sempre pode definir os outros menus administrativos da impressora para usar o modelo de segurança para obter mais proteção. Para obter mais informações sobre os controles de acesso, consulte " Compreensão dos controles de acesso a funções e permissões" na página 58.

Antes de adicionar esse componente a uma configuração, certifique-se de definir a senha e as credenciais da impressora.



Compreensão dos controles de acesso a funções e permissões

As impressoras podem ser configuradas para restringir o acesso público a menus administrativos e recursos de gerenciamento de dispositivos. Em modelos de impressora mais recentes, as permissões para acessar as funções da impressora podem ser protegidas por diferentes tipos de métodos de autenticação. Em modelos de impressora mais antigos, um modelo de segurança pode ser aplicado a um controle de acesso a funções (FAC).

Para se comunicar com essas impressoras protegidas e gerenciá-las, o MVE requer certas permissões ou FACs, dependendo do modelo da impressora.

A tabela a seguir explica quais funções de gerenciamento de impressora podem ser gerenciadas no MVE e quais permissões ou FACs são exigidas.

Note que o MVE requer as credenciais de autenticação quando o Gerenciamento remoto estiver protegido. Se outros menus administrativos e permissões de gerenciamento de dispositivos ou FACs estiverem protegidos, o Gerenciamento remoto também deve estar protegido. Caso contrário, o MVE não poderá executar as funções.

Essas permissões e controles de acesso a funções são predefinidos no MVE como componentes de segurança avançados padrão e podem ser facilmente usados em uma configuração. Para obter mais informações, consulte " Proteção das impressoras usando as configurações padrão" na página 56.

Se você não estiver usando os componentes de segurança avançada padrão, verifique se esses controles de acesso a funções e permissões estão configurados na impressora manualmente. Para obter mais informações, consulte " Configurando a segurança da impressora" na página 59.

Permissões ou FACs	Descrição
Gerenciamento remoto	A capacidade de ler e gravar definições remotamente. Se quaisquer outras permissões ou FACs listados nesta tabela estiverem protegidas, o Gerenciamento remoto também deve estar protegido.
Atualizações de firmware	A capacidade de atualizar o firmware a partir de qualquer método.
Configuração de aplicativos	A capacidade de instalar ou remover aplicativos da impressora e enviar arquivos de definições do aplicativo para a impressora.
Importar/exportar todas as definições ou **Importação/exportação do arquivo de configuração**	A capacidade de enviar arquivos de configuração para a impressora.
Menu de segurança ou **Menu segurança exibido remotamente**	A capacidade de gerenciar métodos de login e configurar opções de segurança da impressora.

Para proteger modelos de impressora mais recentes no MVE, desative o acesso público para as permissões de Gerenciamento remoto e de Menu de segurança. Para modelos de impressora mais antigos, aplique um modelo de segurança ao FAC do Gerenciamento remoto.

Configurando a segurança da impressora

1 No menu Impressoras, clique em **Listagem de impressoras**.

2 Clique no endereço IP da impressora e clique em **Abrir Embedded Web Server**.

3 Clique em **Definições** ou em **Configuração**.

4 Dependendo do modelo da sua impressora, faça o seguinte:

- Clique em **Segurança** > **Métodos de login**e, em seguida, faça o seguinte:

  ### Para modelos de impressora recentes

  a Na seção Segurança, crie um método de login.
  b Clique em **Gerenciar grupo/permissões** ou **Gerenciar permissões** ao lado do método de login.
  c Expanda **Menus administrativos** e selecione **Menu de segurança**.
  d Expanda **Acesso a funções** e selecione as seguintes permissões:
  - **Gerenciamento remoto**
  - **Atualizações de firmware**
  - **Configuração de aplicativos**
  - **Importar/exportar todas as definições**

  e Clique em **Salvar**.
  f Na seção Público, clique em **Gerenciar permissões**.
  g Expanda **Menus administrativos**, e desmarque **Menu de segurança**.
  h Expanda **Gerenciamento de dispositivo** e desmarque **Gerenciamento remoto**.
  i Clique em **Salvar**.

- Clique em **Segurança** > **Configuração de segurança** ou em **Editar configuração de segurança** e faça o seguinte:

  ### Para modelos de impressora antigos

  a Na seção Configuração de segurança avançada, crie um bloco de construção e um modelo de segurança.
  b Clique em **Controles de acesso** e expanda **Menus administrativos**.
  c No Menu de segurança remoto, selecione o modelo de segurança.
  d Expanda **Gerenciamento** e selecione o modelo de segurança para os seguintes controles de acesso a funções:
  - **Configuração de aplicativos**
  - **Gerenciamento remoto**
  - **Atualizações de firmware**
  - **Importação/exportação do arquivo de configuração**

  e Clique em **Enviar**.

Proteção das comunicações da impressora no parque de impressão

1 Descobrir uma impressora protegida. Para mais informações, consulte " Descoberta de impressoras" na página 34.

Notas:

- Uma impressora está protegida quando é exibido perto dela. Para obter informações sobre como proteger uma impressora, consulte o **documento de ajuda**.
- Para obter mais informações sobre os estados de segurança da impressora, consulte " Noções básicas sobre os estados de segurança da impressora" na página 55.

2. Criar uma configuração a partir de uma impressora. Para mais informações, consulte " Criando uma configuração a partir de uma impressora" na página 71.
3. Atribuir a configuração ao parque de impressão. Para mais informações, consulte " Como atribuir configurações a impressoras" na página 62.
4. Aplicar a configuração. Para mais informações, consulte " Aplicando configurações" na página 62. Um símbolo de cadeado é exibido ao lado da impressora protegida.

Outras maneiras de proteger suas impressoras

Para obter mais informações sobre como definir as configurações de segurança da impressora, consulte o *Guia do administrador do Embedded Web Server* da impressora.

Verifique as seguintes configurações em suas impressoras:

- A criptografia de disco está ativada.
- As seguintes portas estão restringidas:
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- A lista de criptografias padrão é a String de criptografia OWASP 'B'.

Gerenciamento de impressoras

Reiniciando a impressora

1. Na pasta Impressoras menu, clique em **Lista de impressoras**.
2. Clique no endereço IP da impressora.
3. Clique em **Reiniciar impressora**.

Exibindo o Embedded Web Server da impressora

O Embedded Web Server é um software integrado na impressora que fornece um painel de controle para configurar a impressora em qualquer navegador da Web.

1. Na pasta Impressoras menu, clique em **Lista de impressoras**.
2. Clique no endereço IP da impressora.
3. Clique em **Abrir o Embedded Web Server**.

Auditando impressoras

Uma auditoria coleta informações de qualquer impressora no estado Gerenciado e armazena as informações no sistema. Para certificar-se de que as informações no sistema sejam atuais, execute uma auditoria regularmente.

1. No menu Impressoras, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Impressora** > **Auditar**.

   Nota: Uma auditoria pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Atualização do status da impressora

O recurso Atualizar status permite a atualização do status da impressora e das informações de suprimentos. Para garantir que o status da impressora e as informações de suprimentos estejam atualizados, atualize o status regularmente.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Impressora** > **Atualizar status**.

   Nota: Uma atualização de status pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Configurando o estado da impressora

Para obter mais informações sobre os estados da impressora, consulte " Compreendendo os estados do ciclo de vida útil da impressora" na página 47.

1. No menu Impressoras, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Impressora** e selecione uma das opções a seguir:
   - **Definir o estado como gerenciado**—A impressora é incluída em todas as atividades que podem ser executadas no sistema.
   - **Definir o estado como não gerenciado**—A impressora é excluída de todas as atividades que podem ser executadas no sistema.
   - **Definir estado como desativado**—A impressora é removida da rede. O sistema mantém as informações da impressora, mas não espera ver a impressora na rede novamente.

Como atribuir configurações a impressoras

Antes de iniciar, certifique-se de que foi criada uma configuração para a impressora. Atribuir uma configuração para uma impressora permite que o sistema execute verificações de conformidade e aplicações. Para obter mais informações, consulte " Criação de configurações" na página 68.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Configurar** > **Atribuir configurações**.
4. Na seção Configuração, selecione uma configuração.

   Nota: Se o sistema estiver definido como **Usar o Markvision para gerenciar certificados de dispositivos**, selecione **Confiar nos dispositivos selecionados**. Essa confirmação é a forma como o usuário verifica se as impressoras são dispositivos reais e não são falsificadas.
5. Clique em **Atribuir configurações**.

Cancelando atribuições de configurações

1. No menu Impressoras, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Configurar** > **Cancelar atribuição de configurações**.
4. Clique em **Cancelar atribuição de configurações**.

Aplicando configurações

O MVE executa uma verificação de conformidade na impressora. Se algumas configurações estiverem fora de conformidade, o MVE altera essas configurações na impressora. O MVE executa uma verificação de conformidade final após alterar as configurações. As atualizações que exigirem a reinicialização da impressora, como atualizações de firmware, podem exigir uma segunda aplicação para concluir.

Antes de iniciar, certifique-se de que uma configuração foi atribuída à impressora. Para obter mais informações, consulte " Como atribuir configurações a impressoras" na página 62.

1 Na pasta Impressoras menu, clique em **Lista de impressoras**.

2 Selecione uma ou mais impressoras.

3 Clique em **Configurar** > **Aplicar configurações**.

Notas:

- Se a impressora estiver em um estado de erro, talvez algumas configurações não sejam atualizadas.
- Para que o MVE implante arquivos de firmware e de solução em uma impressora, o controle de acesso à função de Atualizações de firmware precisa estar definido como **Sem segurança**. Se a segurança estiver aplicada, o controle de acesso à função de Atualizações de firmware deverá usar o mesmo modelo de segurança que o controle de acesso à função de Gerenciamento remoto. Para obter mais informações, consulte " Implantando arquivos em impressoras" na página 63.
- Uma aplicação pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Verificando a conformidade da impressora com uma configuração

Durante uma verificação de conformidade, o MVE verifica as configurações da impressora e se elas correspondem à configuração atribuída. O MVE não faz alterações na impressora durante essa operação.

Antes de iniciar, certifique-se de que uma configuração foi atribuída à impressora. Para obter mais informações, consulte " Como atribuir configurações a impressoras" na página 62.

1 Na pasta Impressoras menu, clique em **Lista de impressoras**.

2 Selecione uma ou mais impressoras.

3 Clique em **Configurar** > **Verificar conformidade**.

Notas:

- É possível visualizar os resultados na página de status da tarefa.
- Uma verificação de conformidade pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Implantando arquivos em impressoras

Você pode implantar os seguintes arquivos na impressora:

- **Certificados CA**: arquivos **.cer** ou **.pem** adicionados ao armazenamento confiável da impressora.
- **Pacote de configuração**: arquivos **.zip** exportados de uma impressora compatível ou obtidos diretamente da Lexmark.
- **Atualização de firmware**: um arquivo **.fls** que é enviado para a impressora.
- **Arquivo genérico**: qualquer arquivo que você deseja enviar para a impressora.
  - **Soquete bruto**: enviado pela porta 9100. A impressora trata como qualquer outro dado de impressão.
  - **FTP**: envie o arquivo por FTP. Este método de implantação não é suportado em impressoras seguras.

- **Certificado de impressora**: um certificado assinado instalado na impressora como o certificado padrão.
- **Universal Configuration File (UCF)**: um arquivo de configuração exportado de uma impressora.
  - **Web service**: o Web service HTTPS é usado quando o modelo da impressora tem suporte a ele. Caso contrário, a impressora usará o Web service HTTP.
  - **FTP**: envie o arquivo por FTP. Este método de implantação não é suportado em impressoras seguras.

1. Na pasta Impressoras menu, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Configurar** > **Implantar arquivo em impressoras**.
4. Clique em **Escolha arquivo** e vá para o arquivo.
5. Selecione um tipo de arquivo e um método de implantação.
6. Clique em **Implantar arquivo**.

Notas:

- Para que o MVE implante arquivos de firmware e de solução em uma impressora, o controle de acesso à função de Atualizações de firmware precisa estar definido como **Sem segurança**. Se a segurança estiver aplicada, o controle de acesso à função de Atualizações de firmware deverá usar o mesmo modelo de segurança que o controle de acesso à função de Gerenciamento remoto.
- Uma implementação de arquivo pode ser programada para ocorrer regularmente. Para obter mais informações, consulte " Como criar uma programação" na página 145.

Atualizando o firmware da impressora

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Configurar** > **Atualizar firmware de impressoras**.
4. Selecione um arquivo de firmware na biblioteca de recursos ou clique em **Escolher arquivo** e navegue até o arquivo de firmware.

   Nota: Para mais informações sobre como adicionar arquivos de firmware à biblioteca, consulte " Importação de arquivos para a biblioteca de recursos" na página 75.
5. Se necessário, para programar a atualização, selecione **Definir janela de atualização** e selecione a data de início, a hora de início e de pausa, e os dias da semana.

   Nota: O firmware é enviado para as impressoras dentro da hora de início e tempo de pausa especificados. A tarefa será pausada após o tempo de pausa e retomada na próxima hora de início até que seja concluída.
6. Clique em **Atualizar firmware**.

Nota: Para que o MVE atualize o firmware da impressora, o controle de acesso à funções de Atualizações de firmware precisa estar definido como **Sem segurança**. Se a segurança estiver aplicada, o controle de acesso à função de Atualizações de firmware deverá usar o mesmo modelo de segurança que o controle de acesso a funções de Gerenciamento remoto. Nesse caso, o MVE deve gerenciar a impressora de forma segura. Para obter mais informações, consulte " Proteção das comunicações da impressora" na página 55.

Desinstalação de aplicativos das impressoras

O MVE pode desinstalar somente os aplicativos que foram adicionados ao sistema no formato Package Builder. Para obter mais informações sobre o carregamento de aplicativos para o sistema, consulte " Importação de arquivos para a biblioteca de recursos" na página 75.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Configurar** > **Desinstalar aplicativos de impressoras**.
4. Selecione os aplicativos.
5. Clique em **Desinstalar aplicativos**.

Atribuindo eventos a impressoras

A opção “atribuindo eventos a impressoras” permite que o MVE execute a ação associada sempre que um dos alertas associados ocorrer na impressora atribuída. Para obter mais informações sobre a criação de eventos, consulte " Gerenciamento de alertas da impressora" na página 135.

Nota: Os eventos podem ser atribuídos somente a impressoras não-seguras.

1. No menu Impressoras, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Atribuir** > **eventos**.
4. Selecione um ou mais eventos.

   Nota: Se o evento já tiver sido atribuído a algumas das impressoras selecionadas, um traço será exibido na caixa de seleção. Se você deixá-lo como um traço, o evento não será alterado. Se você marcar a caixa de seleção, o evento será atribuído a todas as impressoras selecionadas. Se você desmarcar a caixa de seleção, a atribuição do evento será cancelada das impressoras às quais havia sido atribuído anteriormente.
5. Clique em **Atribuir eventos**.

Atribuindo palavras-chave a impressoras

Atribuir palavras-chave a impressoras permite organizar suas impressoras. Para obter mais informações sobre a criação de palavras-chave, consulte " Gerenciamento de palavras-chave" na página 47.

1. No menu Impressoras, clique em **Lista de impressoras**.
2. Selecione uma ou mais impressoras.
3. Clique em **Atribuir** > **Palavras-chave**.
4. Se necessário, no menu Exibir, selecione uma categoria.

5 Selecione uma ou mais palavras-chave.

Nota: As palavras-chave são listadas de acordo com uma categoria. Se a palavra-chave já tiver sido atribuída a algumas das impressoras selecionadas, um traço será exibido na caixa de seleção. Se você deixar o traço inalterado, a palavra-chave não será atribuída às impressoras selecionadas ou a atribuição será cancelada. Se você marcar a caixa de seleção, a palavra-chave será atribuída a todas as impressoras selecionadas. Se você desmarcar a caixa de seleção, a atribuição da palavra-chave será cancelada das impressoras às quais havia sido atribuída anteriormente.

6 Clique em **Atribuir palavras-chave**.

Inserindo credenciais em impressoras protegidas

Impressoras protegidas podem ser descobertas e registradas. Para se comunicar com essas impressoras, você pode aplicar uma configuração ou inserir as credenciais diretamente no MVE.

Nota: Uma impressora está protegida quando um é exibido próximo a ela.

Para inserir as credenciais, faça o seguinte:

1 No menu Impressoras, clique em **Listagem de impressoras**.

2 Selecione uma ou mais impressoras protegidas.

3 Clique em **Segurança** > **Inserir credenciais**.

4 Selecione o método de autenticação e insira as credenciais.

5 Clique em **Inserir credenciais**.

Nota: As impressoras registradas protegidas que não têm as credenciais corretas salvas no MVE são marcadas como Credenciais ausentes no filtro Comunicações. Após inserir as credenciais corretas, as impressoras são marcadas como Protegida.

Configuração manual dos certificados da impressora padrão

Quando não estiver usando o recurso de gerenciamento de certificado automatizado, o MVE pode ajudar a facilitar o processo de assinatura do certificado de impressora padrão em um parque de impressão. O MVE reúne as solicitações de assinatura de certificado da frota e, em seguida, implanta os certificados assinados às impressoras adequadas após serem assinados.

Um administrador do sistema deve fazer o seguinte:

1 gerar as solicitações de assinatura do certificado da impressora.

   a No menu Impressoras, clique em **Listagem de impressoras**.

   b Selecione uma ou mais impressoras.

   c Clique em **Segurança** > **Gerar solicitações de assinatura do certificado da impressora**.

Nota: Você pode selecionar uma ou mais impressoras ao gerar solicitações de assinatura do certificado, mas apenas um conjunto de solicitações pode existir por vez. Para evitar a substituição de qualquer solicitação de assinatura do certificado existente, você deve baixar as solicitações de assinatura do certificado antes de gerar outro conjunto.

2 Aguarde até que a tarefa seja concluída e baixe as solicitações de assinatura do certificado da impressora.
   a No menu Impressoras, clique em **Listagem de impressoras**.
   b Clique em **Segurança** > **Baixar solicitações de assinatura do certificado da impressora**.
3 Use um CA confiável para assinar as solicitações de assinatura do certificado.
4 Salve os certificados assinados em um arquivo ZIP.

   Nota: Todos os certificados assinados devem estar no local raiz do arquivo ZIP. Caso contrário, o MVE não poderá analisar o arquivo.
5 No menu Impressoras, clique em **Listagem de impressoras**.
6 Selecione uma ou mais impressoras.
7 Clique em **Configurar** > **Implantar arquivo em impressoras**.
8 Clique em **Escolher arquivo** e busque o arquivo ZIP.
9 No menu Tipo de arquivo, selecione **Certificados da impressora**.
10 Clique em **Implantar arquivo**.

Remoção de impressoras

1 No menu Impressoras, clique em **Listagem de impressoras**.
2 Selecione uma ou mais impressoras.
3 Clique em **Impressora**.
4 Se necessário, para remover o certificado da impressora, selecione **Excluir certificado(s) associado(s) do dispositivo**.

   Nota: Se o MVE estiver gerenciando os certificados de dispositivo, a remoção do certificado da impressora excluirá o certificado padrão da impressora. Em seguida, a impressora gera um novo certificado autoassinado.
5 Execute um dos seguintes procedimentos:
   - Para reter informações da impressora, clique em **Aposentar impressora**.
   - Para remover a impressora do sistema, clique em **Excluir impressora**.

Gerenciamento de configurações

Visão geral

O MVE usa configurações para gerenciar o parque de impressão.

Uma configuração é um conjunto de definições que podem ser atribuídas e aplicadas a uma impressora ou grupo de impressoras. Em uma configuração, você pode modificar as configurações da impressora e implantar aplicativos, licenças, firmwares e certificado de impressoras.

Você pode criar uma configuração composta pelos seguintes itens:

- Configurações básicas da impressora
- Configurações de segurança avançada
- Permissões de impressão colorida

  Nota: Essa configuração está disponível somente em impressoras coloridas compatíveis.
- Firmware da impressora
- Aplicativos
- Certificados CA
- Arquivos de recursos

Usando as configurações, você pode fazer o seguinte para gerenciar as impressoras:

- Atribuir uma configuração a impressoras.
- Aplicar a configuração às impressoras. As definições especificadas na configuração são aplicadas às impressoras. O firmware, os aplicativos, o certificado da impressora, os arquivos de aplicativo (.fls) e os certificados CA estão instalados.
- Verificar se as impressoras estão em conformidade com uma configuração. Se uma impressora estiver fora de conformidade, a configuração poderá ser aplicada à impressora.

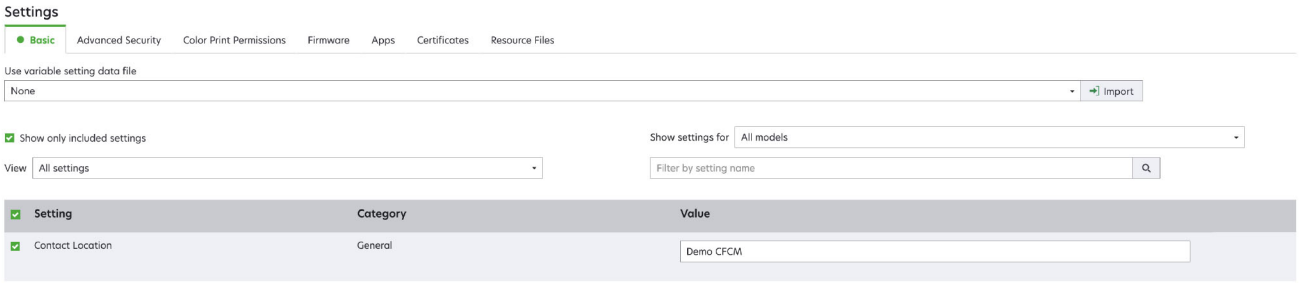
  Nota: Uma verificação e uma aplicação de conformidade podem ser programadas para ocorrer regularmente.
- Se a impressora suportar as definições de configuração, mas os valores não forem aplicáveis, a impressora será exibida como fora de conformidade.

Criação de configurações

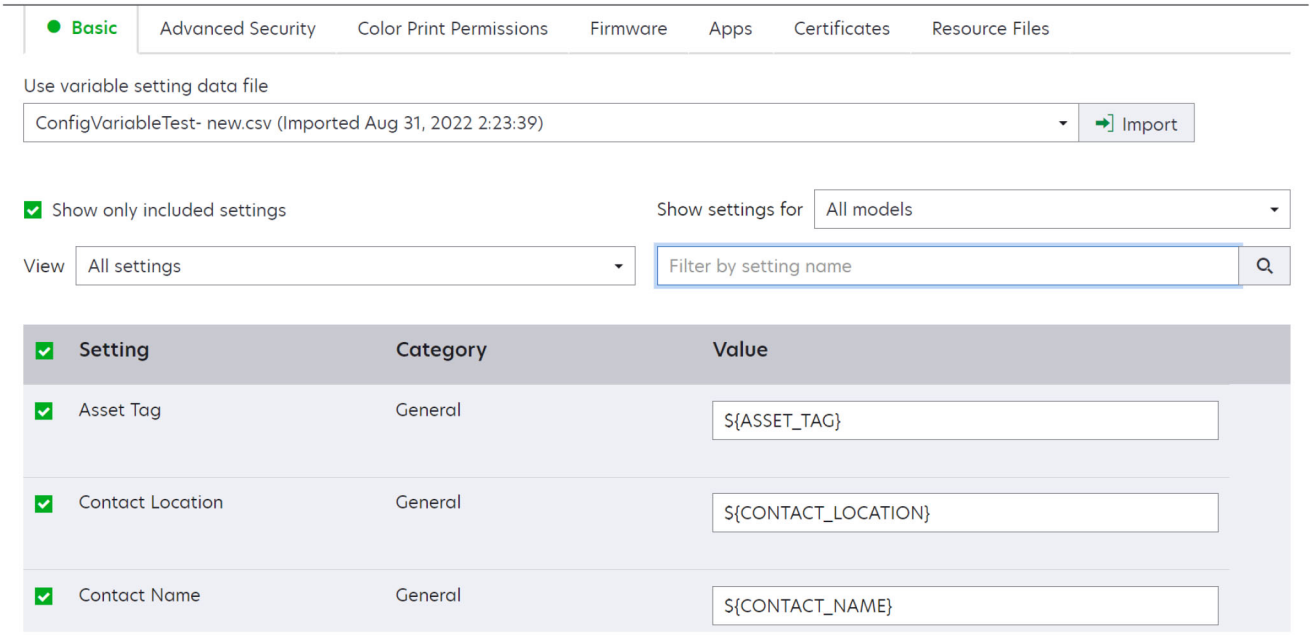
Uma configuração é um conjunto de definições que podem ser atribuídas e aplicadas a uma impressora ou grupo de impressoras. Em uma configuração, é possível modificar as configurações da impressora e implantar aplicativos, licenças, firmware e certificados CA a impressoras.

1. No menu Configurações, clique em **Todas as configurações** > **Criar**.
2. Digite um nome exclusivo para a configuração e sua descrição.
3. Na lista Configurações, execute um ou mais dos seguintes procedimentos:
   - Na guia Básico, selecione uma ou mais configurações e especifique os valores. Se o valor for uma configuração de variável, insira **`${}`** no cabeçalho. Por exemplo, **`${Contact_Name}`**. Para usar um arquivo de configuração de variável, selecione o arquivo no menu Utilizar arquivo de dados de

configuração de variáveis ou importe o arquivo. Para obter mais informações, consulte " Aprendendo sobre definições de variável" na página 72.



- Selecione uma ou mais configurações e especifique os valores. Se o valor for uma configuração de variável, insira **${}** no cabeçalho. Por exemplo, **${Contact_Name}**. Para usar um arquivo de configuração de variável, selecione o arquivo no menu Utilizar arquivo de dados de configuração de variáveis ou importe o arquivo. Para obter mais informações, consulte " Aprendendo sobre definições de variável" na página 72.



- Se um ou mais certificados forem adicionados a essa configuração, você poderá selecionar qualquer um dos certificados no menu suspenso **Valor**.

- Na guia Segurança avançada, selecione um componente de segurança avançada.

  Notas:

  - Para criar um componente de segurança avançada, consulte " Criação de um componente de segurança avançada a partir de uma impressora" na página 72.
  - Você pode gerenciar as configurações de segurança avançada somente ao criar uma configuração a partir de uma impressora selecionada. Para obter mais informações, consulte " Criando uma configuração a partir de uma impressora" na página 71.

- Na guia Permissões de impressão colorida, defina as configurações. Para obter mais informações, consulte " Configurando as permissões de impressão colorida" na página 73.

  Nota: Essa configuração está disponível somente para impressoras coloridas compatíveis.
- Na guia Firmware, selecione um arquivo de firmware. Se várias versões do mesmo firmware estiverem presentes em uma configuração, somente a versão do firmware superior será considerada durante a conformidade e a aplicação. Para importar um arquivo de firmware, consulte " Importação de arquivos para a biblioteca de recursos" na página 75.
- Na guia Aplicativos, selecione um ou mais aplicativos para implantar. Para obter mais informações, consulte " Criando um pacote de aplicativos" na página 74.

  Nota: O MVE não é compatível com a implantação de aplicativos com licenças de teste. É possível implantar somente aplicativos gratuitos ou que tenham licenças de produção.
- Na guia Certificados, selecione um ou mais certificados para implantar. Para importar um arquivo de certificado, consulte " Importação de arquivos para a biblioteca de recursos" na página 75.

  Nota: Selecione **Usar o Markvision para gerenciar certificados de dispositivos** para MVE para avaliar certificados ausentes, inválidos, revogados e expirados e depois os substitua automaticamente.

  Selecione uma das seguintes opções:
  - Certificado padrão do dispositivo
  - Certificado nomeado do dispositivo

    Nota: Por padrão, um usuário pode adicionar 10 certificados nomeados por instalação do MVE e 5 certificados nomeados por configuração do MVE.

  Nota: Para obter mais informações, consulte " Configuração do MVE para gerenciamento automatizado de certificados" na página 78.
- Na guia Arquivos de recursos, selecione uma das seguintes opções a ser implantada:
  - **Arquivo do aplicativo (.fls)**
  - **Conjunto de configurações (.zip)**
  - **Arquivo de configuração universal (.ucf)**

  Notas:

  - Nenhuma opção na guia do recurso possui verificações de conformidade.
  - Nós não recomendamos usar vários conjuntos de configurações e UCF em uma única configuração.
  - Este método não se aplica a arquivos UCF ao configurar a digitalização para rede em impressoras legadas. Os arquivos UCF devem ser implantados usando a ação **Implantar arquivo na impressora**.

4 Clique em **Criar configuração**.

Nota: A lista a seguir mostra a sequência de implantação em uma configuração:

- **Certificados CA**
- **Arquivos do aplicativo**
- **Pacotes de soluções**
- **Segurança avançada**
- **Certificados de dispositivo**
- **Configurações básicas**

- **UCF e conjunto de configurações**
- **Firmware**

Criando uma configuração a partir de uma impressora

Os componentes a seguir não estão incluídos:

- Firmware da impressora
- Aplicativos
- Certificados

Para adicionar firmware, aplicativos e certificados, edite a configuração no MVE.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione a impressora e clique em **Configurar** > **Criar configuração a partir da impressora**.
3. Se necessário, selecione **Incluir definições de segurança avançada** para criar um componente de segurança avançada a partir da impressora selecionada.
4. Se a impressora estiver protegida, selecione o método de autenticação e insira as credenciais.
5. Digite um nome exclusivo para a configuração e sua descrição e clique em **Criar configuração**.
6. No menu Configurações, clique em **Todas as configurações**.
7. Selecione a configuração e clique em **Editar**.
8. Se necessário, edite as definições.
9. Clique em **Salvar alterações**.

Amostra de cenários: Clonagem de uma configuração

Quinze impressoras Lexmark MX812 foram adicionadas ao sistema após a descoberta. Como equipe de TI, você deve aplicar as configurações das impressoras existentes às impressoras recém-descobertas.

Nota: Você também pode clonar uma configuração de uma impressora e, em seguida, aplicar a configuração a um grupo de modelos de impressoras.

Exemplo de implementação

1. Na lista de impressoras existentes, selecione uma impressora Lexmark MX812.
2. Crie uma configuração a partir da impressora.

   Nota: Para proteger as impressoras, inclua as configurações de segurança avançada.
3. Atribua e aplique a configuração às impressoras recentemente descobertas.

Criação de um componente de segurança avançada a partir de uma impressora

Crie um componente de segurança avançada a partir de uma impressora para gerenciar as definições de segurança avançada. O MVE lê todas as definições dessa impressora e cria um componente que inclui essas definições. O componente pode ser associado a várias configurações para modelos de impressora que têm a mesma estrutura de segurança.

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Selecione a impressora e clique em **Configurar** > **Criar componente de segurança avançada a partir da impressora**.
3. Digite um nome exclusivo para o componente e sua descrição.
4. Se a impressora estiver protegida, selecione o método de autenticação e insira as credenciais.
5. Clique em **Criar componente**.

   Nota: Quando você cria e aplica uma configuração com um componente de segurança avançada que contém contas locais, as contas locais são adicionadas às impressoras. Todas as contas locais existentes pré-configuradas na impressora serão retidas.

Geração de uma versão para impressão das definições de configuração

1. Edite uma configuração ou um componente de segurança avançada.
2. Clique em **Versão compatível com impressora**.

Noções básicas sobre configurações dinâmicas

- Essas configurações incluem Certificado de dispositivo 802.1x, Certificado de dispositivo HTTPS e Certificado de dispositivo IPSec, que são listados na guia Básico de uma configuração.
- As opções para cada uma dessas configurações são preenchidas com os certificados selecionados na guia Certificado.
- Quando você clona, exporta ou importa uma configuração, os valores pré-selecionados dessas configurações são apagados. Você deve selecionar os valores manualmente.

Aprendendo sobre definições de variável

Configurações de variáveis permitem que você gerencie as configurações de toda a sua frota, que são exclusivas de cada impressora, como nome do host ou etiqueta de ativo. Ao criar ou editar uma configuração, é possível selecionar um arquivo CSV para ser associado com a configuração.

Formato CSV de amostra:

```
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
```

Na linha do cabeçalho do arquivo variável, a primeira coluna é um token identificador exclusivo da impressora. O token deve ser um dos seguintes:

- **HOSTNAME**
- **IP_ADDRESS**
- **SYSTEM_NAME**
- **SERIAL_NUMBER**

Cada coluna subsequente na linha do cabeçalho do arquivo variável é um token de substituição definido pelo usuário. Esse token deve ser mencionado na configuração utilizando o formato ${HEADER}. Ele é substituído pelos valores nas linhas subsequentes quando a configuração é aplicada. Certifique-se de que os tokens não contenham espaços.

É possível importar o arquivo CSV que contém definições de variáveis ao criar ou editar uma configuração. Para obter mais informações, consulte " Criação de configurações" na página 68.

Configurando as permissões de impressão colorida

O MVE permite que você restrinja a impressão colorida para computadores host e usuários específicos.

Nota: Esta configuração está disponível somente em impressoras coloridas compatíveis.

1. No menu Configurações, clique em **Todas as configurações**.
2. Crie ou edite uma configuração.
3. Na guia Permissões de impressão colorida, execute um dos seguintes procedimentos:

Configurar as permissões de impressão colorida para computadores host

a. No menu Exibir, selecione **Computadores host** e, em seguida, selecione **Incluir permissões de impressão colorida para computadores host**.
b. Clique em **Adicionar** e, em seguida, insira o nome do computador host.
c. Para permitir que o computador host faça impressão colorida, selecione **Permitir impressão colorida**.
d. Para permitir que os usuários que se conectam ao computador host façam impressões coloridas, selecione **Substituir permissão do usuário**.
e. Clique em **Salvar e adicionar** ou em **Salvar**.

Configurar permissões de impressão colorida para usuários

a. No menu Exibir, selecione **Usuários** e, em seguida, selecione **Incluir permissões de impressão colorida para usuários**.
b. Toque em **Adicionar** e digite o nome do usuário.
c. Selecione **Permitir impressão colorida**.
d. Clique em **Salvar e adicionar** ou em **Salvar**.

Criando um pacote de aplicativos

1. Exporte a exibição Lista de impressoras do MVE usando o recurso Exportar dados.
   a. Na pasta Impressoras menu, clique em **Exibições**.
   b. Selecione **Lista de impressoras** e clique em **Exportar dados**.
   c. Selecione uma pesquisa salva.
   d. No menu "Selecione um tipo de arquivo para exportação de dados", selecione **CSV**.
   e. Clique em **Exportar dados**.
2. Acessar o Criador de pacote.

   Nota: Se for necessário acessar o Criador de pacote, entre em contato com o representante da Lexmark.

   a. Efetue login no Criador de pacote em **cdp.lexmark.com/package-builder**.
   b. Importe a lista de impressoras e clique em **Próximo**.
   c. Digite a descrição do pacote e então digite seu endereço de e-mail.
   d. No Produto selecione os aplicativos e, se necessário, adicione licenças.
   e. Clique em **Avançar** > **Concluir**. O link para download do pacote é enviado para o seu e-mail.
3. Baixe o pacote.

Notas:

- O MVE não é compatível com a implantação de aplicativos com licenças de teste. É possível implantar somente aplicativos gratuitos ou que tenham licenças de produção. Se precisar de códigos de ativação, entre em contato com seu representante Lexmark.
- Para adicionar os aplicativos a uma configuração, importe o pacote de aplicativos para a biblioteca de recursos. Para obter mais informações, consulte " Importação de arquivos para a biblioteca de recursos" na página 75.

Importando ou exportando uma configuração

Antes de começar a importar um arquivo de configuração, verifique se ele será exportado de um MVE com a mesma versão.

1. No menu Configurações, clique em **Todas as configurações**.
2. Execute uma das seguintes opções:
   - Para importar um arquivo de configuração, clique em **Importar**, vá até o arquivo de configuração e clique em **Importar**.
   - Para exportar um arquivo de configuração, selecione uma configuração e clique em **Exportar**.

   Notas:

   – Ao exportar uma configuração, as senhas são excluídas. Após a importação, adicione manualmente as senhas.
   – UCF, pacotes de configuração e arquivos de aplicativos não fazem parte de uma configuração exportada.

Importação de arquivos para a biblioteca de recursos

A biblioteca de recursos é uma coleção de arquivos de firmware, certificados CA e pacotes de aplicativos importados para o MVE. Esses arquivos podem ser associados a uma ou mais configurações.

1. No menu Configurações, clique em **Biblioteca de recursos**.
2. Clique em **Importar** > **Escolher arquivo** e, em seguida, localize o arquivo.

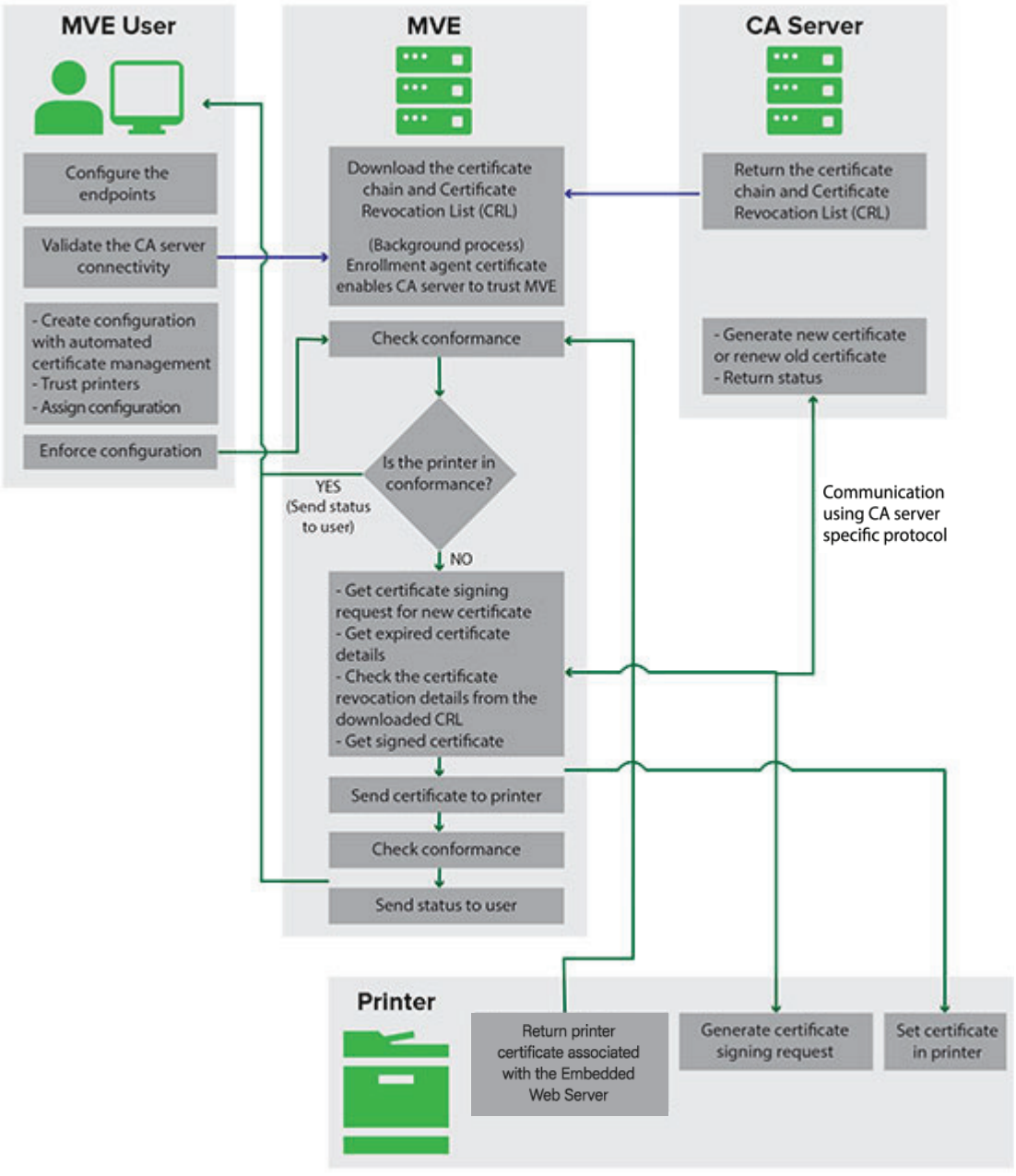
   Nota: Somente arquivos de firmware/aplicativos (.fls), pacotes de aplicativos ou conjuntos de configurações (.zip), certificados CA (.pem) e arquivos de configuração universal (.ucf) podem ser importados.
3. Clique em **Importar recurso**.

Gerenciamento de certificados

Configuração do MVE para o gerenciamento automático de certificados

Noções básicas sobre o recurso de gerenciamento automatizado de certificados

Você pode configurar o MVE para gerenciar certificados de impressora automaticamente e, em seguida, instalá-los nas impressoras por meio da aplicação de configuração. O diagrama a seguir descreve o processo, ponto a ponto, do recurso de gerenciamento automatizado de certificados.



Os endpoints de autoridade de certificado, como o servidor CA e o endereço do servidor, devem ser definidos no MVE.

Os seguintes servidores CA são suportados:

- **OpenXPKI CA** — Os usuários podem usar um dos seguintes protocolos:
  - Simple Certificate Encryption Protocol (SCEP)
  - Conector EST

  Notas:

  - EST é a maneira recomendada de se conectar ao servidor OpenXPKI.
  - Para obter mais informações sobre como configurar o OpenXPKI CA usando o protocolo EST, consulte " Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo EST" na página 117
  - Para obter mais informações sobre como configurar o OpenXPKI CA usando o protocolo SCEP, consulte " Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo SCEP" na página 99
- **CA corporativa da Microsoft** — Os usuários podem usar um dos seguintes protocolos
  - Simple Certificate Encryption Protocol (SCEP)
  - Serviço da Web de registro de certificado da Microsoft (MSCEWS)

  Notas:

  - O MSCEWS é a maneira recomendada de se conectar ao servidor de AC corporativa da Microsoft.
  - Para obter mais informações sobre como configurar o Microsoft CA usando o protocolo MSCEWS, consulte " Gerenciando certificados usando a autoridade de certificações da Microsoft pelo MSCEWS" na página 88
  - Para obter mais informações sobre como configurar o Microsoft CA usando o protocolo SCEP, consulte " Gerenciamento de certificados usando a autoridade de certificações da Microsoft pelo SCEP" na página 81

A conexão entre o MVE e os servidores CA deve ser validada. Durante a validação, o MVE comunica-se com o servidor CA para baixar a cadeia de certificados e a CRL (Certificate Revocation List, lista de revogação de certificados). O certificado do agente de registro ou o certificado de teste também é gerado. Esse certificado permite que o servidor CA confie no MVE.

Para obter mais informações sobre como definir os endpoints e a validação, consulte " Configuração do MVE para gerenciamento automatizado de certificados" na página 78.

Uma configuração definida como **Usar o Markvision para gerenciar certificados de dispositivos** deve ser atribuída e aplicada à impressora.

Para obter mais informações, consulte os tópicos a seguir:

- " Criação de configurações" na página 68
- " Aplicando configurações" na página 62

Durante a aplicação, o MVE verifica a conformidade da impressora.

Para **Certificado padrão do dispositivo**

- O certificado é validado em relação à cadeia de certificados baixada do servidor de AC.
- Se a impressora estiver fora de conformidade, uma solicitação de assinatura de certificado (CSR) será solicitada para a impressora.

Para **Certificado nomeado do dispositivo**

- O certificado é validado em relação à cadeia de certificados baixada do servidor de AC.
- O MVE cria um certificado de dispositivo nomeado autoassinado no dispositivo.
- Se a impressora estiver fora de conformidade, uma solicitação de assinatura de certificado (CSR) será gerada para a impressora.

Notas:

- O MVE se comunica com o servidor de AC usando os protocolos configurados.
- O servidor CA gera o novo certificado e, em seguida, o MVE envia o certificado para a impressora.
- Se existir um certificado nomeado na impressora, um novo certificado nomeado não será criado, mas uma solicitação de assinatura de certificado será gerada para a impressora.

Configuração do MVE para gerenciamento automatizado de certificados

1. Clique em no canto superior direito da página.
2. Clique em **Autoridade de certificações** > **Usar o servidor de autoridade de certificações**.

   Nota: O botão Usar o servidor da autoridade de certificações aparece apenas ao configurar a autoridade de certificações pela primeira vez ou quando o certificado é excluído.
3. Configure os parâmetros do servidor.
   - **Servidor CA**: o servidor CA (autoridade de certificações) que gera os certificados da impressora. Você pode selecionar um dos seguintes:
     - **OpenXPKI CA**
     - **Microsoft CA- Enterprise**

     Nota: O usuário também pode configurar um servidor de AC que suporte o protocolo de **EST (Enrollment over Secure Transport, inscrição sobre transporte seguro)**.

     - O servidor de AC deve implementar o protocolo EST conforme definido na RFC 7030.

       Nota: Qualquer desvio da especificação pode resultar em uma configuração inválida.
     - EST é o protocolo recomendado para se conectar ao servidor de AC OpenXPKI.

       Nota: O servidor Microsoft CA Enterprise não suporta o protocolo EST.
   - **Endereço do servidor CA**: o endereço IP ou o nome do host do seu servidor CA. Este campo é aplicável somente aos protocolos SCEP e EST.

     Nota: Digite qualquer um dos seguintes:

     - Para servidor MSCA (usando SCEP): <Server IP Address or Hostname>/certsrv/mscep/mscep.dll
     - Para servidor OpenXPKI (usando SCEP): <Server IP Address or Hostname>/scep/scep
     - Para EST, digite qualquer um dos seguintes:
       - https://172.87.95.240
       - https://estserver.com
       - estserver.com
   - **Etiqueta do servidor de AC (Opcional)** — se o usuário criar um novo realm, o mesmo nome de realm deverá ser colocado neste campo.
   - **Endereço do servidor de CEP** — este campo é aplicável somente ao protocolo MSCEWS.

Nota: Digite qualquer um dos seguintes:

- Para Autenticação de nome de usuário e senha: https://democep.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP
- Para Autenticação integrada do Windows: https://democep.com/ADPolicyProvider_CEP_Kerberos/service.svc/CEP
- Para Autenticação do certificado do cliente: https://democep.com/ADPolicyProvider_CEP_Certificate/service.svc/CEP

- **Nome do host do servidor de AC**— o nome do host do servidor de AC.

  Nota: Por exemplo, para o protocolo MSCEWS, o usuário pode selecionar **`democa.lexmark.com`**

- **Nome do host do servidor de CES**— o nome do host do servidor de CES.

  Nota: Por exemplo, para o protocolo MSCEWS, o usuário pode selecionar **`democes.lexmark.com`**

- **Senha de desafio** — A senha necessária para validar a identidade do MVE no servidor de AC. Essa senha é necessária somente para a AC do OpenXPKI. Ela não é suportada na AC corporativa da Microsoft.

Nota: Dependendo do seu servidor de AC, você deve configurar o modo de autenticação do servidor. Execute um dos seguintes procedimentos:

- Se você selecionar o protocolo **EST**, no menu **Modo de autenticação do servidor de AC**, selecione qualquer um dos seguintes:
  - **Autenticação de nome de usuário e senha**
  - **Autenticação do certificado do cliente**
- Se você selecionar o protocolo **MSCEWS**, no menu **Modo de autenticação do servidor de AC**, selecione qualquer um dos seguintes:
  - **Autenticação de nome de usuário e senha**
  - **Autenticação do certificado do cliente**
  - **Autenticação integrada do Windows**
- O protocolo **SCEP** suporta apenas o modo de autenticação **Senha de desafio**.

Nota: Dependendo do servidor de AC, consulte qualquer uma das seções:

- " Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo SCEP" na página 99
- " Gerenciamento de certificados usando a autoridade de certificações da Microsoft pelo SCEP" na página 81
- " Gerenciando certificados usando a autoridade de certificações da Microsoft pelo MSCEWS" na página 88
- " Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo EST" na página 117

4 Clique em **Salvar alterações e validar** > **OK**.

Notas:

- A opção **Descartar alterações** só funciona se as alterações ainda não foram salvas ou salvas e validadas.
- O usuário não pode recuperar dados de uma configuração inválida, pois o MVE não armazena o último estado válido de nenhuma configuração. O MVE armazena apenas uma única configuração de certificado por vez, que pode ou não ser válida.

Notas:

- A conexão entre o MVE e os servidores CA deve ser validada. Durante a validação, o MVE comunica-se com o servidor CA para baixar a cadeia de certificados e a CRL (Certificate Revocation List, lista de revogação de certificados). O certificado do agente de registro ou o certificado de teste também é gerado. Esse certificado permite que o servidor CA confie no MVE.
- Você pode selecionar um ou vários modelos CEP ao usar o protocolo MSCEWS. Faça o seguinte:

a Após clicar em **Salvar alterações e validar**, a janela Seleção de modelo CEP é exibida.

b Selecione um ou mais dos modelos disponíveis.

- A caixa de diálogo usar servidor da autoridade de certificação busca a lista de revogação de certificados.
- Uma caixa de diálogo confirma que a validação do certificado foi bem-sucedida.

c Você pode ver os modelos CEP selecionados na página de configuração do servidor de AC.

Nota: Quando você aplica essa configuração a qualquer dispositivo, um certificado é criado de acordo com o modelo selecionado.

5 Navegue de volta para a página Configuração do sistema e depois analise o certificado CA.

Nota: É possível também fazer download ou excluir um certificado CA.

Configuração do Microsoft Enterprise CA com NDES

Visão geral

No cenário de implantação a seguir, todas as permissões são baseadas em permissões definidas nos modelos de certificado publicados no controlador de domínio. As solicitações de certificado enviadas à CA são baseadas em modelos de certificados.

Para essa configuração, verifique se você tem o seguinte:

- Uma máquina que hospeda a AC subordinada
- Uma máquina que hospeda o serviço NDES
- Um controlador de domínio

Usuários necessários

Crie os seguintes usuários no controlador de domínio:

- Administrador do serviço
  - Nomeado como **SCEPAdmin**
  - Deve ser membro dos grupos **local admin** e **Enterprise Admin**
  - Deve ser registrado localmente quando a instalação da função NDES for acionada
  - Tem **Permissão de registro** para os modelos de certificado
  - Tem **Permissão para adicionar modelo** na CA
- Conta de serviço
  - Nomeado como **SCEPSvc**
  - Deve ser membro do grupo local **IIS_IUSRS**
  - Deve ser um usuário do domínio e ter permissões de **leitura** e **registro** nos modelos configurados
  - Tem permissão de **solicitação** na CA

- Administrador da AC corporativa
  - Nomeado como **CAAdmin**
  - Membro do grupo **Enterprise Admin**
  - Deve fazer parte do grupo **local admin**

Gerenciamento de certificados usando a autoridade de certificações da Microsoft pelo SCEP

Esta seção fornece instruções sobre o seguinte:

- Configuração da CA (Certificate Authority, autoridade de certificações) do Microsoft Enterprise usando o NDES (Network Device Enrollment Service, serviço de registro de dispositivo de rede) da Microsoft
- Criar um servidor CA raiz

Nota: O sistema operacional Windows Server 2016 é usado para todas as configurações deste documento.

Visão geral

O servidor CA raiz é o servidor CA principal em qualquer organização, e é o topo da infraestrutura PKI. A CA raiz autentica o servidor CA subordinado. Esse servidor geralmente é mantido em modo off-line para evitar qualquer invasão e proteger a chave privada.

Para configurar o servidor CA raiz, proceda da seguinte forma:

1. Certifique-se de que o servidor CA raiz esteja instalado. Para mais informações, consulte " Instalação do servidor CA raiz" na página 81.
2. Defina as configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade. Para mais informações, consulte " Definição das configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade" na página 84.
3. Configurar a acessibilidade de CRL. Para mais informações, consulte " Configuração da acessibilidade da CRL" na página 85.

Instalação do servidor CA raiz

1. No Gerenciador de servidores, clique em **Gerenciar > Adicionar funções e recursos**.
2. Clique em **Funções do servidor**, selecione **Serviços de certificados do Active Directory** e todos os seus recursos e clique em **Avançar**.
3. Na seção Serviços de função AD CS, selecione **Autoridade de certificação** e clique em **Avançar > Instalar**.
4. Após a instalação, clique em **Configurar serviços de certificados do Active Directory no servidor de destino**.
5. Na seção Serviços de função, selecione **Autoridade de certificação > Avançar**.
6. Na seção Tipo de configuração, selecione **CA independente** e clique em **Avançar**.
7. Na seção Tipo de CA, selecione **CA raiz** e clique em **Avançar**.
8. Clique em **Criar nova chave privada** e clique em **Avançar**.

9 No menu Selecione um provedor de serviços de criptografia, selecione **Provedor de armazenamento de chave de software RSA#Microsoft**.

10 No menu Comprimento da chave, selecione **4096**.

11 Na lista de algoritmos de hash, selecione **SHA512** e clique em **Avançar**.

12 No campo Nome comum para esta CA, digite o nome do servidor host.

13 No campo Sufixo de nome diferenciado, digite o componente de domínio.

Configuração do nome da CA de amostra

Nome de domínio totalmente qualificado (FQDN) da máquina: **`test.dev.lexmark.com`**

Nome comum (CN): **`TESTE`**

Sufixo de nome diferenciado: **`DC=DEV,DC=LEXMARK,DC=COM`**

14 Clique em **Avançar**.

15 Especifique o período válido e clique em **Avançar**.

Nota: Geralmente, o período de validade é de 10 anos.

16 Não altere nada na janela de locais do banco de dados.

17 Conclua a instalação.

Configuração do Microsoft Enterprise CA com NDES

Visão geral

No cenário de implantação a seguir, todas as permissões são baseadas em permissões definidas nos modelos de certificado publicados no controlador de domínio. As solicitações de certificado enviadas à CA são baseadas em modelos de certificados.

Para essa configuração, verifique se você tem o seguinte:

- Uma máquina que hospeda a AC subordinada
- Uma máquina que hospeda o serviço NDES
- Um controlador de domínio

Usuários necessários

Crie os seguintes usuários no controlador de domínio:

- Administrador do serviço
  - Nomeado como **SCEPAdmin**
  - Deve ser membro dos grupos **local admin** e **Enterprise Admin**
  - Deve ser registrado localmente quando a instalação da função NDES for acionada
  - Tem **Permissão de registro** para os modelos de certificado
  - Tem **Permissão para adicionar modelo** na CA
- Conta de serviço
  - Nomeado como **SCEPSvc**
  - Deve ser membro do grupo local **IIS_IUSRS**

- Deve ser um usuário do domínio e ter permissões de **leitura** e **registro** nos modelos configurados
- Tem permissão de **solicitação** na CA

Configuração do servidor CA subordinado

Visão geral

O servidor CA subordinado é o servidor CA intermediário e está sempre on-line. Geralmente, ele lida com o gerenciamento de certificados.

Para configurar o servidor CA subordinado, proceda da seguinte forma:

1. Certifique-se de que o servidor CA subordinado está instalado. Para mais informações, consulte " Instalação do servidor CA subordinado" na página 83.
2. Defina as configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade. Para mais informações, consulte " Definição das configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade" na página 84.
3. Configurar a acessibilidade de CRL. Para mais informações, consulte " Configuração da acessibilidade da CRL" na página 85.

Instalação do servidor CA subordinado

1. No servidor, faça login como um usuário do domínio **CAAdmin**.
2. No Gerenciador de servidores, clique em **Gerenciar** > **Adicionar funções e recursos**.
3. Clique em **Funções do servidor**, selecione **Serviços de certificados do Active Directory** e todos os seus recursos e clique em **Avançar**.
4. Na seção Serviços de função AD CS, selecione **Autoridade de certificação** e **Registro de autoridade de certificações na Web** e clique em **Avançar**.

   Nota: Verifique se todos os recursos de Registro de autoridade de certificações na Web foram adicionados.
5. Na seção Serviços de função do Servidor Web (IIS), mantenha as configurações padrão.
6. Após a instalação, clique em **Configurar serviços de certificados do Active Directory no servidor de destino**.
7. Na seção Serviços de função, selecione **Autoridade de certificação** e **Registro de autoridade de certificações na Web** e clique em **Avançar**.
8. Na seção Tipo de configuração, selecione **Enterprise CA** e clique em **Avançar**.
9. Na seção Tipo de CA, selecione **CA subordinada** e clique em **Avançar**.
10. Clique em **Criar nova chave privada** e clique em **Avançar**.
11. No menu Selecione um provedor de serviços de criptografia, selecione **Provedor de armazenamento de chave de software RSA#Microsoft**.
12. No menu Comprimento da chave, selecione **4096**.
13. Na lista de algoritmos de hash, selecione **SHA512** e clique em **Avançar**.

14 No campo Nome comum para esta CA, digite o nome do servidor host.

15 No campo Sufixo de nome diferenciado, digite o componente de domínio.

Configuração do nome da CA de amostra

Nome de domínio totalmente qualificado (FQDN) da máquina: **`test.dev.lexmark.com`**

Nome comum (CN): **`TESTE`**

Sufixo de nome diferenciado: **`DC=DEV,DC=LEXMARK,DC=COM`**

16 Na caixa de diálogo Solicitação de certificado, salve o arquivo de solicitação e clique em **Avançar**.

17 Não altere nada na janela de locais do banco de dados.

18 Conclua a instalação.

19 Assine a solicitação da CA raiz e exporte o certificado assinado no formato PKCS7.

20 Na CA subordinada, abra **Autoridade de certificação**.

21 No painel esquerdo, clique com o botão direito na CA e clique em **Todas as tarefas > Instalar certificado CA**.

22 Selecione o certificado assinado e inicie o serviço da CA.

Definição das configurações de Ponto de distribuição de certificação e de Acesso a informações de autoridade

Nota: Defina as configurações do CDP (Certification Distribution Point, ponto de distribuição de certificação) e do AIA (Authority Information Access, acesso às informações da autoridade) para a CRL (Certificate Revocation List, lista de revogação de certificados).

1 No Gerenciador de servidores, clique em **Ferramentas > Autoridade de certificação**.

2 No painel esquerdo, clique com o botão direito na CA e, em seguida, clique em **Propriedades > Extensões**.

3 No menu Selecionar extensão, selecione **Ponto de distribuição da CRL (Certificate Revocation List, lista de revogação de certificados)**.

4 Na lista de certificados revogados, selecione **C:Windows/system32** e faça o seguinte:

   a Selecione **Publicar CRLs neste local**.

   b Desmarque **Publicar CRLs Delta neste local**.

5 Exclua todas as outras entradas, exceto **C:\Windows\system32**.

6 Clique em **Adicionar**.

7 No campo Local, adicione **`http://`*`serverIP`*`/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl`**, onde ***`serverIP`*** é o endereço IP do servidor.

   Nota: Se seu servidor estiver acessível ao usar o FQDN, use **<ServerDNSName>** em vez do seu endereço IP.

8 Clique em **OK**.

9 Selecione **Incluir na extensão CDP de certificados emitidos** para a entrada criada.

10 No menu Selecionar extensão, selecione **Acesso a informações da autoridade (AIA)**.

11 Exclua todas as outras entradas, exceto **C:\Windows\system32**.

12 Clique em **Adicionar**.

13 No campo Local, adicione **`http://serverIP/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt`**, onde ***`serverIP`*** é o endereço IP do servidor.

Nota: Se seu servidor estiver acessível ao usar o FQDN, use **<ServerDNSName>** em vez do seu endereço IP.

14 Clique em **OK**.

15 Selecione **Incluir na extensão AIA de certificados emitidos** para a entrada criada.

16 Clique em **Aplicar** > **OK**.

Nota: Se necessário, reinicie o serviço de certificação.

17 No painel esquerdo, expanda a CA, clique com o botão direito em **Certificados revogados** e clique em **Propriedades**.

18 Especifique o valor para Intervalo de publicação da CRL e para Publicar intervalo de publicação de CRLs Delta e clique em **Aplicar > OK**.

19 No painel esquerdo, clique com o botão direito em **Certificados revogados**, clique em **Todas as tarefas** e publique a Nova CRL.

Configuração da acessibilidade da CRL

Nota: Antes de começar, verifique se o Gerenciador do IIS (Internet Information Services, serviços de informações da internet) está instalado.

1 No Gerenciador do IIS, expanda a CA e expanda **Sites**.

2 Clique com o botão direito em **Site da Web padrão** e, em seguida, clique em **Adicionar diretório virtual**.

3 No campo Alias, digite **`CertEnroll`**.

4 No campo Caminho físico, digite **`C:\Windows\System32\CertSrv\CertEnroll`**.

5 Clique em **OK**.

6 Clique com o botão direito em **CertEnroll** e depois em **Editar permissões**.

7 Na guia Segurança, remova qualquer acesso de gravação, exceto para o sistema.

8 Clique em **OK**.

Configuração do servidor do NDES

1 No servidor, faça login como um usuário do domínio **SCEPAdmin**.

2 No Gerenciador de servidores, clique em **Gerenciar** > **Adicionar funções e recursos**.

3 Clique em **Funções do servidor**, selecione **Serviços de certificados do Active Directory** e todos os seus recursos e clique em **Avançar**.

4 Na seção Serviços de função AD CS, desmarque **Autoridade de certificação**.

5. Selecione **Serviço de registro de dispositivo de rede** e todos os seus recursos e clique em **Avançar**.
6. Na seção Serviços de função do Servidor Web (IIS), mantenha as configurações padrão.
7. Após a instalação, clique em **Configurar serviços de certificados do Active Directory no servidor de destino**.
8. Na seção Serviços de função, selecione **Serviço de registro de dispositivo de rede** e clique em **Avançar**.
9. Selecione a conta de serviço **SCEPSvc**.
10. Na seção CA para NDES, selecione **Nome da CA** ou **Nome do computador** e clique em **Avançar**.
11. Na seção Informações da AR, especifique as informações e clique em **Avançar**.
12. Na seção Criptografia para NDES, faça o seguinte:
    - Selecione os provedores de assinatura e de chave de criptografia apropriados.
    - No menu Comprimento da chave, selecione o mesmo comprimento de chave que o servidor CA.
13. Clique em **Avançar**.
14. Conclua a instalação.

Agora você pode acessar o servidor NDES por um navegador da Web como um usuário SCEPSvc. No servidor NDES, você pode exibir a impressão digital do certificado CA, a senha de desafio de registro e o período de validade da senha de desafio.

Acesso ao servidor NDES

Abra um navegador da Web e digite **`http://NDESserverIP/certsrv/mscep_admin`**, onde ***`NDESserverIP`*** é o endereço IP do servidor NDES.

Configuração do NDES para MVE

Nota: Antes de começar, verifique se o servidor NDES está funcionando corretamente.

Criação de modelos de certificado

1. Na CA subordinada (certserv), abra **Autoridade de certificação**.
2. No painel esquerdo, expanda a CA, clique com o botão direito em **Modelos de certificados** e clique em **Gerenciar**.
3. No Console de modelos de certificado, crie uma cópia do **Servidor Web**.
4. Na guia Geral, digite **`MVEWebServer`** como o nome do modelo.
5. Na guia Segurança, conceda aos usuários **SCEPAdmin** e **SCEPSvc** as permissões apropriadas.

   Nota: Para mais informações, consulte " Usuários necessários" na página 82.
6. Na guia Nome da entidade, selecione **Fornecer na solicitação**.
7. Na CA subordinada (certserv), abra **Autoridade de certificação**.
8. Na guia Extensões, selecione **Políticas de aplicativos** > **Editar**.
9. Clique em **Adicionar** >**Autenticação de cliente** > **OK**.

10 No painel esquerdo, expanda a CA, clique com o botão direito em **Modelos de certificados** e clique em **Novo** > **Modelo de certificado para emitir**.

11 Selecione os certificados criados recentemente e clique em **OK**.

Agora você pode acessar os modelos usando o portal de registro na Web da CA.

Acesso aos modelos

1 Abra um navegador da Web e digite **`http://CAserverIP/certsrv/certrqxt.asp`**, onde ***`CAserverIP`*** é o endereço IP do servidor CA.

2 No menu Modelo de certificado, exiba os modelos.

Configuração de modelos de certificado para NDES

1 No computador, inicie o editor do registro.

2 Navegue até **HKEY_LOCAL_MACHINE >SOFTWARE >Microsoft > Cryptography > MSCEP**.

3 Configure e defina o seguinte como **MVEWebServer**:
- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

4 Conceda ao usuário SCEPSvc permissão total para o MSCEP.

5 No Gerenciador do IIS, expanda a CA e clique em **Pools de aplicativos**.

6 No painel direito, clique em **Reciclar** para reiniciar o pool de aplicativos SCEP.

7 No Gerenciador de IIS, expanda a CA e, em seguida, expanda **Sites** > **Site padrão da Web**.

8 No painel direito, clique em **Reiniciar**.

Desativação da Senha de desafio no servidor Microsoft CA

1 No computador, inicie o editor do registro.

2 Navegue até **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP**.

3 Defina EnforcePassword como **0**.

4 No Gerenciador do IIS, expanda a CA, clique em **Pools de aplicativos** e selecione **SCEP**.

5 No painel direito, clique em **Configurações avançadas**.

6 Defina Carregar perfil de usuário como **Verdadeiro** e clique em **OK**.

7 No painel direito, clique em **Reciclar** para reiniciar o pool de aplicativos SCEP.

8 No Gerenciador de IIS, expanda a CA e, em seguida, expanda **Sites** > **Site padrão da Web**.

9 No painel direito, clique em **Reiniciar**.

Ao abrir o NDES pelo navegador da Web, agora é possível visualizar apenas a impressão digital da CA.

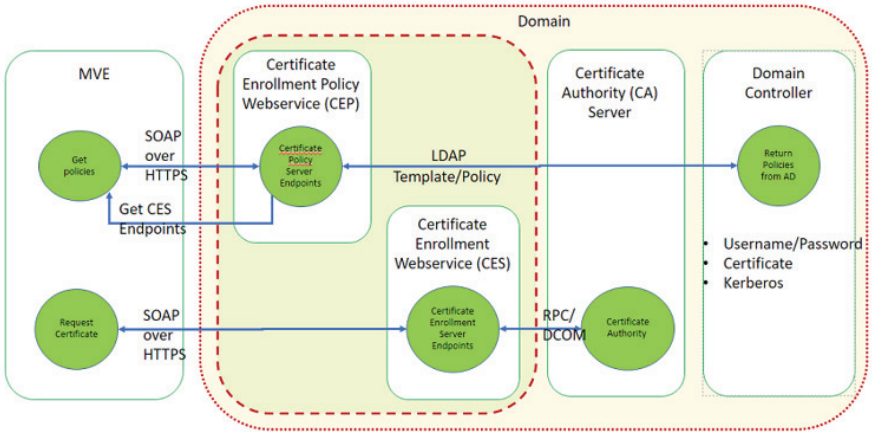
Gerenciando certificados usando a autoridade de certificações da Microsoft pelo MSCEWS

Esta seção fornece informações sobre como configurar o Serviço da Web de política de registro de certificado (CEP) e o Serviço da Web de registro de certificado (CES). Como a Microsoft recomenda instalar o CEP e o CES em duas máquinas diferentes, estamos seguindo a mesma instrução neste documento. Esses serviços da Web serão chamados aqui de servidor de CEP e servidor de CES, respectivamente.

Nota: O usuário deve ter uma autoridade de certificações (CA) Enterprise pré-configurada e um controlador de domínio.

Requisitos de sistema

O sistema operacional a partir do Windows Server 2012 R2 é usado para todas as configurações deste documento. Os requisitos e os recursos de instalação a seguir aplicam-se ao CEP e ao CES, a menos que seja especificado de outra forma.



Crie os seguintes tipos de conta no controlador de domínio:

- Administrador do serviço: nomeado como **CEPAdmin** e **CESAdmin**
  - Esse usuário tem que fazer parte do **grupo local admin** e dos respectivos servidores de CEP e CES.
  - Este usuário deve ser membro do grupo **Enterprise Admin**.
- Conta de serviço: nomeada como **CEPSvc** e **CESSvc**
  - Esse usuário deve fazer parte do grupo **IIS_IUSRS local**.
  - Requer a permissão **Solicitar certificados** na AC para o respectivo **CEPSvc** e **CESSvc**.

Requisitos de conectividade de rede

- Os requisitos de conectividade de rede são uma parte essencial do planejamento da implantação, especialmente para situações em que o CEP e o CES estão hospedados em uma rede de perímetro.
- Toda a conectividade do cliente com ambos os serviços ocorre dentro de uma sessão de HTTPS, de modo que somente o tráfego HTTPS é permitido entre o cliente e os serviços da Web.

- O CEP comunica-se com os Serviços de domínio do Active Directory (AD DS) usando o protocolo LDAP (Lightweight Directory Access Protocol) padrão e as portas LDAP (LDAPS) seguras (TCP 389 e 636 respectivamente).
- O CES comunica-se com a AC usando o DCOM (Distributed Component Object Model).

  Notas:

  - Por padrão, o DCOM usa portas efêmeras aleatórias.
  - A AC pode ser configurada para reservar uma faixa específica de portas para simplificar a configuração do firewall.

Criando certificados SSL para servidores de CEP e CES

CES e CEP devem usar SSL (Secure Sockets Layer) para comunicação com clientes (usando HTTPS). Todos os serviços precisam ter um certificado válido que tenha uma política de uso avançado de chave (EKU) de autenticação de servidor no armazenamento de certificados do computador local.

1. Instale o serviço IIS no servidor.
2. Faça login no servidor de CEP e adicione o Certificado CA raiz no repositório da Autoridade de certificações raiz confiável.
3. Inicie o Console de Gerenciamento do IIS e, em seguida, selecione **Página inicial do servidor**.
4. Na seção Exibição principal, abra **Certificados de servidor**.
5. Clique em **Ações** > **Criar solicitação de certificado**.
6. Na janela Propriedades de nome diferenciado, forneça as informações necessárias e, em seguida, clique em **Avançar**.
7. Na caixa de diálogo Propriedades do provedor de serviços criptográficos, selecione o tamanho do bit e clique em **Avançar**.
8. Salve o arquivo.
9. Obtenha o arquivo assinado pela AC que você pretende usar para CEP e CES.

   Nota: Verifique se o EKU de autenticação de servidor está ativado no certificado assinado.
10. Copie o arquivo assinado de volta para o servidor de CEP.
11. No Console de gerenciamento do IIS, selecione **Página inicial do servidor**.
12. Na seção Exibição principal, abra **Certificados de Servidor**.
13. Clique em **Ações** > **Concluir solicitação de certificado**.
14. Na janela Especificar resposta da autoridade de certificações, selecione o arquivo assinado.
15. Digite um nome e, em seguida, no menu Repositório de certificados, selecione **Pessoal**.
16. Conclua a instalação do certificado.
17. Em Console de gerenciamento do IIS, selecione o website padrão.
18. Clique em **Ações** > **Vínculos**.
19. Na caixa de diálogo Vínculos de site, clique em **Adicionar**.

20 Na caixa de diálogo Adicionar vínculo de site, defina o Tipo como **https** e, em seguida, no certificado SSL, pesquise o certificado recém-criado.

21 No Console de gerenciamento do IIS, selecione **Default Web Site** e abra as configurações de SSL.

22 Ative Exigir SSL e defina Certificados de cliente como **Ignorar**.

23 Reinicie o IIS.

Nota: Siga o mesmo procedimento para o servidor de CES.

Criando modelos de certificado

O usuário deve criar um modelo de certificado para o registro do certificado. Faça o seguinte para copiar de um modelo de certificado existente:

1 Faça login na AC corporativa com as credenciais de administrador da AC.

2 Expanda a AC, clique com o botão direito do mouse em **Modelo de certificados** e, em seguida, clique em **Gerenciar**.

3 Em Console de modelos de certificado, clique com o botão direito do mouse em **Modelo de certificado do servidor da Web** e, em seguida, clique em **Duplicar modelo**.

4 Na guia Geral do modelo, atribua o nome **MVEWebServer** ao modelo.

5 Na guia Segurança, atribua as permissões de **Leitura**, **Gravação** e **Registro** ao administrador de AC.

6 Conceda as permissões de **Leitura** e **Registro** para os usuários autenticados.

7 Na guia Nome da entidade, selecione **Suprimento** na solicitação.

8 Na guia Geral, defina o período de validade do certificado.

9 Se você pretende usar esse modelo de certificado para emitir um **Certificado 802.1X** para impressoras, execute as seguintes ações:

   a Na guia **Extensões**, selecione **Políticas de aplicativo** na lista de extensões incluídas nesse modelo.

   b Clique em **Editar** > **Adicionar**.

   c Na caixa de diálogo Adicionar política de aplicativo, selecione **Autenticação do cliente**.

   d Clique em **OK**.

10 Na caixa de diálogo Propriedades do modelo de certificado, clique em **OK**.

11 Na janela da AC, clique com o botão direito do mouse em **Modelos de certificado** e clique em **Novo** > **Modelo de certificado**.

12 Selecione **MVEWebServer** e, em seguida, clique em **OK**.

Noções básicas sobre métodos de autenticação

O CEP e o CES são compatíveis com os seguintes métodos de autenticação:

- A autenticação integrada do Windows, também conhecida como **Autenticação Kerberos**
- A autenticação do certificado do cliente, também conhecida como **Autenticação do certificado X.509**
- **Autenticação de nome de usuário e senha**

autenticação integrada do Windows

A autenticação integrada do Windows usa Kerberos para fornecer um fluxo de autenticação ininterrupto para dispositivos conectados à rede interna. Esse método é preferido para implantações internas porque usa a infraestrutura Kerberos existente no AD DS. Também requer alterações mínimas nos computadores de clientes com certificado.

Nota: Use esse método de autenticação se deseja que os clientes acessem *apenas* o serviço da Web enquanto estiverem conectados diretamente à sua rede interna.

autenticação do Certificado do cliente

Esse método é o preferido em relação à autenticação de nome de usuário e senha, pois é o mais seguro. Ele não requer uma conexão direta com a rede corporativa.

Notas:

- Use esse método de autenticação se você planeja fornecer aos clientes os certificados X.509 digitais para autenticação.
- Esse método ativa os serviços da Web disponíveis na Internet.

Autenticação de nome de usuário e senha

O método de nome de usuário e senha é a forma mais simples de autenticação. Esse método é normalmente usado para atender a clientes que não estão diretamente conectados à rede interna. É uma opção de autenticação menos segura do que a autenticação de certificado do cliente, mas não requer a concessão de um certificado.

Nota: Use esse método de autenticação quando puder acessar o serviço da Web na rede interna ou pela Internet.

Requisitos de delegação

A delegação permite que um serviço represente uma conta de usuário ou de computador para acessar recursos em toda a rede.

A delegação é necessária para o servidor de CES em todas situações a seguir:

- A AC e o CES não residem no mesmo computador.
- O CES pode processar solicitações de registro iniciais, em vez de processar apenas solicitações de renovação de certificado.
- O tipo de autenticação é definido como **Autenticação Integrada do Windows** ou **Autenticação de certificado do cliente**.

A delegação é necessária para o servidor de CES nas situações a seguir:

- A AC e o CES residem no mesmo computador.
- O nome de usuário e a senha são o método de autenticação.

Notas:

- A Microsoft recomenda executar o CEP e o CES como contas de usuários do domínio.
- Os usuários precisam criar um nome principal do serviço (SPN) apropriado antes de configurar a delegação na conta de usuário do domínio.

Ativando a delegação

1. Para criar um SPN para uma conta de usuário de domínio, use o comando **setspn** conforme a seguir:

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

   Notas:

   - O nome da conta é CESSvc.
   - O CES está sendo executado em um computador com um nome de domínio totalmente qualificado (FQDN) do **ces.msca.com** no domínio msca.com.

2. Abra a conta de usuário do domínio CESSvc no controlador de domínio.
3. Na guia Delegação, selecione **Confiar neste usuário para delegação apenas aos serviços especificados**.
4. Selecione a delegação apropriada com base no método de autenticação.

   Notas:

   - Se você selecionar a autenticação integrada do Windows, configure a delegação para usar **apenas Kerberos**.
   - Se o serviço está usando autenticação do certificado do cliente, configure a delegação para usar qualquer protocolo de autenticação.
   - Se você pretende configurar vários métodos de autenticação, configure a delegação para usar qualquer protocolo de autenticação.

5. Clique em **Adicionar**.
6. Na caixa de diálogo Adicionar serviços, selecione **Usuários** ou **Computadores**.
7. Digite o nome do host do servidor de AC e, em seguida, clique em **Verificar nomes**.
8. Na caixa de diálogo Adicionar serviços, selecione um dos seguintes serviços para delegar:
   - Serviço de host (HOST) para esse servidor de AC
   - Serviço do sistema da chamada de procedimento remoto (RPC) para esse servidor de AC
9. Feche a caixa de diálogo de propriedades do usuário do domínio.

Para usuários do domínio CEP que usam autenticação integrada do Windows, faça o seguinte:

1. Para criar um SPN para uma conta de usuário de domínio, use o comando **setspn** conforme a seguir:

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

   Nota: O nome da conta é CEPSvc.

2. Abra a conta de usuário do domínio CEPSvc no controlador de domínio.
3. Na guia Delegação, selecione **Não confiar neste usuário para delegação**.

Configuração da autenticação integrada do Windows

Para instalar o CEP e o CES, use o Windows PowerShell.

Configurando o CEP

O cmdlet **Install-AdcsEnrollmentPolicyWebService** configura o Serviço da Web de política de registro de certificado (CEP). Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1. Faça login no servidor de CEP com o nome de usuário CEPAdmin e, em seguida, inicie o PowerShell no modo administrativo.
2. Execute o comando **`Import-Module ServerManager`**.
3. Execute o comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.
4. Execute o comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Kerberos -SSLCertThumbprint "sslCertThumbPrint"`**.

   Nota: Substitua <*sslCertThumbPrint*> pela impressão digital do certificado SSL criado para o servidor de CEP, após excluir os espaços entre os valores de impressão digital.
5. Para concluir a instalação, selecione **Y** ou **A**.
6. Inicie o Console de gerenciamento do IIS.
7. No painel Conexões, expanda o servidor da Web que está hospedando o CEP.
8. Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual adequado da instalação **ADPolicyProvider_CEP_Kerberos**.
9. No aplicativo virtual chamado **Home**, faça clique duplo nas configurações do aplicativo e em **FriendlyName**.
10. Digite o nome em Valor e feche a caixa de diálogo.
11. Faça clique duplo em **URI** e, em seguida, copie o **Valor**.

    Notas:

    - Se desejar configurar outro método de autenticação no mesmo servidor de CEP, você deverá alterar o ID.
    - Essa URL é usada no MVE ou em qualquer aplicativo cliente.
12. No painel esquerdo, clique em **Pools de aplicativos**.
13. Selecione **WSEnrollmentPolicyServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas** .
14. Em Modelo de processo, selecione o campo Identidade.
15. Na caixa de diálogo Identidade do pool de aplicativos, selecione a conta personalizada e, em seguida, digite **`CEPSvc`** como nome de usuário do domínio.
16. Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.
17. No PowerShell, digite **`iisreset`** para reiniciar o IIS.

Configuração do CES

O cmdlet **Install-AdcsEnrollmentWebService** configura o Serviço da Web de registro de certificado (CES). Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1. Faça login no servidor de CES com o nome de usuário **`CESAdmin`** e, em seguida, inicie o PowerShell no modo administrativo.
2. Execute o comando **`Import-Module ServerManager`**.
3. Execute o comando **`Add-WindowsFeature Adcs-Enroll-Web-Svc`**.
4. Execute o comando **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Kerberos`**.

   Notas:

   - Substitua *<sslCertThumbPrint>* pela impressão digital do certificado SSL criado para o servidor de CES, após excluir os espaços entre os valores de impressão digital.
   - Substitua **`CA1.contoso.com`** pelo nome do computador da AC.
   - Substitua **`contoso-CA1-CA`** pelo nome comum da AC.
5. Para concluir a instalação, selecione **Y** ou **A**.
6. Inicie o Console de gerenciamento do IIS.
7. No painel Conexões, expanda o servidor da Web que está hospedando o CES.
8. Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual adequado da instalação: **contoso-CA1-CA _CES_Kerberos**.
9. No painel esquerdo, clique em **Pools de aplicativos**.
10. Selecione **WSEnrollmentServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas**.
11. Em Modelo de processo, selecione o campo Identidade.
12. Na caixa de diálogo **`Identidade do pool de aplicativos`**, selecione a conta personalizada e, em seguida, digite **`CESSvc`** como nome de usuário do domínio.
13. Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.
14. No PowerShell, digite **`iisreset`** para reiniciar o IIS.
15. Para os usuários do domínio CESSvc, ative a delegação. Para obter mais informações, consulte " Ativando a delegação" na página 92.

Configuração da autenticação do certificado do cliente

Configurando o CEP

O cmdlet **Install-AdcsEnrollmentPolicyWebService** configura o CEP. Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1. Faça login no servidor de CEP com o nome de usuário CEPAdmin e, em seguida, inicie o PowerShell no modo administrativo.
2. Execute o comando **`Import-Module ServerManager`**.
3. Execute o comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.
4. Execute o comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Certificate -SSLCertThumbprint "sslCertThumbPrint"`**.

   Nota: Substitua <*sslCertThumbPrint*> pela impressão digital do certificado SSL criado para o servidor de CEP, após excluir os espaços entre os valores de impressão digital.
5. Para concluir a instalação, selecione **Y** ou **A**.
6. Inicie o Console de gerenciamento do IIS.
7. No painel Conexões, expanda o servidor da Web que está hospedando o CEP.
8. Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual da instalação adequado **ADPolicyProvider_CEP_Certificate**.
9. No aplicativo virtual chamado **Home**, faça clique duplo nas configurações do aplicativo e em **FriendlyName**.
10. Digite o nome em Valor e feche a caixa de diálogo.
11. Faça clique duplo em **URI** e, em seguida, copie o **Valor**.

    Notas:

    - Se desejar configurar outro método de autenticação no mesmo servidor de CEP, você deverá alterar o ID.
    - Essa URL é usada no MVE ou em qualquer aplicativo cliente.
12. No painel esquerdo, clique em **Pools de aplicativos**.
13. Selecione **WSEnrollmentPolicyServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas**.
14. Em Modelo de processo, selecione o campo Identidade.
15. Na caixa de diálogo Identidade do pool de aplicativos, selecione a conta personalizada e, em seguida, digite **`CEPSvc`** como nome de usuário do domínio.
16. Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.
17. No PowerShell, digite **`iisreset`** para reiniciar o IIS.

Configuração do CES

O cmdlet **Install-AdcsEnrollmentWebService** configura o Serviço da Web de registro de certificado (CES). Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1. Faça login no servidor de CES com o nome de usuário **CESAdmin** e, em seguida, inicie o PowerShell no modo administrativo.
2. Execute o comando **Import-Module ServerManager**.
3. Execute o comando **Add-WindowsFeature Adcs-Enroll-Web-Svc**.
4. Execute o comando **Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Certificate**.

   Notas:

   - Substitua <*sslCertThumbPrint*> pela impressão digital do certificado SSL criado para o servidor de CES, após excluir os espaços entre os valores de impressão digital.
   - Substitua **CA1.contoso.com** pelo nome do computador da AC.
   - Substitua **contoso-CA1-CA** pelo nome comum da AC.
   - Se você já configurou um método de autenticação no host, remova **ApplicationPoolIdentity** do comando.
5. Para concluir a instalação, selecione **Y** ou **A**.
6. Inicie o Console de gerenciamento do IIS.
7. No painel Conexões, expanda o servidor da Web que está hospedando o CEP.
8. Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual adequado da instalação: **contoso-CA1-CA _CES_Certificate**.
9. No painel esquerdo, clique em **Pools de aplicativos**.
10. Selecione **WSEnrollmentServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas**.
11. Em Modelo de processo, selecione o campo Identidade.
12. Na caixa de diálogo Identidade do pool de aplicativos, selecione a conta personalizada e, em seguida, digite **CESSvc** como nome de usuário do domínio.
13. Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.
14. No PowerShell, digite **iisreset** para reiniciar o IIS.
15. Para o usuário do domínio CESSvc, ative a delegação. Para obter mais informações, consulte " Ativando a delegação" na página 92.

Criação de um certificado do cliente

1. Em qualquer conta de usuário de domínio, abra **certlm.msc**.
2. Clique em **Certificados** > **Pessoal** > **Certificados** > **Todas as tarefas** > **Solicitar novo certificado**.
3. Clique em **Avançar**.
4. Clique em **Registro do Active Directory** > **Acesso do cliente**.

Nota: Se não quiser usar as opções do **Registro do Active Directory**:

a Clique em **Configurado por você** > **Adicionar novo**.

b Digite o URI do servidor da política de registro como endereço do servidor CEP para nome de usuário_senha ou Autenticação Kerberos.

c Selecione tipo de autenticação como **Integrada ao Windows**.

d Clique em **Validar servidor**.

e Após a validação bem-sucedida, clique em **Adicionar**.

f Clique em **Avançar**.

g Selecione qualquer modelo.

5 Clique em **Detalhes** > **Propriedades**.

6 Clique em **Registrar**.

7 Na guia Assunto, forneça um nome de domínio totalmente qualificado (FQDN).

8 Na guia Chave privada, selecione **Tornar chave privada exportável**.

9 Clique em **Aplicar** > **Registro**.

Depois de registrar o certificado do cliente, faça o seguinte para exportar o certificado do cliente no formato PFX:

1 Clique em **Certificado** > **Todas as tarefas** > **Exportar**.

2 Clique em **Avançar** > **Sim, exportar a chave privada**.

3 Clique em **Avançar**.

4 Digite a senha fornecida pelo cliente.

5 Clique em **Avançar**.

6 Especifique o nome do arquivo na caixa de diálogo Exportação de certificado.

7 Clique em **Avançar** > **Concluir**.

Configuração da autenticação de nome de usuário e senha

Configurando o CEP

O cmdlet **Install-AdcsEnrollmentPolicyWebService** configura o Serviço da Web de política de registro de certificado (CEP). Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1 Faça login no servidor de CEP com o nome de usuário CEPAdmin e, em seguida, inicie o PowerShell no modo administrativo.

2 Execute o comando **`Import-Module ServerManager`**.

3 Execute o comando **`Add-WindowsFeature Adcs-Enroll-Web-Pol`**.

4 Execute o comando **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType UserName -SSLCertThumbprint "sslCertThumbPrint"`**.

Nota: Substitua *<sslCertThumbPrint>* pela impressão digital do certificado SSL criado para o servidor de CEP, após excluir os espaços entre os valores de impressão digital.

5 Para concluir a instalação, selecione **Y** ou **A**.

6 Inicie o Console de gerenciamento do IIS.

7 No painel Conexões, expanda o servidor da Web que está hospedando o CEP.

8 Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual adequado da instalação: **ADPolicyProvider_CEP_UsernamePassword**.

9 No aplicativo virtual chamado **Home**, faça clique duplo nas configurações do aplicativo e em **FriendlyName**.

10 Digite o nome em **Valor** e feche a caixa de diálogo.

11 Faça clique duplo em **URI** e, em seguida, copie o **Valor**.

Notas:

- Se desejar configurar outro método de autenticação no mesmo servidor de CEP, você deverá alterar o ID.
- Essa URL é usada no MVE ou em qualquer aplicativo cliente.

12 No painel esquerdo, clique em **Pools de aplicativos**.

13 Selecione **WSEnrollmentPolicyServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas**.

14 Em Modelo de processo, selecione o campo Identidade.

15 Na caixa de diálogo Identidade do pool de aplicativos, selecione a conta personalizada e, em seguida, digite **`CEPSvc`**.

16 Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.

17 No PowerShell, digite **`iisreset`** para reiniciar o IIS.

Configuração do CES

O cmdlet **Install-AdcsEnrollmentWebService** configura o Serviço da Web de registro de certificado (CES). Ele também é usado para criar outras instâncias do serviço em uma instalação existente.

1 Faça login no servidor de CES com o nome de usuário **`CESAdmin`** e, em seguida, inicie o PowerShell no modo administrativo.

2 Execute o comando **`Import-Module ServerManager`**.

3 Execute o comando **`Add-WindowsFeature Adcs-Enroll-Web-Svc`**.

4 Execute o comando **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType UserName`**.

Notas:

- Substitua *<sslCertThumbprint>* pela impressão digital do certificado SSL criado para o servidor de CES, após excluir os espaços entre os valores de impressão digital.
- Substitua **`CA1.contoso.com`** pelo nome do computador da AC.
- Substitua **`contoso-CA1-CA`** pelo nome comum da AC.

- Se você já configurou um método de autenticação no host, remova **`ApplicationPoolIdentity`** do comando.

5. Para concluir a instalação, selecione **Y** ou **A**.
6. Inicie o Console de gerenciamento do IIS.
7. No painel Conexões, expanda o servidor da Web que está hospedando o CES.
8. Expanda **Sites** e **Default Web Site**; em seguida, clique no nome do aplicativo virtual adequado da instalação: **contoso-CA1-CA_CES_UsernamePassword**.
9. No painel esquerdo, clique em **Pools de aplicativos**.
10. Selecione **WSEnrollmentServer** e, em seguida, no painel direito, clique em **Ações** > **Definições avançadas** em Ações.
11. Em Modelo de processo, selecione o campo Identidade.
12. Na caixa de diálogo Identidade do pool de aplicativos, selecione a conta personalizada e, em seguida, digite **`CESSvc`** como nome de usuário do domínio.
13. Feche todas as caixas de diálogo e, em seguida, recicle o IIS do painel direito do Console de gerenciamento do IIS.
14. No PowerShell, digite **`iisreset`** para reiniciar o IIS.

Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo SCEP

Esta seção fornece instruções sobre como configurar o OpenXPKI CA versão 2.5.x usando o Protocolo de registro de certificado simples (SCEP).

Notas:

- Certifique-se de que você esteja usando o sistema operacional Debian 8 Jessie.
- Para obter mais informações sobre OpenXPKI, acesse **www.openxpki.org**.

Configuração do OpenXPKI CA

Instalação do OpenXPKI CA

1. Conecte a máquina usando o PuTTY ou outro cliente.
2. No cliente, execute o comando **`sudo su -`** para ir para o usuário raiz.
3. Insira a senha raiz.
4. Em **nano /etc/apt/sources.list**, altere a origem para a instalação de atualizações.
5. Atualize o arquivo. Por exemplo:

```
#

# 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 Salve o arquivo.

7 Execute os seguintes comandos:

- **apt-get update**
- **apt-get upgrade**

8 Atualize as listas de certificados CA no servidor usando **apt-get install ca-certificates**.

9 Instale **en_US.utf8 locale** usando **dpkg-reconfigure locales**.

10 Selecione o local **en_US.UTF-8 UTF-8** e torne-o o local padrão para o sistema.

Nota: Use a tecla Tab e a barra de espaço para selecionar e navegar pelo menu.

11 Verifique os locais gerados usando **locale -a**.

Saída de amostra

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

12 Copie a impressão digital do pacote OpenXPKI usando **nano /home/Release.key**. Neste exemplo, copie a chave em **/home**.

13 Digite **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** como o valor.

14 Execute o seguinte comando:

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

15 Adicione o pacote usando o comando **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -**.

16 Adicione o repositório à lista de origem (jessie) usando **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list** e, em seguida, **aptitude update**.

17 Instale a ligação MySQL e Perl MySQL usando **aptitude install mysql-server libdbd-mysql-perl**.

18 Instale apache2.2-common usando **aptitude install apache2.2-common**.

19 Em **nano /etc/apt/sources.list**, instale o módulo fastcgi para acelerar a interface de usuário.

Nota: Recomendamos usar **mod_fcgid**.

20 Adicione a linha **deb http://http.us.debian.org/debian/jessie main** ao arquivo, e salve-o.

21 Execute os seguintes comandos:

```
apt-get update
aptitude install libapache2-mod-fcgid
```

22 Ative o módulo fastcgi usando **a2enmod fcgid**.

23 Instale o pacote de núcleo OpenXPKI usando **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Reinicie o servidor Apache® usando **service apache2 restart**.

25 Verifique se a instalação foi bem-sucedida usando **openxpkiadm version**.

Nota: Se a instalação for bem-sucedida, o sistema mostrará a versão do OpenXPKI instalado. Por exemplo, **Versão (núcleo): 2.5.5**.

26 Crie o banco de dados vazio e atribua o usuário do banco de dados usando **mysql -u root -p**.

Notas:

- Esse comando deve ser digitado no cliente. Caso contrário, não será possível inserir a senha.
- Digite a senha para o MySQL. Nesta instância, **root** é o usuário MySQL.
- **openxpki** é o usuário no qual o OpenXPKI está instalado.

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

Se o serviço MySQL não estiver em execução, execute **/etc/init.d/mysql start** para iniciar o serviço.

27 Digite **quit** para sair do MySQL.

28 Armazene as credenciais usadas em **/etc/openxpki/config.d/system/database.yaml**.

Conteúdo de arquivo de amostra

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

Nota: Altere **user** e **passwd** para que correspondam ao nome de usuário e à senha do MySQL.

29 Salve o arquivo.

30 Para esquema de banco de dados vazio, execute **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki** no arquivo de esquema fornecido.

31 Insira a senha do banco de dados.

Configuração do OpenXPKI CA usando o script padrão

Nota: O script padrão configura apenas o realm padrão, **ca-one**. O CDP e as CRLs não estão configurados.

1. Descompacte o script de exemplo para instalar o certificado usando **`gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz`**.
2. Execute o script usando **`bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh`**.
3. Confirme a configuração usando **`openxpkiadm alias --realm ca-one`**.

Saída de amostra

```
=== 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. Verifique se a instalação foi bem-sucedida usando **`openxpkictl start`**.

Saída de amostra

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

5. Faça o seguinte para acessar o servidor OpenXPKI:
   a. Em um navegador da Web, digite **`http://ipaddress/openxpki/`**.
   b. Faça login como **Operador**. A senha padrão é **`openxpki`**.

      Nota: O login de Operador tem duas contas de operador pré-configuradas, **raop** e **raop2**.
6. Crie uma solicitação de certificado e teste-a.

Configuração manual do OpenXPKI CA

Visão geral

Nota: Antes de começar, certifique-se de ter um conhecimento básico sobre a criação de certificados OpenSSL.

Para configurar o OpenXPKI CA manualmente, crie o seguinte:

1. Certificado CA raiz. Para mais informações, consulte " Criação de certificados CA raiz" na página 104.
2. Certificado do signatário da CA, assinado pela CA raiz. Para mais informações, consulte " Criação de certificados do signatário" na página 105.
3. Certificado do vault de dados, autoassinado. Para mais informações, consulte " Criação de certificados de vault" na página 105.
4. Certificado SCEP, assinado pelo certificado do signatário.

Notas:

- Ao selecionar o hash de assinatura, use SHA256 ou SHA512.
- Alterar o tamanho da chave pública é opcional.

Neste exemplo, estamos usando o diretório **/etc/certs/openxpki_ca-one/** para a geração de certificados. No entanto, você pode usar qualquer diretório.

Criação de arquivos de configuração OpenSSL

1. Execute o seguinte comando:

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

   Nota: Se seu servidor estiver acessível usando o nome de domínio totalmente qualificado (FQDN), use o DNS do servidor em vez do seu endereço IP.

Arquivo de exemplo

```
# 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:stlopenxpki.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 Altere o endereço IP e o nome do certificado CA com suas informações de configuração.

3 Salve o arquivo.

Criação de arquivos de senha para chaves de certificado

1 Execute o seguinte comando:

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

2 Digite a senha.

3 Salve o arquivo.

Criação de certificados CA raiz

Nota: Você pode criar um certificado CA raiz autoassinado ou gerar uma solicitação de certificado e, em seguida, fazer com que seja assinado pela CA raiz.

Execute os seguintes comandos:

Nota: Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. **openssl genrsa -out /etc/certs/openxpki_ca-one/ca-root-1.key -passout file:/etc/certs/openxpki_ca-one/pd.pass 4096**
2. **openssl req -new -key /etc/certs/openxpki_ca-one/ca-root-1.key -subj /DC=COM/DC=LEXMARK/DC=DEV/DC=CA-ONE/CN=MYOPENXPKI_ROOTCA -out /etc/certs/openxpki_ca-one/ca-root-1.csr**
3. **openssl req -config /etc/certs/openxpki_ca-one/openssl.conf -extensions v3_ca_extensions -x509 -days 3560 -in /etc/certs/openxpki_ca-one/ca-root-1.csr -key /etc/certs/openxpki_ca-one/ca-root-1.key -out /etc/certs/openxpki_ca-one/ca-root-1.crt -sha256**

Criação de certificados do signatário

Nota: Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. Execute o seguinte comando:

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

2. Altere o assunto na solicitação com suas informações CA usando **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**.
3. Obtenha o certificado assinado pela CA raiz usando **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**.

Criação de certificados de vault

Notas:

- O certificado do vault é autoassinado.
- Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. Execute o seguinte comando:

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

2 Altere o assunto na solicitação com suas informações CA usando **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**.

3 Execute o seguinte comando:

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

Criação de certificados SCEP

Nota: O certificado SCEP é assinado pelo certificado do signatário.

Execute os seguintes comandos:

Nota: Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

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**

Cópia de arquivos de chaves e criação de symlinks

1 Copie os arquivos de chave para **/etc/openxpki/ca/ca-one/**.

Nota: Os arquivos de chave devem ser legíveis pelo OpenXPKI.

```
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 Crie o symlink.

Nota: Symlinks são aliases usados pela configuração padrão.

```
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
```

Importação de certificados

Importe o certificado raiz, o certificado do signatário, o certificado do vault e o certificado SCEP para o banco de dados com os tokens apropriados.

Execute os seguintes comandos:

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. Verifique se a importação foi bem-sucedida usando **openxpkiadm alias --realm ca-one**.

Saída de amostra

```
=== 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
```

Inicialização do OpenXPKI

1. Execute o comando **openxpkictl start**.

Saída de amostra

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

2 Faça o seguinte para acessar o servidor OpenXPKI:

a Em um navegador da Web, digite **http://ipaddress/openxpki/**.

Nota: Em vez de **ipaddress**, você também pode usar o FQDN do servidor.

b Faça login como **Operador**. A senha padrão é **openxpki**.

Nota: O login de Operador tem duas contas de operador pré-configuradas, **raop** e **raop2**.

3 Crie uma solicitação de certificado e teste-a.

Geração de informações do CRL

Nota: Se o seu servidor estiver acessível usando FQDN, use o DNS do servidor em vez de seu endereço IP.

1 Pare o serviço OpenXPKI usando **Openxpkictl stop**.

2 Em **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml**, atualize a seção **conectores: cdp** para o seguinte:

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

a Em **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml**, atualize o seguinte:

- **crl_distribution_points:** seção

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

- **authority_info_access:** seção

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

Altere o endereço IP e o nome do certificado CA de acordo com o servidor CA.

b Em **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml**, faça o seguinte:

- Se necessário, atualize **nextupdate** e **renewal**.
- Adicione **ca_issuers** à seguinte seção:

```
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/
```

Altere o endereço IP e o nome do certificado CA de acordo com o servidor CA.

3 Inicie o serviço OpenXPKI usando **Openxpkictl start**.

Configuração da acessibilidade da CRL

1 Interrompa o serviço Apache usando **service apache2 stop**.

2 Crie um diretório **CertEnroll** para a CRL no diretório **/var/www/openxpki/**.

3 Defina **openxpki** como o proprietário do diretório e configure as permissões para permitir que o Apache leia e execute, enquanto outros serviços sejam somente leitura.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Adicione uma referência ao arquivo Apache alias.conf usando **nano /etc/apache2/mods-enabled/alias.conf**.

5 Após a seção **<Directory "/usr/share/apache2/icons">**, adicione o seguinte:

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

6 Adicione uma referência no arquivo apache2.conf usando **nano /etc/apache2/apache2.conf**.

7 Adicione o seguinte na seção **servidor Apache2 HTTPD**:

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

8 Inicie o serviço Apache usando **service apache2 start**.

Ativação do serviço SCEP

1 Pare o serviço OpenXPKI usando **openxpkictl stop**.

2 Instale o pacote openca-tools usando **aptitude install openca-tools**.

3 Inicie o serviço OpenXPKI usando **openxpkictl start**.

Teste o serviço usando qualquer cliente, como certnanny com SSCEP.

Nota: SSCEP é um cliente de linha de comando para SCEP. Você pode fazer download do SSCEP em **https://github.com/certnanny/sscep**.

Ativação do certificado Signatário em nome de (agente de inscrição)

Para solicitações automáticas de certificado, estamos usando o recurso de certificado Signatário em nome de OpenXPKI.

1 Pare o serviço OpenXPKI usando **openxpkictl stop**.

2 Em **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, na seção **authorized_signer:** adicione uma regra para o nome do assunto do certificado do signatário.

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

Notas:

- Nessa regra, qualquer CN de certificado iniciado com **Markvision_** é o certificado Signatário em nome de.

- O nome do assunto é definido no MVE para gerar o certificado Signatário em nome de.
- Revise o espaço e o recuo no arquivo de script.
- Se o CN for alterado no MVE, adicione o CN atualizado em OpenXPKI.
- Você pode especificar apenas um certificado como Signatário em nome de e, em seguida, especificar o CN completo.

3 Salve o arquivo.

4 Inicie o serviço OpenXPKI usando **`openxpkictl start`**.

Ativação da aprovação automática de solicitações de certificado no OpenXPKI CA

1 Pare o serviço OpenXPKI usando **`openxpkictl stop`**.

2 Em **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, atualize **`elegível:`** seção:

Conteúdo antigo

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

Novo conteúdo

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

Notas:

- Revise o espaço e o recuo no arquivo de script.
- Para aprovar certificados manualmente, comente o **`valor: 1`** e, em seguida, remova o comentário das outras linhas que foram comentadas anteriormente.

3 Salve o arquivo.

4 Inicie o serviço OpenXPKI usando **`openxpkictl start`**.

Criação de um segundo realm

No OpenXPKI, várias estruturas PKI podem ser configuradas no mesmo sistema. Os tópicos a seguir mostram como criar outro realm para MVE chamado **ca-two**.

Cópia e configuração de diretórios

1. Copie a árvore de diretórios de exemplo **/etc/openxpki/config.d/realm/ca-one** para um novo diretório (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) dentro do diretório do realm.
2. Em **/etc/openxpki/config.d/system/realms.yaml**, atualize a seguinte seção:

Conteúdo antigo

```
# 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/
```

Novo conteúdo

```
# 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. Salve o arquivo.

Criação de certificados

As instruções a seguir mostram como gerar o certificado do signatário, o certificado do vault e o certificado SCEP. A CA raiz assina o certificado do signatário e, em seguida, o certificado do signatário assina o certificado SCEP. O certificado do vault é autoassinado.

1. Gere e assine os certificados. Para mais informações, consulte " Configuração manual do OpenXPKI CA" na página 103.

   Nota: Altere o nome comum do certificado para que o usuário possa distinguir facilmente entre diferentes certificados para diferentes realms. Você pode alterar **DC=CA-ONE** para **DC=CA-TWO**. Os arquivos de certificado são criados no diretório **/etc/certs/openxpki_ca-two/**.

2. Copie os arquivos de chave para **/etc/openxpki/ca/ca-two/**.

   Nota: Os arquivos de chave devem ser legíveis pelo OpenXPKI.

   ```
   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 Crie o symlink. Além disso, crie um symlink para o certificado CA raiz.

Nota: Symlinks são aliases usados pela configuração padrão.

```
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 Importe o certificado do signatário, o certificado do vault e o certificado SCEP para o banco de dados com os tokens apropriados para **ca-two**.

```
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 Verifique se a importação foi bem-sucedida usando **openxpkiadm alias --realm ca-two**.

Saída de amostra

```
=== 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
```

Nesse caso, as informações da CA raiz são as mesmas para **ca-one** e **ca-two**.

6 Se tiver alterado a senha da chave de certificado durante a criação do certificado, atualize **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.

7 Gere as CRLs para o realm. Para mais informações, consulte " Geração de informações do CRL" na página 108.

8 Publique as CRLs para o realm. Para mais informações, consulte " Configuração da acessibilidade da CRL" na página 108.

9 Reinicie o serviço OpenXPKI usando **openxpkictl restart**.

Saída de amostra

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

10 Faça o seguinte para acessar o servidor OpenXPKI:

a Em um navegador da Web, digite **http://ipaddress/openxpki/**.

b Faça login como **Operador**. A senha padrão é **openxpki**.

Nota: O login de Operador tem duas contas de operador pré-configuradas, **raop** e **raop2**.

Configuração do endpoint SCEP para vários realms

O endpoint SCEP do realm padrão é **http://<ipaddress>/scep/scep**. Se você tiver vários realms, configure um endpoint SCEP exclusivo (arquivo de configuração diferente) para cada realm. Nas instruções a seguir, usamos dois realms PKI, **ca-one** e **ca-two**.

1 Copie o arquivo de configuração padrão em **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

Nota: Nomeie o arquivo como **ca-one.conf**.

2 Em **nano /etc/openxpki/scep/ca-one.conf**, altere o valor do realm para **realm=ca-one**.

3 Crie outro arquivo de configuração em **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

Nota: Nomeie o arquivo como **ca-two.conf**.

4 Em **nano /etc/openxpki/scep/ca-two.conf**, altere o valor do realm para **realm=ca-two**.

5 Reinicie o serviço OpenXPKI usando **openxpkictl restart**.

Os endpoints SCEP são os seguintes:

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

Se quiser diferenciar entre credenciais de login e modelos de certificado padrão para diferentes realms PKI, talvez uma configuração avançada seja necessária.

Ativando vários certificados ativos com a mesma entidade a estar presente por vez

Por padrão, no OpenXPKI, somente um certificado com o mesmo nome de entidade pode estar ativo por vez. Mas, quando você está impondo vários certificados nomeados, vários certificados ativos com o mesmo nome de entidade precisam estar presentes de cada vez.

1. Em **/etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, na seção **`política`**, altere o valor de **`max_active_certs`** de **1** para **0**.

   Notas:

   - REALM NAME é o nome do realm. Por exemplo, **ca-one**.
   - Revise o espaço e o recuo no arquivo de script.

2. Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Configuração do número de portas padrão para OpenXPKI CA

Por padrão, o Apache escuta na porta número 80. Configure o número de porta padrão para OpenXPKI CA, para evitar conflitos.

1. Em **/etc/apache2/ports.conf**, adicione ou modifique uma porta. Por exemplo, **`Escutar 8080`**.
2. Em **/etc/apache2/sites-enabled/000-default.conf**, adicione ou modifique a seção **`VirtualHost`** para mapear a nova porta. Por exemplo, **`<VirtualHost *:8080>`**.
3. Reinicie o servidor Apache usando **`systemctl restart apache2`**.

Para verificar o status, execute **`netstat -tlpn| grep apache`**. O URL de OpenXPKI SCEP agora é **http://ipaddress:8080/scep/ca-one**, e o URL da Web é **http://ip address:8080/openxpki**.

Rejeitando solicitações de certificado sem Senha de desafio na AC do OpenXPKI

Por padrão, o OpenXPKI aceita solicitações sem verificar a senha de desafio. A solicitação de certificado não é rejeitada, e a CA e o administrador da CA determinam se a solicitação deve ser aprovada ou rejeitada. Para evitar possíveis problemas de segurança, desative esse recurso para que todas as solicitações de certificados que contenham senhas inválidas sejam rejeitadas imediatamente. No MVE, a Senha de desafio é necessária somente ao gerar o certificado do agente de inscrição.

1. Em **etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, na seção **`política`**, altere o valor de **`allow_man_authen`** de **1** para **0**.

   Notas:

   - REALM NAME é o nome do realm. Por exemplo, **ca-one**.
   - Revise o espaço e o recuo no arquivo de script.

2. Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Adição de EKU de autenticação de cliente em certificados

1. Em **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, na seção **`extended_key_usage:`** altere o valor **`de client_auth:`** para **1**.

   Notas:

   - REALM NAME é o nome do realm. Por exemplo, **ca-one**.
   - Revise o espaço e o recuo no arquivo de script.

2. Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Obtenção de entidades de certificado completo ao solicitar pelo SCEP

Por padrão, o OpenXPKI lê apenas o CN do assunto do certificado solicitante. As demais informações, como país, localidade e DC, são codificadas. Por exemplo, se o assunto de um certificado é **`C=US`**, **`ST=KY`**, **`L=Lexington`**, **`O=Lexmark`**, **`OU=ISS`**, **`CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`**, após assinar o certificado pelo SCEP, o assunto é alterado para **`DC=Teste de implantação`**, **`DC= OpenXPKI`**, **`CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`**.

Nota: REALM NAME é o nome do realm. Por exemplo, **ca-one**.

1. Em **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, na seção **`inscrever`**, altere o valor de **`dn`** para:

   ```
   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. Salve o arquivo.

3. Crie um arquivo chamado **l.yaml** no diretório **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

4. Adicione o seguinte:

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

5. Salve o arquivo.

6. Crie um arquivo chamado **st.yaml** no diretório **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

7. Adicione o seguinte:

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

8 Salve o arquivo.

Nota: OpenXPKI deve possuir ambos os arquivos e deve ser legível, gravável e executável.

9 Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Revogando certificados e publicando o CRL

1 Acesse o servidor OpenXPKI.

   a Em um navegador da Web, digite **`http://ipaddress/openxpki/`**.

   b Faça login como **Operador**. A senha padrão é **`openxpki`**.

   Nota: O login de Operador tem duas contas de operador pré-configuradas, **raop** e **raop2**.

2 Clique em **Pesquisa de fluxo de trabalho** > **Pesquisar agora**.

3 Clique em um certificado para revogar e, em seguida, clique no link do certificado.

4 Na seção Ação, clique em **solicitação de revogação**.

5 Digite os valores apropriados e clique em **Continuar** > **Enviar solicitação**.

6 Na próxima página, aprove a solicitação. A revogação de certificado está aguardando a próxima publicação da CRL.

7 Na seção Operação de PKI, clique em **Emitir uma CRL (Certificate Revocation List, lista de revogação de certificados)**.

8 Clique em **Aplicar criação de listas de revogação** > **Continuar**.

9 Na seção Operação de PKI, clique em **Publicar CA/CRL**.

10 Clique em **Pesquisa de fluxo de trabalho** > **Pesquisar agora**.

11 Clique no certificado revogado com um tipo **certificate_revogation_request_v2**.

12 Clique em **Forçar ativação**.

Na nova CRL, você pode encontrar o número de série e o motivo da revogação do certificado revogado.

Gerenciamento de certificados usando a autoridade de certificações da OpenXPKI pelo EST

Esta seção ajuda o usuário a configurar o OpenXPKI CA versão 3.x.x usando o protocolo EST.

Notas:

- Certifique-se de que você esteja usando o sistema operacional Debian 10 Buster.
- Para obter mais informações sobre OpenXPKI, acesse **www.openxpki.org**.

Configuração do OpenXPKI CA

Instalação do OpenXPKI CA

1. Conecte a máquina usando o PuTTY ou outro cliente.
2. No cliente, execute o comando **`sudo su -`** para ir para o usuário raiz.
3. Insira a senha raiz.
4. Em **nano /etc/apt/sources.list**, altere a origem para a instalação de atualizações.
5. Atualize o arquivo. Por exemplo:

```
#

# 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. Salve o arquivo.
7. Execute os seguintes comandos:
   - **`apt-get update`**
   - **`apt-get upgrade`**
8. Atualize as listas de certificados CA no servidor usando **`apt-get install ca-certificates`**.
9. Instale **en_US.utf8 locale** usando **`dpkg-reconfigure locales`**.
10. Selecione o local **en_US.UTF-8 UTF-8** e torne-o o local padrão para o sistema.

    Nota: Use a tecla Tab e a barra de espaço para selecionar e navegar pelo menu.

11 Verifique os locais gerados usando **locale -a**.

Saída de amostra

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

12 Copie a impressão digital do pacote OpenXPKI usando **nano /home/Release.key**. Neste exemplo, copie a chave em **/home**.

13 Insira **55D89776 006F632B E0196E3E D2495509 BAFDDC74 22FEAAD2 F055074E 0FE3A724** como o valor.

14 Execute o seguinte comando:

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

15 Adicione o pacote usando o comando **wget https://packages.openxpki.org/v3/debian/Release.key -O - | apt-key add -** command.

16 Adicione o repositório à lista de origem (buster) usando **echo "deb http://packages.openxpki.org/v3/debian/ buster release" > /etc/apt/sources.list.d/openxpki.list** e, em seguida, **apt update**.

17 Instale a ligação MySQL e Perl MySQL usando **apt install mariadb-server libdbd-mariadb-perl**.

18 Instale apache2.2-common usando **apt install apache2**.

19 Em **nano /etc/apt/sources.list**, instale o módulo fastcgi para acelerar a interface de usuário.

Nota: Recomendamos usar **mod_fcgid**.

20 Adicione a linha **deb http://http.us.debian.org/debian/ buster main** ao arquivo, e salve-o.

21 Execute os seguintes comandos:

```
apt-get update
apt install libapache2-mod-fcgid
```

22 Ative o módulo fastcgi usando **a2enmod fcgid**.

23 Instale o pacote de núcleo OpenXPKI usando **apt install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Reinicie o servidor Apache usando **service apache2 restart**.

25 Verifique se a instalação foi bem-sucedida usando **openxpkiadm version**.

Nota: Se a instalação for bem-sucedida, o sistema mostrará a versão do OpenXPKI instalado. Por exemplo, **Versão (núcleo): 3.18.2**.

26 Crie o banco de dados vazio e atribua o usuário do banco de dados usando **mariadb -u root -p**.

Notas:

- Esse comando deve ser digitado no cliente. Caso contrário, não será possível inserir a senha.
- Digite a senha para o MySQL. Nesta instância, **root** é o usuário MySQL.

- **openxpki** é o usuário no qual o OpenXPKI está instalado.

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

Se o serviço MySQL não estiver em execução, execute **/etc/init.d/mysql start** para iniciar o serviço.

27 Digite **quit** para sair do MySQL.

28 Armazene as credenciais usadas em **/etc/openxpki/config.d/system/database.yaml**.

Conteúdo de arquivo de amostra

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

Nota: Altere **user** e **passwd** para que correspondam ao nome de usuário e à senha do MariaDB.

29 Salve o arquivo.

30 Para esquema de banco de dados vazio, execute **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mariadb.sql.gz | \ mysql -u root --password --database openxpki** no arquivo de esquema fornecido.

31 Digite a senha do banco de dados.

Configuração do OpenXPKI CA usando o script padrão

Nota: O script padrão configura apenas o realm padrão, **ca-one**. O CDP e as CRLs não estão configurados.

1 Execute o script usando **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh**.

2 Confirme a configuração usando **openxpkiadm alias --realm democa**.

Saída de amostra

```
=== 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
```

3 Verifique se a instalação foi bem-sucedida usando **openxpkictl start**.

Saída de amostra

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

4 Faça o seguinte para acessar o servidor OpenXPKI:

a Em um navegador da Web, digite **http://ipaddress/openxpki/**.

b Adicione o nome de usuário e suas senhas correspondentes em um arquivo **userdb.yaml**. Para adicionar o nome de usuário e a senha, faça o seguinte:

- Faça check-out para **/home/pkiadm** e depois **nanoterdb.yaml**.
- Cole o seguinte:

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

Nota: Neste caso, estRA refere-se ao nome de usuário. Para gerar a senha, digite **openxpkiadm hashpwd**. Quando uma mensagem solicitando a senha e uma senha criptografada ssha256 for exibida, copie-a e cole-a no resumo de qualquer usuário.

Nota: As funções disponíveis no login Operador são Operador RA, Operador CA e usuário.

5 Insira o nome de usuário e a senha.

6 Crie uma solicitação de certificado e teste-a.

Configuração manual do OpenXPKI CA

Visão geral

Nota: Antes de começar, certifique-se de ter um conhecimento básico sobre a criação de certificados OpenSSL.

Para configurar o OpenXPKI CA manualmente, crie o seguinte:

1 Certificado CA raiz. Para obter mais informações, consulte " Criação de certificados CA raiz" na página 104.

2 Certificado do signatário da CA, assinado pela CA raiz. Para obter mais informações, consulte " Criação de certificados do signatário" na página 105.

3 Certificado do vault de dados, autoassinado. Para obter mais informações, consulte " Criação de certificados de vault" na página 105.

4 Certificado Web, assinado pelo certificado do signatário. Para obter mais informações, consulte " Configuração do servidor da Web" na página 124.

Notas:

- Ao selecionar o hash de assinatura, use SHA256 ou SHA512.
- Alterar o tamanho da chave pública é opcional.

Para a versão 3,10 ou posterior, você pode gerenciar as chaves diretamente usando o comando alias openxpkiadm:

- Execute **mkdir -p /etc/openxpki/local/keys** para criar o diretório. O local padrão do diretório é **/etc/openxpki/local/keys**.
- Execute **openxpkictl start** para iniciar o servidor.

Neste exemplo, estamos usando o diretório **/etc/certs/openxpki_democa/** para a geração de certificados. No entanto, você pode usar qualquer diretório.

Criação de arquivos de configuração OpenSSL

O arquivo de configuração OpenSSL contém X.509 extensões para geração e assinatura de solicitações de certificado.

1 Execute o seguinte comando:

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

Nota: Se seu servidor estiver acessível usando o nome de domínio totalmente qualificado (FQDN), use o DNS do servidor em vez do seu endereço IP.

Arquivo de exemplo

```
# 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.crl
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. Substitua o endereço IP e o nome do certificado CA com suas informações de configuração.
3. Salve o arquivo.

Criação de arquivos de senha para chaves de certificado

1. Execute o seguinte comando:

   nano /etc/certs/openxpki_democa/pd.pass

2. Digite a senha.
3. Salve o arquivo.

Criação de certificados CA raiz

Você pode criar um certificado CA raiz autoassinado ou gerar uma solicitação de certificado e, em seguida, fazer com que seja assinado pela CA raiz.

Nota: Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. Execute o seguinte comando:

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

2. Substitua o assunto na solicitação por suas informações da CA usando **openssl req -new -key /etc/certs/openxpki_democa/ca-root-1.key -out /etc/certs/openxpki_democa/ca-root-1.csr**.

3. Obtenha o certificado assinado pela CA raiz usando **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**.

4. Vá para **/etc/certs/openxpki_democa/** onde **ca-root-1.crt** está salvo.

5. Execute o seguinte comando:

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

Criação de certificados do signatário

Nota: Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. Execute o seguinte comando:

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

2. Altere o assunto na solicitação com suas informações CA usando **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**.

3. Obtenha o certificado assinado pela CA raiz usando **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**.

4. Execute o seguinte comando:

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

Criação de certificados de vault

Notas:

- O certificado do vault é autoassinado.
- Substitua o comprimento da chave, o algoritmo de assinatura e o nome do certificado pelos valores apropriados.

1. Execute o seguinte comando:

   ```
   openssl req -new -x509 -keyout vault.key -out vault.crt -days 1100 -
   config /etc/certs/openxpki_democa/openssl.conf
   ```

2. Altere o assunto na solicitação com suas informações de CA usando **openxpkiadm certificate import --file vault.crt**.

3. Execute o seguinte comando:

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

   Nota: Forneça os valores necessários, mas mantenha **/CN=DataVault** como o assunto.

Criação de um certificado da Web

1. Execute o seguinte comando:

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

2. Altere o assunto na solicitação com suas informações CA usando **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**.

3. Execute o seguinte comando:

   ```
   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
   ```

Configuração do servidor da Web

1. Execute os seguintes comandos:

   ```
   a2enmod ssl rewrite headers
   a2ensite openxpki
   a2dissite 000-default default-ssl
   mkdir -m755 -p /etc/openxpki/tls/chain
   cp /etc/certs/openxpki_democa/ca-root-1.crt /etc/openxpki/tls/chain/
   cp /etc/certs/openxpki_democa/ca-signer-1.crt /etc/openxpki/tls/chain/
   c_rehash /etc/openxpki/tls/chain/
   mkdir -m755 -p /etc/openxpki/tls/endentity
   ```

```
mkdir -m700 -p /etc/openxpki/tls/private
cp /etc/certs/openxpki_democa/web-1.crt /etc/openxpki/tls/endentity/openxp
ki.crt
cat /etc/certs/openxpki_democa/ca-signer-1.crt
>> /etc/openxpki/tls/endentity/openxpki.crt
openssl rsa -in /etc/certs/openxpki_democa/web-1.key -passin
file:/etc/certs/openxpki_democa/pd.pass -
out /etc/openxpki/tls/private/openxpki.pem
chmod 400 /etc/openxpki/tls/private/openxpki.pem
```

2 Reinicie o serviço Apache usando **apache2 restart**.

3 Execute o seguinte comando para verificar a importação bem-sucedida dos arquivos:

```
openxpkiadm alias --realm democa
```

Saída de amostra

```
=== 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
```

Disponibilização da senha da chave de certificado para OpenXPKI

1 Altere o valor no arquivo **nano /etc/openxpki/config.d/system/crypto.yaml**.

2 Descomente o cache: **daemon under secret: padrão**:

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

Inicialização do OpenXPKI

1 Execute o comando **openxpkictl start**.

Saída de amostra

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

2 Acesse o servidor OpenXPKI:

a Em um navegador da Web, digite **http://ipaddress/openxpki/**.

b Adicione os nomes de usuário e as senhas correspondentes em um arquivo **userdb.yaml**:

- Faça check-out para **/home/pkiadm** e depois para **nanoterdb.yaml**.
- Cole o seguinte:

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

Nota: Aqui estRA refere-se ao nome de usuário.

- Para gerar a senha, digite **openxpkiadm hashpwd**. Uma mensagem mostrando a senha e uma senha criptografada ssha256 é exibida.
- Copie a senha e cole-a no resumo de qualquer usuário.

Nota: O login do operador tem duas funções pré-configuradas disponíveis: Operador RA, Operador CA e usuário.

3 Digite um nome de usuário e uma senha.

4 Crie uma solicitação de certificado e teste-a.

Geração de informações do CRL

Nota: Se o seu servidor estiver acessível usando FQDN, use o DNS do servidor em vez de seu endereço IP.

1 Pare o serviço OpenXPKI usando **openxpkictl stop**.

2 Em **nano /etc/openxpki/config.d/realm/democa/publishing.yaml**, atualize a seção **conectores: cdp** para o seguinte:

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

a Em **nano /etc/openxpki/config.d/realm/democa/profile/default.yaml**, atualize o seguinte:

- **crl_distribution_points:** seção

```
critical: 0
uri:
    - https://FQDN of the est/openxkpi/CenrtEnroll/[% ISSUER.CN.0 %].crl
    - ldap://localhost/[% ISSUER.DN %]
```

- **authority_info_access:** seção

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

Altere o endereço IP e o nome do certificado CA de acordo com o servidor CA.

Nota: O caminho Authority_info_access (AIA) é salvo na pasta Download, mas você pode definir o local de acordo com sua preferência.

b Em **nano /etc/openxpki/config.d/realm/democa/crl/default.yaml**, faça o seguinte:

- Se necessário, atualize **nextupdate** e **renewal**.
- Adicione **ca_issuers** à seguinte seção:

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

Altere o endereço IP e o nome do certificado CA de acordo com o servidor CA.

3 Inicie o serviço OpenXPKI usando **openxpkictl start**.

Publicação de informações de CRL

Depois de criar as CRLs, você deve publicá-las para serem acessadas por todos.

1 Interrompa o serviço Apache usando **service apache2 stop**.

2 Crie um diretório **CertEnroll** para a CRL no diretório **/var/www/openxpki/**.

3 Defina **openxpki** como o proprietário do diretório e configure as permissões para permitir que o Apache leia e execute, enquanto outros serviços sejam somente leitura.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Adicione uma referência ao arquivo Apache alias.conf usando **nano /etc/apache2/mods-enabled/alias.conf**.

5 Após a seção **<Directory "/usr/share/apache2/icons">**, adicione o seguinte:

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

6 Adicione uma referência no arquivo apache2.conf usando **nano /etc/apache2/apache2.conf**.

7 Adicione o seguinte na seção **servidor Apache2 HTTPD**:

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

8 Inicie o serviço Apache usando **service apache2 start**.

Ativação da aprovação automática de solicitações de certificado no OpenXPKI CA

1. Pare o serviço OpenXPKI usando **`openxpkictl stop`**.
2. Em **/etc/openxpki/config.d/realm/democa/est/default.yaml**, atualize o **`elegível:`** seção:

Conteúdo antigo

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

Novo conteúdo

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

Notas:

- Revise o espaço e o recuo no arquivo de script.
- Para aprovar certificados manualmente, comente o **`valor: 1`** e, em seguida, remova o comentário das outras linhas que foram comentadas anteriormente.

3. Salve o arquivo.
4. Inicie o serviço OpenXPKI usando **`openxpkictl start`**.

Alterar detalhes para habilitar o download de ca-certs

1. Execute o seguinte comando:

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

2. Substituir **`my $mime = "application/pkcs7-mime; smime-type=certs-only";`** por **`my $mime = "application/pkcs7-mime";`**.
3. Inicie o serviço OpenXPKI usando **`openxpkictl`**.

Criação de um segundo realm

No OpenXPKI, várias estruturas PKI podem ser configuradas no mesmo sistema. Os tópicos a seguir mostram como criar outro realm para MVE chamado **democa-two**.

Cópia e configuração de diretórios

1. Crie um diretório, ou seja, **democa2**, para o segundo realm dentro de **/etc/openxpki/config.d/realm**.
2. Copie a árvore de diretórios de exemplo **/etc/openxpki/config.d/realm/ca-one** para um novo diretório (**cp -r /etc/openxpki/config.d/realm.tpl/*/etc/openxpki/config.d/realm/democa2**) dentro do diretório do realm.
3. Em **/etc/openxpki/config.d/system/realms.yaml**, atualize a seguinte seção:

Conteúdo antigo

```
# 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/
```

Novo conteúdo

```
# 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. Salve o arquivo.

Configuração do endpoint EST para vários realms

Você pode configurar o endpoint EST com um tuplo composto pela parte de autoridade do URI e o rótulo opcional (por exemplo, www.example.com:80 e arbitraryLabel1). Nas instruções a seguir, usamos dois realms PKI, **`democa`** e **`democa2`**.

1. Copie o arquivo de configuração padrão em **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa.conf**.

   Nota: Nomeie o arquivo como **`democa.conf`**.

2. Em **nano /etc/openxpki/scep/democa.conf**, altere o valor do realm para **`realm=democa`**.

   Nota: De acordo com suas necessidades, você pode precisar desfazer o comentário das linhas correspondentes para as seções **simpleenroll**, **simplereenroll**, **csrattrs** e **cacerts**. Mantenha as seções de ambiente comentadas. Faça o mesmo para **default.conf**.

3 Crie outro arquivo de configuração em **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa2.conf**.

Nota: Nomeie o arquivo como **`democa2.conf`**.

4 Em **nano /etc/openxpki/scep/democa2.conf**, altere o valor do realm para **`realm=democa2`**.

Nota: De acordo com suas necessidades, você pode precisar desfazer o comentário das linhas correspondentes para as seções **simpleenroll**, **simplereenroll**, **csrattrs** e **cacerts**. Mantenha as seções de ambiente comentadas.

5 Copie o arquivo **default.yaml** nos seguintes locais:

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

Nota: Nomeie o arquivo como **`democa.yaml`**.

6 Copie o arquivo **default.yaml** nos seguintes locais:

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

Nota: Nomeie o arquivo como **`democa2.yaml`**.

7 Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Selecione os seguintes URLs para abrir o servidor da EST correspondente a um realm por meio de um navegador da Web:

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

Se quiser diferenciar entre credenciais de login e modelos de certificado padrão para diferentes realms PKI, talvez uma configuração avançada seja necessária.

Criação de certificados do signatário

As instruções a seguir mostram como gerar um certificado de signatário no segundo realm. Você pode usar os mesmos certificados raiz e de vault que os do primeiro realm.

1 Crie um arquivo de configuração OpenSSL no **nano /etc/certs/openxpki_democa2/openssl.conf**.

Nota: Altere o nome comum do certificado para que o usuário possa distinguir facilmente entre diferentes certificados para diferentes realms. Os arquivos de certificado são criados no diretório **/etc/certs/openxpki_democa2/**.

2 Vá para o diretório do certificado do vault no primeiro realm e importe o certificado do primeiro realm.

3 Execute o seguinte código:

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

Criação de arquivos de senha para chaves de certificado

1 Execute o seguinte comando:

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

2 Digite a senha.

3 Crie um certificado do signatário. Para obter mais informações, consulte " Criação de certificados do signatário" na página 105.

4 Verifique se a importação foi bem-sucedida usando **openxpkiadm alias --realm democa2**.

Nota: Se você alterou a senha da chave do certificado durante a criação do certificado, atualize **nano /etc/openxpki/config.d/realm/democa2/crypto.yaml**.

5 Gere as CRLs para o segundo realm. Para obter mais informações, consulte " Geração de informações do CRL" na página 108.

Nota: Certifique-se de usar o nome correto do Certificado CA de acordo com o realm.

6 Publique as CRLs para o realm. Para obter mais informações, consulte " Publicação de informações de CRL" na página 127.

7 Reinicie o serviço OpenXPKI usando **openxpkictl restart**.

Saída de amostra

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

Ativação de vários certificados ativos com o mesmo assunto a estar presente por vez

Por padrão, no OpenXPKI, somente um certificado com o mesmo nome de entidade pode estar ativo por vez. Mas, quando você está impondo vários certificados nomeados, vários certificados ativos com o mesmo nome de entidade precisam estar presentes de cada vez.

1 Em **/etc/openxpki/config.d/realm/REALM NAME/est/< REALM NAME >.yaml**, na seção **`política`**, altere o valor de **`max_active_certs`** de **`1`** para **`0`**.

Notas:

- REALM NAME é o nome do realm. Por exemplo, **ca-one**.
- Revise o espaço e o recuo no arquivo de script.

2 Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

Configuração do número de portas padrão para OpenXPKI CA

Por padrão, o Apache escuta na porta número 443 para https. Configure o número de porta padrão para OpenXPKI CA, para evitar conflitos.

1 Em **/etc/apache2/ports.conf**, modifique a porta 443 para qualquer outra porta. Por exemplo:

Conteúdo antigo

```
Listen 80

<IfModule ssl_module>
   Listen 443
</IfModule>

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

Novo conteúdo

```
Listen 80

<IfModule ssl_module>
   Listen 9443
</IfModule>

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

2 Em **/etc/apache2/sites-available/openxpki.conf**, adicione ou modifique a seção **`VirtualHost`** para mapear a nova porta. Por exemplo, **`<VirtualHost *:443>`** para **`<VirtualHost *:9443>`**.

3 Em **/etc/apache2/sites-available/default-ssl.conf**, adicione ou modifique a seção **`VirtualHost_default`** para mapear a nova porta. Por exemplo, altere **`<VirtualHost *:443>`** para **`<VirtualHost *:9443>`**.

4 Reinicie o servidor Apache usando **`systemctl restart apache2`**.

Nota: Se ele solicitar a senha **SSL/TLS**, digite a senha enquanto adiciona o certificado do servidor Web TLS no servidor EST.

5 Em **tinddopenxpkiweb01.dhcp.dev.lexmark.com:9443 (RSA):**, digite a senha para as chaves **SSL/TLS**.

Para verificar o status, execute **`netstat -tlpn| grep apache`**. O URL de OpenXPKI SCEP agora é **https://ipaddress**, e o URL da Web é **FQDN:9443/openxpki**.

Habilitação da autenticação básica

1 Execute o seguinte comando:

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

2 Crie uma conta de usuário que tenha acesso ao servidor. Insira os seguintes dados:

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

3 Vá para o diretório **`cd /etc/apache2/sites-enabled/`**.

4 Em **nano openxpki.conf**, adicione as seguintes linhas no **`<VirtualHost *: 443 block>`**:

```
#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 Adicione **`ErrorDocument 401 %{unescape:%00}`** antes do **SSLEngine** no mesmo bloco de host virtual.

Exemplo

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

6 Reinicie o **apache2 service** usando **service apache2 restart**.

Nota: A autenticação básica funciona usando o nome de usuário e a senha acima.

Ativação do certificado do cliente

1 Vá para o seguinte diretório: **`cd /etc/apache2/sites-enabled/`**.

2 Para o host necessário no **nano openxpki.conf**, adicione **SSLVerifyClient require**.

Por exemplo, se você estiver usando a porta 443, modifique a seção **VirtualHost** para:

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

3 Remova o comando **SSLVerifyClient optional_no_ca**.

4 Salve o arquivo e digite **`quit`** para sair do MySQL.

5 Vá para o seguinte diretório: **`cd /etc/openxpki/config.d/realm/democa/est`**.

6 Abra **default.yaml** e **democra.yaml**.

Nota: Se a etiqueta for diferente, altere o arquivo YAML.

7 Execute o seguinte comando:

`vi default.yaml`

8 Na seção **authorized_signer**, adicione o seguinte:

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

Por exemplo, se o nome do assunto do certificado do cliente for **test123**, adicione o seguinte na seção **`authorized_signer`**:

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

9 Salve o arquivo e digite **`quit`** para sair do MySQL.

10 Reinicie o serviço OpenXPKI usando **`openxpkictl restart`**.

11 Reinicie o serviço Apache usando **`service apache2 start`**.

O que causa o erro de incompatibilidade de SAN que impede o sistema de buscar a CRL?

O erro de incompatibilidade de SAN pode ocorrer ao ativar as informações de CRL. Esse erro indica que o IP ou o nome do host não corresponde ao valor da SAN no certificado da Web. Para evitar esse erro, use o FQDN no caminho da CRL em vez do IP. Você também pode configurar o certificado da Web e usar o FQDN do seu sistema no campo SAN.

Por que os tokens ca-signer-1 e vault-1 estão offline?

Se a página Status do sistema mostrar que seus tokens ca-signer-1 e vault-1 estão offline, faça o seguinte:

1. Em **/etc/openxpki/config.d/realm/realm name/crypto.yaml**, altere a senha da chave do certificado.
2. Reinicie o serviço OpenXPKI.

Gerenciamento de alertas da impressora

Visão geral

Os alertas são acionados quando uma impressora requer atenção. As ações permitem enviar e-mails personalizados ou executar scripts quando ocorrer um alerta. Os eventos definem quais ações são executadas quando alertas específicos estão ativos. Para registrar alertas de uma impressora, crie ações e as associe com um evento. Atribua o evento às impressoras que deseja monitorar.

Nota: Esse recurso não se aplica a impressoras protegidas.

Como criar uma ação

Uma ação é uma notificação de e-mail ou um registro de visualizador de evento. Ações atribuídas a eventos são acionadas quando ocorre um alerta da impressora.

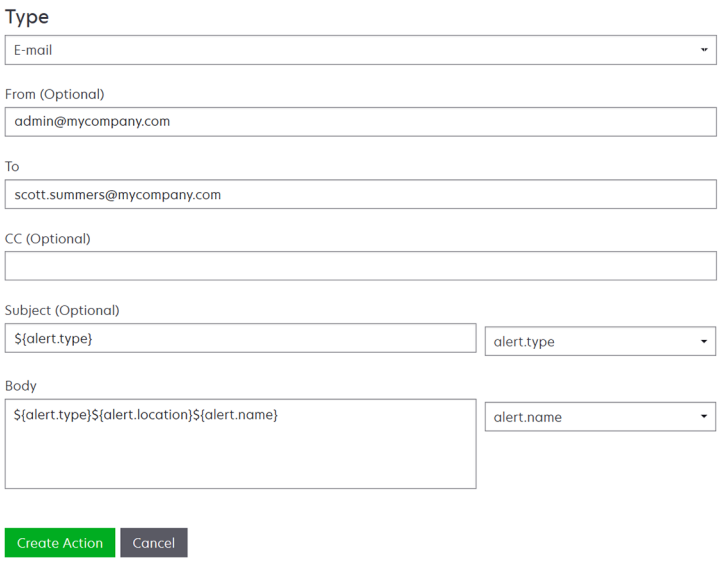
1. No menu Impressoras, clique em **Eventos e ações** > **Ações** > **Criar**.
2. Digite um nome exclusivo para a ação e sua descrição.
3. Selecione um tipo de ação.

E-mail

Nota: Antes de começar, certifique-se de que as definições de e-mail estejam configuradas. Para obter mais informações, consulte " Definição das configurações de e-mail" na página 147.

a. No menu Tipo, selecione **E-mail**.

b. Digite os valores apropriados nos campos. Você também pode usar os espaços reservados disponíveis como assunto, no todo ou em parte, ou como parte de uma mensagem de e-mail. Para obter mais informações, consulte " Compreendendo espaços reservados de ação" na página 136.

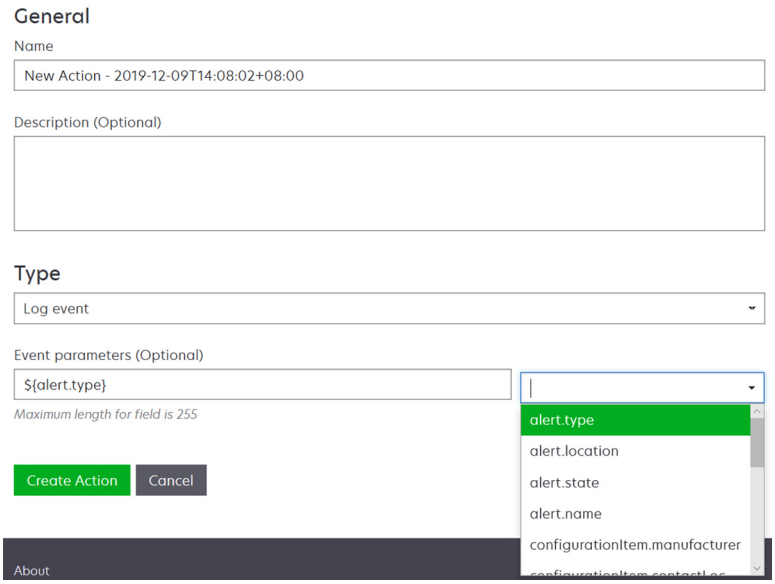


c. Clique em **Criar ação**.

Evento de registro

a No menu Tipo, selecione **Evento de registro**.

b Digite os parâmetros do evento. Você também pode usar os espaços reservados disponíveis no menu suspenso. Para obter mais informações, consulte " Compreendendo espaços reservados de ação" na página 136.



c Clique em **Criar ação**.

Compreendendo espaços reservados de ação

Use os espaços reservados disponíveis no título do assunto ou na mensagem de e-mail. Os espaços reservados são elementos variáveis e serão substituídos pelos valores reais quando usados.

- **${eventHandler.timestamp}**—a data e a hora em que o MVE processou o evento. Por exemplo, **`14 de março de 2017 1:42:24 PM`**.
- **${eventHandler.name}**—O nome do evento.
- **${configurationItem.name}**—O nome de sistema da impressora que acionou o alerta.
- **${configurationItem.address}**—O endereço MAC da impressora que acionou do alerta.
- **${configurationItem.ipAddress}**—O endereço IP da impressora que acionou do alerta.
- **${configurationItem.ipHostname}**—O nome do host da impressora que acionou o alerta.
- **${configurationItem.model}**—O nome do modelo da impressora que acionou do alerta.
- **${configurationItem.serialNumber}**—O número de série da impressora que acionou o alerta.
- **${configurationItem.propertyTag}**—A etiqueta de propriedade da impressora que acionou o alerta.
- **${configurationItem.contactName}**—O nome de contato da impressora que acionou o alerta.
- **${configurationItem.contactLocation}**—A localização do contato da impressora que acionou o alerta.
- **${configurationItem.manufacturer}**—O fabricante da impressora que acionou o alerta.
- **${alert.name}**—O nome do alerta que é acionado.
- **${alert.state}**—O estado do alerta. Ele pode ser ativado ou excluído.

- **${alert.location}**—O local na impressora onde ocorreu o acionamento do alerta.
- **${alert.type}**—A gravidade do alerta acionado, como **`Aviso`** ou **`Intervenção necessária`**.

Gerenciamento de ações

1. No menu Impressoras, clique em **Eventos e Ações** > **Ações**.
2. Tente um dos seguintes métodos:

Editar uma ação

a. Selecione uma ação e clique em **Editar**.
b. Configure as definições.
c. Clique em **Salvar alterações**.

Excluir ações

a. Selecione uma ou mais ações.
b. Clique em **Excluir**e confirme a exclusão.

Teste uma ação

a. Selecione uma ação e clique em **Testar**.
b. Para verificar os resultados do teste, verifique os registros das tarefas.

Notas:

- Para obter mais informações, consulte " Exibindo registros" na página 143.
- Se você estiver testando uma ação de e-mail, verifique se o e-mail for enviado ao destinatário.

Criação de um evento

É possível monitorar alertas em sua frota de impressoras. Crie um evento e defina uma ação a ser executada quando os alertas especificados ocorrerem. Eventos não são suportados em impressoras protegidas.

1. No menu Impressoras, clique em **Eventos e ações** > **Eventos** > **Criar**.
2. Digite um nome exclusivo para a evento e sua descrição.
3. Na seção Alertas, selecione um ou mais alertas. Para obter mais informações, consulte " Compreendendo alertas da impressora" na página 138.
4. Na seção Ações, selecione uma ou mais ações para executar quando os alertas selecionados estiverem ativos.

   Nota: Para obter mais informações, consulte " Como criar uma ação" na página 135.
5. Ative o sistema para executar as ações selecionadas quando alertas são removidos da impressora.
6. Defina um período de cortesia antes de executar quaisquer ações selecionadas.

   Nota: Se o alerta for removido durante o período de cortesia, a ação não será executada.
7. Clique em **Criar evento**.

Compreendendo alertas da impressora

Os alertas são acionados quando uma impressora requer atenção. Os seguintes alertas podem ser associados com um evento no MVE:

- **Atolamento do Alimentador Automático de Documentos (ADF)**—Uma folha de papel está atolada no ADF e deve ser fisicamente removida.
  - Atolamento na saída do ADF do scanner
  - Atolamento no alimentador do ADF do scanner
  - Atolamento no inversor do ADF do scanner
  - Papel do ADF do scanner removido
  - Papel do ADF do scanner ausente
  - Atolamento no pré-registro do ADF do scanner
  - Atolamento no registro do ADF do scanner
  - Alerta do scanner - Recoloque todos os originais para reiniciar o trabalho
- **Porta ou tampa aberta**—Uma porta está aberta na impressora e deve ser fechada.
  - Verificar porta/tampa - Caixa de correio
  - Porta aberta
  - Alerta de tampa
  - Tampa fechada
  - Tampa aberta
  - Tampa aberta ou Cartucho ausente
  - Tampa da unidade duplex aberta
  - Tampa do ADF do scanner aberta
  - Tampa de Acesso ao Atolamento do Scanner Aberta
- **Tamanho ou tipo de mídia incorreto**—Um trabalho está sendo impresso e requer que um tipo de papel específico seja carregado na bandeja.
  - Tamanho de envelope incorreto
  - Alimentação manual incorreta
  - Mídia incorreta
  - Tamanho de mídia incorreto
  - Carregar mídia
- **Memória cheia ou erro**—A impressora está com pouca memória e é necessário fazer alterações.
  - Página complexa
  - Os arquivos serão excluídos
  - Memória de agrupamento insuficiente
  - Memória de desfragmentação insuficiente
  - Memória de fax insuficiente
  - Memória insuficiente
  - Memória insuficiente - Os trabalhos retidos podem ser perdidos
  - Memória insuficiente para economia de recursos
  - Memory Full (Memória cheia)
  - Memória PS insuficiente

  - Excesso de páginas no scanner - trabalho de digitalização cancelado
  - Redução de resolução
- **Mau funcionamento de opção**—Uma opção associada à impressora está em um estado de erro. As opções incluem opções de entrada, opções de saída, cartões de fontes, cartões de memória flash do usuário, discos e encadernadores.
  - Verificar alinhamento/conexão
  - Verificar a conexão da unidade duplex
  - Verificar a instalação do encadernador/caixa de correio
  - Verificar a energia
  - Opção corrompida
  - Opção danificada
  - Desconectar dispositivo
  - Alerta da unidade duplex
  - Bandeja da unidade duplex ausente
  - Adaptador de rede externo perdido
  - Alerta do encadernador
  - Porta do encadernador ou bloqueador aberto
  - Parede de papel do encadernador aberta
  - Dispositivo duplex incompatível
  - Dispositivo de entrada incompatível
  - Dispositivo de saída incompatível
  - Dispositivo desconhecido incompatível
  - Instalação de opção incorreta
  - Alerta de entrada
  - Erro ao configurar entrada
  - Alerta de opção
  - Compartimento de saída cheio
  - Compartimento de saída quase cheio
  - Erro de configuração da saída
  - Opção cheia
  - Opção ausente
  - Mecanismo de alimentação de papel ausente
  - Trabalhos de impressão na opção
  - Reconectar dispositivo
  - Reconectar dispositivo de saída
  - Muitas entradas instaladas
  - Muitas opções instaladas
  - Muitas saídas instaladas
  - Bandeja ausente
  - Bandeja ausente durante inicialização
  - Erro do sensor de bandejas

  - Entrada não calibrada
  - Opção não formatada
  - Opção não suportada
  - Reconectar dispositivo de entrada
- **Atolamento do papel**—Uma folha de papel está atolada na impressora e deve ser fisicamente removida.
  - Atolamento de papel interno
  - Alerta de atolamento
  - Atolamento de papel
- **Erro do scanner**—O scanner apresenta um problema.
  - Cabo traseiro do scanner desconectado
  - Carro do scanner bloqueado
  - Limpar vidro/fita de suporte da base de cópia do scanner
  - Scanner desativado
  - Tampa do scanner de mesa aberta
  - Cabo frontal do scanner desconectado
  - Registro do scanner inválido
- **Erro de suprimentos**—Um suprimento da impressora apresenta um problema.
  - Suprimento anormal
  - Incompatibilidade de região do cartucho
  - Suprimento danificado
  - Unidade do fusor ou OCR ausente
  - Cartucho esquerdo inválido ou ausente
  - Cartucho direito inválido ou ausente
  - Suprimento inválido
  - Falha na preparação
  - Alerta de suprimento
  - Atolamento de suprimentos
  - Suprimento ausente
  - Alavanca de ejeção do cartucho de toner puxada
  - Cartucho de toner não instalado corretamente
  - Suprimento não calibrado
  - Suprimento não licenciado
  - Suprimento não suportado
- **Suprimentos ou consumível vazio**—Um suprimento da impressora deve ser substituído.
  - Entrada vazia
  - Vida útil esgotada
  - Impressora pronta para manutenção
  - Manutenção programada
  - Suprimento vazio
  - Suprimento cheio
  - Suprimento cheio ou ausente

Nota: A impressora envia o alerta como um erro e um aviso. Se um desses alertas for disparado, sua ação associada ocorrerá duas vezes.

- **Suprimentos ou consumível baixo**—Um suprimento da impressora está acabando.
  - Aviso antecipado
  - Primeiro baixo
  - Entrada baixa
  - Acabando
  - Quase vazio
  - Quase baixo
  - Pouco suprimento
  - Suprimento quase cheio
- **Alerta ou condição não categorizada**
  - Falha na calibração de cores
  - Erro de transmissão de dados
  - Falha no CRC do mecanismo
  - Alerta externo
  - Conexão de fax perdida
  - Ventilador travado
  - Hex ativo
  - Insira a página frente e verso e pressione Ir para
  - Alerta interno
  - O adaptador de rede interno precisa de manutenção
  - Alerta de unidade lógica
  - Off-line
  - Off-line para prompt de aviso
  - Falha na operação
  - Alerta de intervenção do operador
  - Erro na página
  - Alerta de porta
  - Falha de comunicação da porta
  - Porta desativada
  - Economia de energia
  - Desligando
  - Tempo limite de trabalho PS
  - Tempo limite de manual PS
  - Config. obrigatória
  - Erro de soma de verificação SIMM
  - Calibração de suprimento
  - Falha no sensor de correção de toner
  - Condição de alerta desconhecida
  - Configuração desconhecida

- Condição de alerta do scanner desconhecida
- Usuário(s) bloqueado(s)
- Alerta de aviso

Gerenciando eventos

1. No menu Impressoras, clique em **Eventos e Ações** > **Eventos**.
2. Execute um dos seguintes procedimentos:

Editar um evento

a. Selecione um evento e clique em **Editar**.
b. Configure as definições.
c. Clique em **Salvar alterações**.

Excluir eventos

a. Selecione um ou mais eventos.
b. Clique em **Excluir**e confirme a exclusão.

Exibição do status e do histórico das tarefas

Visão geral

Tarefas são todas as atividades de gerenciamento da impressora executadas no MVE, como descoberta, auditoria e aplicação de configurações da impressora. A página Status exibe o status de todas as tarefas atuais sendo executadas e as tarefas executadas nas últimas 72 horas. As informações sobre as tarefas sendo executadas no momento são inseridas no registro. As tarefas com mais de 72 horas podem ser exibidas somente como entradas individuais de registro na página Registro, e podem ser pesquisadas usando os IDs da tarefa.

Visualizando o status da tarefa

No menu Tarefas, clique em **Status**.

Nota: O status da tarefa é atualizado em tempo real.

Interrupção de tarefas

1. No menu Tarefas, clique em **Status**.
2. Na seção Tarefas em execução, selecione uma ou mais tarefas.
3. Clique em **Parar**.

Exibindo registros

1. No menu Tarefas, clique em **Registros**.
2. Selecione categorias da tarefa, tipos da tarefa, ou um período de tempo.

   Notas:

   - Use o campo de pesquisa para pesquisar vários IDs de tarefas. Use vírgulas para separar diversos IDs de tarefas ou um hífen para indicar um intervalo. Por exemplo, **`11, 23, 30-35`**.
   - Para exportar os resultados de pesquisa, clique em **Exportar para CSV**.

Limpando registros

1. No menu Tarefas, clique em **Registro**.
2. Clique em **Limpar registro** e, em seguida, selecione uma data.
3. Clique em **Limpar registro**.

Exportando registros

1. Na pasta Tarefas menu, clique em **Registro**.
2. Selecione categorias da tarefa, tipos da tarefa, ou um período de tempo.
3. Clique em **Exportar para CSV**.

Programação de tarefas

Como criar uma programação

1. No menu Tarefas, clique em **Programar** > **Criar**.
2. Na seção Geral, digite um nome exclusivo para as tarefas programadas e sua descrição.
3. Na seção Tarefa , execute um dos seguintes procedimentos:

Programar uma auditoria

a. Selecione **Auditar**.
b. Selecione uma pesquisa salva.

Programar uma verificação de conformidade

a. Selecione **Conformidade**.
b. Selecione uma pesquisa salva.

Programar uma verificação de status da impressora

a. Selecione **Estado atual**.
b. Selecione uma pesquisa salva.
c. Selecionar uma ação.

Programar uma implantação de configuração

a. Selecione **Implantar arquivo**.
b. Selecione uma pesquisa salva.
c. Vá até o arquivo e selecione o tipo de arquivo.
d. Se necessário, selecione um método ou protocolo de implantação.

Programar descoberta

a. Selecione **Descoberta**.
b. Selecione um perfil de descoberta.

Programar uma aplicação de configuração

a. Selecione **Aplicação**.
b. Selecione uma pesquisa salva.

Programe uma validação de certificado

Selecione **Validar certificado**.

Nota: Durante a validação, o MVE comunica-se com o servidor CA para baixar a cadeia de certificados e a Lista de revogação de certificados (CRL). O certificado do agente de inscrição também é gerado. Esse certificado permite que o servidor CA confie no MVE.

Programar uma exportação de exibição

a Selecione **Exportar exibição**.

b Selecione uma pesquisa salva.

c Selecione um modelo de exibição.

d Digite a lista de endereços de e-mail para os quais os arquivos exportados serão enviados.

4 Na seção Programar, defina data, hora e frequência da tarefa.

5 Clique em **Criar tarefa programada**.

Gerenciando tarefas programadas

1 Na pasta Tarefas menu, clique em **Programar**.

2 Execute um dos seguintes procedimentos:

Editar tarefa programada

a Selecione uma tarefa e clique em **Editar**.

b Configure as definições.

c Clique em **Editar tarefa programada**.

Nota: As informações da última execução são removidas quando uma tarefa programada é editada.

Exclua uma tarefa programada

a Selecione uma tarefa e clique em **Excluir**.

b Clique em **Excluir tarefa programada**.

Execução de outras tarefas administrativas

Configurando as definições gerais

1. Clique em no canto superior direito da página.
2. Clique em **Geral**e selecione uma origem de nome do host.
   - **Impressora**—O sistema recupera o nome do host da impressora.
   - **Pesquisa de DNS reverso**—O sistema recupera o nome do host a partir da tabela de DNS utilizando o endereço IP.
3. Definir a frequência de registro do alerta.

   Nota: Impressoras podem perder o estado de registro de alerta quando ocorrem alterações, como reiniciar ou atualizar o firmware. O MVE tenta recuperar o estado automaticamente no próximo intervalo definido na frequência de registro de alerta.
4. Clique em **Salvar alterações**.

Definição das configurações de e-mail

Ative a configuração de SMTP para que o MVE envie arquivos de exportação de dados e notificações de eventos por e-mail.

1. Clique em no canto superior direito da página.
2. Clique em **E-mail**e selecione **Ativar configuração SMTP de e-mail**.
3. Digite o servidor e a porta de e-mail SMTP.
4. Selecione a criptografia adequada.

   Notas:

   - Para criptografia SSL, selecione a porta 465.
   - Para criptografia TLS/STARTTLS, selecione a porta 587.
5. Digite o endereço de e-mail do remetente.
6. Se um usuário precisar efetuar login antes de enviar e-mails, selecione **Login necessário** e digite as credenciais do usuário.
7. Clique em **Salvar alterações**.

Adição de isenção de responsabilidade no login

É possível configurar uma isenção de responsabilidade no login para ser exibida quando usuários efetuarem login em uma nova sessão. Os usuários devem aceitar a isenção de responsabilidade antes de acessar o MVE.

1. Clique em no canto superior direito da página.
2. Clique em **Isenção de responsabilidade**e selecione **Ativar isenção de responsabilidade antes de efetuar login**.
3. Digite o texto de isenção de responsabilidade.
4. Clique em **Salvar alterações**.

Assinatura do certificado do MVE

O SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) é um protocolo de segurança que usa criptografia de dados e autenticação de certificado para proteger a comunicação entre servidor e cliente. No MVE, o TLS é usado para proteger informações confidenciais compartilhadas entre o servidor MVE e o navegador da Web. As informações protegidas podem ser senhas da impressora, políticas de segurança, credenciais de usuário do MVE ou informações de autenticação da impressora, como LDAP ou Kerberos.

O TLS permite que o servidor MVE e o navegador da Web criptografem os dados antes de enviá-los e os descriptografem após serem recebidos. O SSL também requer que o servidor apresente um certificado ao navegador da Web comprovando que o servidor é quem realmente diz ser. Esse certificado é autoassinado ou assinado usando uma CA confiável de terceiros. Por padrão, o MVE está configurado para usar o certificado autoassinado.

1. Faça download da solicitação de assinatura do certificado.
   a. Clique em no canto superior direito da página.
   b. Clique em **TLS** > **Download**.
   c. Selecione **Solicitação de assinatura do certificado**.

   Nota: A solicitação de assinatura do certificado inclui Nomes de assuntos alternativos (SAN).
2. Use uma CA confiável para assinar a solicitação de assinatura do certificado.
3. Instale o certificado assinado pela CA.
   a. Clique em no canto superior direito da página.
   b. Clique em **TLS** > **Instalar o certificado assinado**.
   c. Faça upload do certificado assinado pela CA e clique em **Instalar o certificado**.
   d. Clique em **Reiniciar o serviço MVE**.

      Nota: Reiniciar o serviço MVE reinicia o sistema, e o servidor pode ficar indisponível durante alguns minutos. Antes de reinicializar o serviço, certifique-se de que não haja tarefas em execução no momento.

Removendo informações e referências de usuário

O MVE está em conformidade com as regras de proteção de dados do Regulamento Geral de Proteção de Dados (GDPR). O MVE pode ser configurado para aplicar o direito de ser esquecido e de remover do sistema informações privadas de usuário.

Removendo usuários

1. Clique em no canto superior direito da página.
2. Clique em **Usuário** e selecione um ou mais usuários.
3. Clique em **Excluir** > **Excluir usuários**.

Removendo referências de usuário no LDAP

1. Clique em no canto superior direito da página.
2. Clique em **LDAP**.
3. Remova todas as informações relacionadas ao usuário nos filtros de pesquisa e nas definições de vinculação.

Removendo referências de usuário no servidor de e-mail

1. Clique em no canto superior direito da página.
2. Clique em **E-mail**.
3. Remova todas as informações relacionadas ao usuário, como credenciais usadas para autenticação com o servidor de e-mail.

Removendo referências de usuário nos registros de tarefas

Para obter mais informações, consulte " Limpando registros" na página 143.

Removendo referências de usuário em uma configuração

1. No menu Configurações, clique em **Todas as configurações**.
2. Clique no nome da configuração.
3. Na guia Básico, remova todos os valores relacionados ao usuário das definições da impressora, como nome e localização de contato.

Removendo referências de usuário em um componente de segurança avançada

1. No menu Configurações, clique em **Todos os componentes de segurança avançada**.
2. Clique no nome do componente.
3. Na seção Definições de segurança avançada, remova todos os valores relacionados ao usuário.

Removendo referências de usuário em pesquisas salvas

1. No menu Impressoras, clique em **Pesquisas salvas**.
2. Clique em uma pesquisa salva.
3. Remova qualquer critério de pesquisa que use valores relacionados ao usuário, como nome e localização do contato.

Removendo referências de usuário em palavras-chave

1. No menu Impressoras, clique em **Listagem de impressoras**.
2. Remova a atribuição de palavras-chave relacionadas ao usuário das impressoras.
3. No menu Impressoras, clique em **Palavras-chave**.
4. Remova qualquer palavra-chave que use informações relacionadas ao usuário.

Removendo referências de usuário em eventos e ações

1. No menu Impressoras, clique em **Eventos e Ações**.
2. Remova todas as ações que contenham referências de e-mail de usuários.

Perguntas frequentes

Perguntas frequentes do Markvision Enterprise

Por que não posso escolher várias impressoras na lista de modelos compatíveis ao criar uma configuração?

As configurações e os comandos de configuração diferem entre os modelos das impressoras.

Outros usuários podem acessar minhas pesquisas salvas?

Sim. Todos os usuários podem acessar pesquisas salvas.

Onde posso encontrar os arquivos de registro?

Você pode encontrar os arquivos de registro de instalação no diretório oculto do usuário que está instalando o MVE. Por exemplo, **C:\Users\Administrator\AppData\Local\Temp\mveLexmark-install.log**.

É possível encontrar os arquivos de registro do aplicativo ***.log** na pasta ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\logs**, na qual ***installation_dir*** é a pasta de instalação do MVE.

Qual a diferença entre nome do host e pesquisa de DNS reverso?

O nome do host é um nome exclusivo atribuído a uma impressora em uma rede. Cada nome de host corresponde a um endereço IP. A pesquisa de DNS reverso é usada para determinar o nome do host designado e o nome de domínio de um determinado endereço IP.

Onde posso encontrar pesquisa de DNS reverso no MVE?

A pesquisa de DNS reverso pode ser encontrada nas configurações gerais. Para mais informações, consulte " Configurando as definições gerais" na página 147.

Como adicionar regras ao firewall do Windows manualmente?

Execute o prompt de comando como administrador e digite o seguinte:

```
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"
```

Onde ***installation_dir*** é a pasta de instalação do MVE.

Como configuro o MVE para usar uma porta diferente da porta 443?

1. Encerre o serviço do Markvision Enterprise.
   a. Abra a caixa de diálogo Executar e digite **services.msc**.
   b. Clique com o botão direito em **Markvision Enterprise**e, em seguida, clique em **Parar**.

2 Abra o arquivo ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Onde ***installation_dir*** é a pasta de instalação do MVE.

3 Altere o valor de **Porta do conector** para outra porta não utilizada.

```
<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 Altere o valor de **redirectPort** para o mesmo número de porta usado como a porta do conector.

```
<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 Reinicie o serviço do Markvision Enterprise.

a Abra a caixa de diálogo Executar e digite **services.msc**.

b Clique com o botão direito em **Markvision Enterprise** e, em seguida, clique em **Reiniciar**.

6 Acesse o MVE usando a nova porta.

Por exemplo, abra um navegador da Web e digite **https://*MVE_SERVER*:*port*/mve**.

Em que ***MVE_SERVER*** é o nome do host ou endereço IP do servidor que hospeda o MVE e ***port*** é o número da porta do conector.

Como personalizo a criptografia e as versões de TLS que o MVE usa?

1 Encerre o serviço do Markvision Enterprise.

a Abra a caixa de diálogo Executar e digite **services.msc**.

b Clique com o botão direito em **Markvision Enterprise**e, em seguida, clique em **Parar**.

2 Abra o arquivo ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Onde ***installation_dir*** é a pasta de instalação do MVE.

3 Configure a criptografia e as versões do TLS.

Para obter mais informações sobre a configuração, consulte as **instruções de configuração do Apache Tomcat SSL/TLS**.

Para obter mais informações sobre os protocolos e valores de criptografia, consulte a **documentação de informações de suporte ao Apache Tomcat SSL**.

4 Reinicie o serviço do Markvision Enterprise.

a Abra a caixa de diálogo Executar e digite **services.msc**.

b Clique com o botão direito em **Markvision Enterprise** e, em seguida, clique em **Reiniciar**.

Como gerenciar arquivos CRL ao usar o Microsoft CA Enterprise?

1. Obtenha o arquivo CRL do servidor CA.

   Notas:

   - Para o Microsoft CA Enterprise, o CRL não é baixado automaticamente por meio do SCEP.
   - Para obter mais informações, consulte o *Guia de configuração da autoridade de certificações da Microsoft*.

2. Salve o arquivo CRL na pasta ***installation_dir*\Lexmark\Markvision Enterprise\apps\library\crl** em que ***installation_dir*** é a pasta de instalação do MVE.
3. Configure a autoridade de certificado no MVE.

Nota: Esse processo é aplicável apenas para o uso do Protocolo de Inscrição de Certificado Simples (SCEP).

Solução de problemas

O usuário esqueceu a senha

Redefinir a senha do usuário

Você precisa ter direitos administrativos para reconfigurar a senha.

1. Clique em no canto superior direito da página.
2. Clique em **Usuário**e selecione um usuário.
3. Clique em **Editar**e altere a senha.
4. Clique em **Salvar alterações**.

Se você esqueceu a senha, faça uma das opções seguintes:

- Entre em contato com outro usuário Admin para redefinir sua senha.
- Entre em contato com o Centro de suporte ao cliente Lexmark.

O usuário Administrador esqueceu a senha

Crie outro usuário Administrador e, em seguida, exclua a conta anterior

Você pode usar o Utilitário de senha do Markvision Enterprise para criar outro usuário Administrador.

1. Navegue até a pasta onde o Markvision Enterprise está instalado.
   Por exemplo, **`C:\Arquivos de Programas\`**
2. Inicie o arquivo **mvepwdutility-windows.exe** no diretório Lexmark\Markvision Enterprise\.
3. Selecione um idioma e clique em **OK** > **Avançar**.
4. Selecione **Adicionar conta de usuário** > **Avançar**.
5. Insira as credenciais de usuário.
6. Clique em **Avançar**.
7. Acesse o MVE e exclua o usuário Administrador anterior.

   Nota: Para obter mais informações, consulte " Gerenciamento de usuários" na página 30.

A página não carrega

Esse problema pode ocorrer se você tiver fechado o navegador da Web sem fazer logout.

Experimente uma ou mais das seguintes opções:

Limpe o cache e exclua os cookies no navegador da Web

Acesse a página de login do MVE e, em seguida, faça login usando suas credenciais

Abra um navegador da Web e digite **`https://MVE_SERVER/mve/login`**, onde ***`MVE_SERVER`*** é o nome do host ou o endereço IP do servidor que hospeda o MVE.

Não é possível detectar uma impressora de rede

Experimente uma ou mais das seguintes opções:

Verificar se a impressora está ligada

Verificar se o cabo de alimentação está conectado na impressora e em uma tomada elétrica devidamente aterrada

Verifique se a impressora está conectada à rede

Reinicie a impressora

Verifique se o TCP/IP está ativado na impressora

Verifique se as portas usadas pelo MVE estão abertas, e se o SNMP e mDNS estão ativados

Para obter mais informações, consulte " Portas e protocolos" na página 160.

Entre em contato com o seu representante da Lexmark

Informações incorretas de impressora

Realize uma auditoria

Para obter mais informações, consulte " Auditando impressoras" na página 61.

O MVE não reconhece uma impressora como segura

Verifique se a impressora é segura

Para obter mais informações sobre como proteger impressoras, consulte o documento *Markvision Enterprise e Segurança da Impressora*.

Certifique-se de que o mDNS esteja ativado e não esteja bloqueado

Exclua a impressora e execute novamente a descoberta de impressoras

Para obter mais informações, consulte " Descoberta de impressoras" na página 34.

A aplicação de configurações com vários aplicativos falha na primeira tentativa, mas é bem-sucedida nas tentativas seguintes

Aumente os tempos limite

1. Navegue até a pasta onde o Markvision Enterprise está instalado.

   Por exemplo, **`C:\Arquivos de Programas\`**
2. Navigate to the Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes folder.
3. Abra o arquivo *platform.properties* usando um editor de texto.
4. Edite o valor **`cdcl.ws.readTimeout`**.

   Nota: O valor está em milissegundos. Por exemplo, 90000 milissegundos é igual a 90 segundos.
5. Abra o arquivo *devCom.properties* usando um editor de texto.
6. Edite os valores **`lst.responseTimeoutsRetries`**.

   Nota: O valor está em milissegundos. Por exemplo, 10000 milissegundos é igual a 10 segundos.

   Por exemplo, **`lst.responseTimeoutsRetries=10000 15000 20000`**. A primeira tentativa de conexão ocorre após 10 segundos, a segunda tentativa de conexão ocorre após 15 segundos e a terceira tentativa de conexão ocorre após 20 segundos.
7. Se necessário, ao usar o LDAP GSSAPI, crie um arquivo *parameters.properties*.

   Insira a seguinte definição: **`lst.negotiation.timeout=400`**

   Nota: O valor está em segundos.
8. Salve as alterações.

Falha na aplicação de configurações com certificado da impressora

Às vezes, nenhum novo certificado é emitido durante a aplicação.

Aumente o número de novas tentativas de inscrição

Adicione a seguinte chave no arquivo **platform.properties**:

```
enrol.maxEnrolmentRetry=10
```

O valor da nova tentativa deve ser maior que cinco.

Autoridade de certificações OpenXPKI

A emissão de certificado falhou ao usar o servidor OpenXPKI CA

Certifique-se de que a chave "signatário em nome" no MVE corresponda à chave do signatário autorizada no servidor CA

Por exemplo:

Se a opção a seguir for a chave **ca.onBehalf.cn** no arquivo **platform.properties** no MVE,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

depois, a opção a seguir deve ser a chave **authorized_signer** no arquivo **generic.yaml** no servidor CA.

```
rule1:
            # Full DN
                    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

Para obter mais informações sobre como configurar o servidor OpenXPKI CA, consulte o *Guia de configuração da autoridade de certificações do OpenXPKI*.

Ocorre um erro interno do servidor

Instale o local en_US.utf8

1. Execute o comando **`dpkg-reconfigure locales`**.
2. Instale o local **en_US.utf8** (locale -a | grep en_US).

O prompt de login não é exibido

Ao acessar **http://yourhost/openxpki/**, você obtém apenas o banner do Open Source Trustcenter, sem um prompt de login.

Ative o `fcgid`

Execute os seguintes comandos:

1. **`a2enmod fcgid`**
2. **`service apache2 restart`**

Ocorre um erro de conector aninhado sem classe

Um erro **`EXCEÇÃO: Conector aninhado sem classe (scep.scep-server-1.connector.initial)`** aparece em /usr/share/perl5/Connector/Multi.pm, na linha 201.

Atualizar `scep.scep-server-1`

Em **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, substitua **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Substitua **`REALM`** pelo nome do realm. Por exemplo, ao usar o realm padrão, use **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Não é possível aprovar certificados manualmente

O botão Aprovação manual não aparece ao aprovar certificados manualmente.

Atualizar `scep.scep-server-1`

Em **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, substitua **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Substitua **`REALM`** pelo nome do realm. Por exemplo, ao usar o realm padrão, use **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Um erro de Perl ocorre ao aprovar solicitações de inscrição

Atualizar `scep.scep-server-1`

Em **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, substitua **`scep.scep-server-1`** por **`scep.generic`**.

Nota: Substitua **`REALM`** pelo nome do realm. Por exemplo, ao usar o realm padrão, use **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Os tokens `ca-signer-1` e `vault-1` estão off-line

A página Status do sistema mostra que os tokens **`ca-signer-1`** e **`vault-1`** estão off-line.

Experimente uma ou mais das seguintes opções:

Alterar a senha da chave do certificado

Em **/etc/openxpki/config.d/realm/ca-one/crypto.yaml**, altere a senha da chave do certificado.

Crie links simbólicos corretos e copie o arquivo de chave

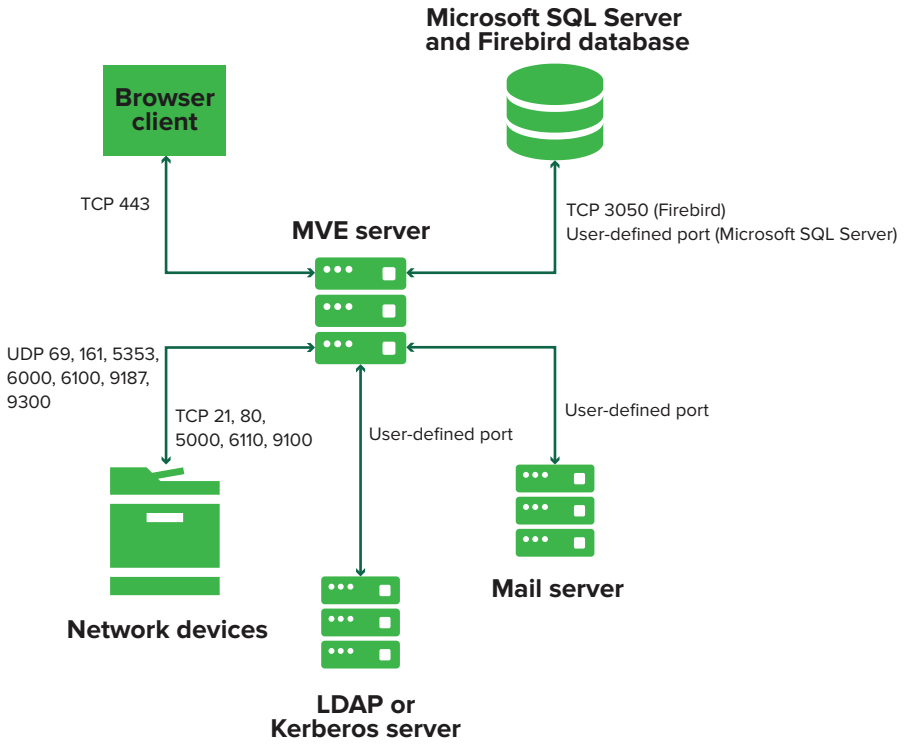
Para mais informações, consulte " Cópia de arquivos de chaves e criação de symlinks" na página 106.

Verifique se o arquivo de chave pode ser lido pelo OpenXPKI

Apêndice

Portas e protocolos

O MVE usa diferentes portas e protocolos para os vários tipos de comunicação de rede, conforme mostrado no diagrama a seguir:



Notas:

- As portas são bidirecionais e devem estar abertas ou ativadas para o MVE funcionar corretamente. Certifique-se de que todas as portas da impressora estão ativadas.
- Algumas comunicações requerem uma porta efêmera alocado, que é um intervalo de portas disponíveis alocado no servidor. Quando um cliente solicita uma sessão de comunicação temporária, o servidor atribui uma porta dinâmica ao cliente. A porta é válida apenas por uma curta duração e pode ficar disponível para reutilização quando a sessão anterior expirar.

Comunicação entre servidor e impressora

Portas e protocolos usados durante a comunicação entre o Servidor do MVE e impressoras de rede

Protocolo	Servidor MVE	Impressora	Usado para
Network Printing Alliance Protocol (NPAP)	UDP 9187	UDP 9300	Comunicando com impressoras de rede da Lexmark.
XML Network Transport (XMLNT)	UDP 9187	UDP 6000	Comunicando com algumas impressoras de rede da Lexmark.
Lexmark Secure Transport (LST)	UDP 6100 Portas efêmera TCP (Transmission Control Protocol) (saudação)	UDP 6100 TCP 6110 (saudação)	Comunicando de forma segura com algumas impressoras de rede da Lexmark.
Multicast Domain Name System (mDNS)	Porta efêmera UDP (User Datagram Protocol)	UDP 5353	Localizando impressoras de rede da Lexmark e determinando recursos de segurança de impressoras. **Nota:** Essa porta será necessária para permitir que o MVE se comunique com impressoras protegidas.
Simple Network Management Protocol (SNMP)	Porta UDP efêmera	UDP 161	Localizando e comunicando com impressoras de rede de terceiros e da Lexmark.
FTP (File Transfer Protocol)	Porta TCP efêmera	TCP 21 TCP 20	Implementando arquivos.
Hypertext Transfer Protocol (HTTP)	Porta TCP efêmera	TCP 80	Implementando arquivos ou aplicando configurações.
		TCP 443	Implementando arquivos ou aplicando configurações.
Hypertext Transfer Protocol sobre SSL (HTTPS)	Porta TCP efêmera	TCP 161 TCP 443	Implementando arquivos ou aplicando configurações.
RAW	Porta TCP efêmera	TCP 9100	Implementando arquivos ou aplicando configurações.

Comunicação entre servidor e impressora

Porta e o protocolo usados durante a comunicação entre as impressoras de rede e o servidor MVE

Protocolo	Impressora	Servidor MVE	Usado para
NPAP	UDP 9300	UDP 9187	Recepção e geração alertas

Comunicação entre servidor e banco de dados

Portas usadas durante a comunicação entre o servidor MVE e os bancos de dados

Servidor MVE	Banco de dados	Usado para
Porta TCP efêmera	Porta definida pelo usuário. A porta padrão é TCP 1433.	Comunicando com um banco de dados do SQL Server.
Porta TCP efêmera	TCP 3050	Comunicando com um banco de dados Firebird.

Comunicação entre servidor e cliente

Porta e protocolo usados durante a comunicação entre o cliente browser e o servidor MVE

Protocolo	Cliente browser	Servidor MVE
Hypertext Transfer Protocol sobre SSL (HTTPs)	Porta TCP	TCP 443

Comunicação entre o servidor e o servidor de e-mail

Porta e protocolo usados durante a comunicação entre o servidor MVE e o servidor de e-mails

Protocolo	Servidor MVE	Servidor SMTP	Usado para
Simple Mail Transfer Protocol (SMTP)	Porta TCP efêmera	Porta definida pelo usuário. A porta padrão é TCP 25.	Fornecimento da funcionalidade de e-mail usada para receber alertas de impressoras.

Comunicação entre o servidor e o servidor de LDAP

Portas e protocolos usados durante a comunicação entre o servidor MVE em um servidor LDAP envolvendo grupos de usuário e a funcionalidade de autenticação

Protocolo	Servidor MVE	Servidor LDAP	Usado para
Lightweight Directory Access Protocol (LDAP)	Porta TCP efêmera	Porta definida pelo usuário. A porta padrão é TCP 389.	Autenticando usuários MVE usando um servidor LDAP.
Lightweight Directory Access Protocol no TLS (LDAPS)	Porta TCP efêmera	Porta definida pelo usuário. A porta padrão é TCP 636.	Autenticando usuários MVE usando um servidor LDAP no TLS.
Kerberos	Porta UDP efêmera	Porta definida pelo usuário. A porta padrão é UDP 88.	Autenticando usuários MVE usando Kerberos.

Ativação da aprovação automática de solicitações de certificado no Microsoft CA

Por padrão, todos os servidores CA estão no modo pendente e você deve aprovar manualmente a solicitação de cada certificado assinado. Como esse método não é viável para solicitações em massa, ative a aprovação automática de certificados assinados.

1. No Gerenciador de servidores, clique em **Ferramentas > Autoridade de certificação**.
2. No painel esquerdo, clique com o botão direito na CA e, em seguida, clique em **Propriedades > Módulo de política**.
3. Na guia Tratamento de solicitação, clique em **Seguir as configurações no modelo de certificado, se aplicável** e clique em **OK**.

   Nota: Se a opção **Definir o status da solicitação de certificado como pendente** estiver selecionada, você deverá aprovar manualmente o certificado.
4. Reinicie o serviço CA.

Revogação de certificados

Nota: Antes de começar, verifique se o servidor CA está configurado para CRLs e se estão disponíveis.

1. No servidor CA, abra **Autoridade de certificação**.
2. No painel esquerdo, expanda a CA e clique em **Certificados emitidos**.
3. Clique com o botão direito em um certificado para revogá-lo e clique em **Todas as tarefas > Revogar certificado**.
4. Selecione um código de motivo e a data e hora da revogação e clique em **Sim**.
5. No painel esquerdo, clique com o botão direito em **Certificados revogados** e clique em **Todas as tarefas > Publicar**.

   Nota: Verifique se o certificado revogado está em Certificados revogados.

Você pode ver o número de série do certificado revogado na CRL.

Avisos

Aviso de edição

Setembro de 2022

O parágrafo a seguir não se aplica a países onde as cláusulas descritas não são compatíveis com a lei local: A LEXMARK INTERNATIONAL, INC. FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM QUALQUER TIPO DE GARANTIA, EXPRESSA OU TÁCITA, INCLUINDO, ENTRE OUTRAS, GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns estados não permitem a contestação de garantias expressas ou implícitas em certas transações. Conseqüentemente, é possível que esta declaração não se aplique ao seu caso.

É possível que esta publicação contenha imprecisões técnicas ou erros tipográficos. Serão feitas alterações periódicas às informações aqui contidas; essas alterações serão incorporadas em edições futuras. Alguns aperfeiçoamentos ou alterações nos produtos ou programas descritos poderão ser feitos a qualquer momento.

As referências feitas nesta publicação a produtos, programas ou serviços não implicam que o fabricante pretenda torná-los disponíveis em todos os países nos quais opera. Qualquer referência a um produto, programa ou serviço não tem a intenção de afirmar ou sugerir que apenas aquele produto, programa ou serviço possa ser usado. Qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja qualquer direito de propriedade intelectual existente poderá ser usado no seu lugar. A avaliação e verificação da operação em conjunto com outros produtos, programas ou serviços, exceto aqueles expressamente designados pelo fabricante, são de responsabilidade do usuário.

Para suporte técnico da Lexmark, vá até **http://support.lexmark.com**.

Para informações sobre a política de privacidade da Lexmark que rege o uso deste produto, vá até **www.lexmark.com/privacy**.

Para informações sobre suprimentos e downloads, vá até **www.lexmark.com**.

© **2017 Lexmark International, Inc.**

Todos os direitos reservados.

Marcas comerciais

Lexmark, o logotipo Lexmark e Markvision são marcas comerciais ou marcas registradas da Lexmark International, Inc. nos Estados Unidos e/ou em outros países.

Windows, Microsoft, Microsoft Edge, PowerShell, SQL Server e Windows Server são marcas comerciais do grupo de empresas Microsoft.

Firebird é uma marca registrada da Firebird Foundation.

Google Chrome é uma marca comercial da Google LLC.

Apple and Safari are registered trademarks of Apple Inc.

Java é uma marca registrada da Oracle e/ou suas afiliadas.

Todas as outras marcas comerciais pertencem a seus respectivos proprietários.

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 Commerical 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

Avisos de licença

Todos os avisos de licenciamento associados a este produto podem ser encontrados na pasta do programa.

Glossário

ação Uma notificação de e-mail ou uma operação de linha de comando. Ações atribuídas a eventos são acionadas quando ocorre um alerta da impressora.

auditoria A tarefa de coletar dados da impressora, como status, suprimentos e recursos.

configuração Um conjunto de configurações que podem ser atribuídas e aplicadas a uma impressora ou grupo de modelos de impressoras. Em uma configuração, é possível modificar as configurações da impressora e implantar aplicativos, licenças, firmware e certificados CA às impressoras.

configurações variáveis Um conjunto de configurações da impressora contendo valores dinâmicos que podem se integrar a uma configuração.

evento Define quais ações executar quando alertas específicos estão ativos.

impressora protegida Uma impressora configurada para se comunicar por um canal criptografado e que requer autenticação para o acesso das suas funções ou aplicativos.

palavra-chave Um texto personalizado atribuído às impressoras que pode ser usado para procurar essas impressoras no sistema. Quando você filtra uma pesquisa usando uma palavra-chave, somente as impressoras marcadas com a palavra-chave são exibidas.

perfil de descoberta Um perfil que contém um conjunto de parâmetros usados para localizar impressoras em uma rede. Também pode conter configurações predefinidas que podem ser atribuídas e aplicadas às impressoras automaticamente durante a descoberta.

token Um identificador que representa valores de dados da impressora para configurações variáveis em uma configuração.

Índice

A

a aplicação de configurações com vários aplicativos falha na primeira tentativa, mas é bem-sucedida nas tentativas seguintes 156
ação
  espaços reservados 136
ação de e-mail 135
ação de evento de registro 135
acessibilidade de CRL
  configuração 85, 108
Acesso a informações da autoridade
  configuração 84
acesso ao MVE 23
ações
  criação 135
  edição 137
  exclusão 137
  gerenciamento 137
  teste 137
adição de alertas de login 148
adição de EKU de autenticação de cliente em certificados 115
a emissão de certificado falhou ao usar o servidor OpenXPKI CA 157
AIA
  configuração 84
alertas da impressora
  noções básicas 138
alteração das configurações do instalador após a instalação 28
alteração da senha 24
alteração da visualização da listagem de impressoras 46
a página fica carregando infinitamente 155
aplicação de configurações 62
aplicativos
  desinstalação 65
aprovação automática de solicitações de certificado
  ativação no Microsoft CA 163
  ativação no OpenXPKI CA 110, 128
arquivo de configuração OpenSSL
  criação 103, 121
arquivos
  implementação 63
arquivos de chaves
  cópia 106
arquivos de registro
  localização 151
arquivos de registro de instalação
  localização 151
arquivos de registro do aplicativo
  localização 151
arquivos de senha para chaves de certificado
  criação 104, 122, 130
assinatura do certificado do MVE 148
ativação da aprovação automática de solicitações de certificado na CA da Microsoft 163
ativação da aprovação automática de solicitações de certificado no OpenXPKI CA 110
ativação da autenticação do servidor LDAP 31
ativação de certificados Signatário em nome de 109
ativação de vários certificados ativos
  mesma entidade 114
ativação do serviço SCEP 109
atribuição de configurações às impressoras 62
atribuição de eventos às impressoras 65
atribuição de palavras-chave 65
atualização do firmware da impressora 64
atualização do status da impressora 61
auditoria de impressoras 61
autenticação
  certificado do cliente 91
  integrada do Windows 91
  nome de usuário e senha 91
autenticação básica
  ativação 132, 133
autenticação de nome de usuário e senha 91
autenticação do certificado do cliente 91
autenticação integrada do Windows 91
aviso de login
  adição 148

B

backup e restauração do banco de dados 26
banco de dados
  backup 26
  configuração 19
  requisitos 15
  restauração 26
banco de dados Firebird 19
bancos de dados suportados 15
barra de pesquisa
  filtragem de impressoras 46
biblioteca de recursos
  importação de arquivos para 75

C

cancelamento da atribuição de configurações 62
ca-signer-1 está off-line
  solução de problemas 159
CDP
  configuração 84
cenário de exemplo para configurações de clonagem 71
CEP
  configuração 93, 95, 97
  instalação 92
certificado da web
  criação 124
certificado do cliente 96
certificado MVE
  assinatura 148
certificados
  criação 111, 130
  importação 107
  revogação 116, 163

certificados CA raiz
  criação 104, 123
certificados com o mesmo assunto
  ativação 131
certificados da impressora
  configuração manual 66
certificados de servidor LDAP
  instalação 33
certificados do signatário
  criação 105, 123, 130
certificados do vault
  criação 105, 124
Certificados SCEP
  criação 106
certificados Signatário em nome de
  ativação 109
certificados SSL
  criação 89
CES
  configuração 94, 96, 98
  instalação 92
chaves de certificado
  criação de arquivos de senha 104, 122, 130
clonagem de configurações
  amostra de cenário 71
como alterar o idioma 24
componente de segurança avançada
  criação 72
comunicações da impressora
  proteção 59
configuração
  conformidade 63
  criação 68, 71
  exportação 74
  importação 74
configuração da acessibilidade da CRL 85, 108
configuração da segurança da impressora 59
configuração das permissões de impressão colorida 73
configuração da visualização padrão 44
configuração de endpoints EST para vários realms 129
configuração de endpoints SCEP para vários realms 113
configuração de modelos de certificado para NDES 87
configuração de servidores do Serviço de registro de dispositivo de rede 85
configuração de servidores NDES 85
configuração do banco de dados 19
configuração do CEP 93, 95, 97
configuração do CES 94, 96, 98
configuração do diretório 111, 129
configuração do estado da impressora 62
configuração do Microsoft Enterprise CA com NDES
  visão geral 80, 82
configuração do MVE como um usuário “executar como” 20
configuração do MVE para gerenciamento automatizado de certificados 78
configuração do OpenXPKI CA usando o script padrão 102, 119
configuração do servidor da web 124
configuração dos números de portas padrão para OpenXPKI CA 114
configuração manual do OpenXPKI CA 103, 120
configuração manual dos certificados da impressora 66
configurações
  aplicação 62
  atribuição 62
  cancelamento de atribuições 62
  gerenciamento 68
configurações de critérios de pesquisa
  noções básicas 51
configurações de e-mail
  configuração 147
configurações dinâmicas
  noções básicas 72
configurações do instalador
  alteração 28
configurações gerais
  configuração 147
configurações padrão 56
configurações variáveis
  noções básicas 72
conformidade
  verificação 63
controles de acesso a funções
  noções básicas 58
cópia de arquivos de chaves 106
cópia de diretórios 111
cópia de exibições 44
cópia de perfis de descoberta 36
cópia de pesquisas salvas 53
cópia do diretório 129
credenciais
  inserção 66
criação de ações 135
criação de arquivos de configuração OpenSSL 103
criação de arquivos de senha para chaves de certificado 104, 130
criação de certificados 111
criação de certificados CA raiz 104
criação de certificados de vault 105
criação de certificados do cliente 96
criação de certificados do signatário 105
criação de certificados SCEP 106
criação de certificados SSL
  servidores de CEP e CES 89
criação de componentes de segurança avançada a partir de uma impressora 72
criação de configurações 68
criação de configurações a partir de uma impressora 71
criação de eventos 137
criação de modelos de certificado 86, 90
criação de pacotes de aplicativos 74
criação de palavras-chave 47
criação de perfis de descoberta 34
criação de pesquisas salvas personalizadas 49
criação de programações 145
criação de symlinks 106

criptografia
personalização 151
criptografia AES256
configuração 151
critérios de pesquisa
operadores 51
parâmetros 51
CRL
publicação 116
CSV
configurações variáveis 72

D

dados da impressora
exportação 44
definição das configurações de Acesso a informações da autoridade 84
definição das configurações de e-mail 147
definição das configurações de Ponto de distribuição de certificação 84
definição das configurações gerais 147
definições de configuração
versão para impressão 72
delegação
ativação 92
requisitos 91
desativação da senha de desafio no servidor de CA da Microsoft 87
descoberta de impressoras 37
desinstalação de aplicativos das impressoras 65
diretório
cópia e configuração 129
download de ca-certs
alteração de detalhes para ativar 128

E

edição de ações 137
edição de exibições 44
edição de palavras-chave 47
edição de perfis de descoberta 36
edição de pesquisas salvas 53
edição de programações 146
EKU de autenticação de cliente
adição de certificados 115
Embedded Web Server
exibição 61
Endpoints SCEP
configuração para vários realms 113
entidades de certificado completo
solicitação pelo SCEP 115
erro de conector aninhado sem classe 158
erro de Perl 158
erro interno do servidor 157
espaços reservados 135
espaços reservados de ação
noções básicas 136
estado da impressora
configuração 62
estados de segurança da impressora
noções básicas 55
estados do ciclo de vida útil da impressora
noções básicas 47
evento
criação 137
eventos
atribuição 65
edição 142
exclusão 142
gerenciamento 142
exclusão de ações 137
exclusão de exibições 44
exclusão de palavras-chave 47
exclusão de perfis de descoberta 36
exclusão de pesquisas salvas 53
exclusão de programações 146
execução de perfis de descoberta 36
execução de pesquisas salva 49
exibições
cópia 44
edição 44
exclusão 44
gerenciamento 44
exportação de CSV
configurações variáveis 72
exportação de dados da impressora 44
exportação de registros 144

F

falha na aplicação de configurações com certificado da impressora 157
filtragem de impressoras usando a barra de pesquisa 46
Firewall do Windows
adição de regras 151
firmware da impressora
atualização 64
funções do usuário
noções básicas 29

G

geração de informações do CRL 108
gerenciamento automatizado de certificados
configuração 78
gerenciamento de ações 137
gerenciamento de certificados 76
gerenciamento de configurações 68
gerenciamento de eventos 142
gerenciamento de exibições 44
gerenciamento de palavras-chave 47
gerenciamento de perfis de descoberta 36
gerenciamento de pesquisas salvas 53
gerenciamento de programações 146
gerenciamento de usuários 30

H

habilitação da autenticação básica 132
histórico de alterações 8

I

idioma
alteração 24
idiomas
compatíveis 16
idiomas suportados 16
implementação de arquivos em impressoras 63

importação de arquivos para a biblioteca de recursos 75
importação de certificados 107
importação de CSV
configurações variáveis 72
importação ou exportação de configurações 74
impressora
conformidade 63
reinicialização 61
impressoras
auditoria 61
descoberta 37
eventos 65
filtragem 46
implementação de arquivos 63
proteção 56, 60
remoção 67
impressoras protegidas
autenticação 66
informação incorreta da impressora 155
informações da impressora
exibição 43
informações de CRL
geração 108, 126
publicação 127
Informações de segurança do dispositivo
gerenciamento 38
informações do usuário
remoção 149
inicialização do OpenXPKI 107
inserção de credenciais em impressoras protegidas 66
instalação de certificados de servidor LDAP 33
instalação de servidores CA raiz 81
instalação de servidores CA subordinados 83
instalação do MVE 20
instalação do OpenXPKI CA 99, 117
instalação silenciosa
MVE 21
instalação silenciosa do MVE 21
interrupção de tarefas 143

L

limpeza dos registros 143
lista de impressoras
exibição 40

M

Markvision Enterprise
noções básicas 12
métodos de autenticação 90
Microsoft Enterprise CA
configuração 151
Microsoft Enterprise CA com NDES
configuração 80, 82
Microsoft SQL Server 19
modelos de certificado 90
criação 86
modelos de certificado para NDES
configuração 87
modelos de impressora suportados 16
modelos suportados
configuração 151
monitoramento de impressoras 54
MVE
acesso 23
instalação 20
upgrade 25

N

não é possível aprovar certificados manualmente 158
não foi possível descobrir uma impressora de rede 155
navegadores da Web suportados 15
noções básicas sobre as funções de usuário 29
noções básicas sobre espaços reservados da ação 136
noções básicas sobre os alertas da impressora 138
noções básicas sobre os estados do ciclo de vida útil da impressora 47
números de porta padrão
configuração para OpenXPKI CA 114
mudança para OpenXPKI CA 131
Números de porta padrão OpenXPKI CA
alteração 131
números de porta padrão para OpenXPKI CA
alteração 131

O

obtenção de entidades de certificado completo ao solicitar pelo SCEP 115
O MVE não reconhece uma impressora como segura 156
OpenXPKI
inicialização 107, 126
OpenXPKI CA
configuração manual 103, 120
configuração usando o script padrão 102, 119
instalação 99, 117
o prompt de login não é exibido 158
o usuário administrador esqueceu a senha 154
o usuário esqueceu a senha 154

P

pacote de aplicativos
criação 74
painel
acesso 38
palavra-chave
atribuição 65
palavras-chave
criação 47
edição 47
exclusão 47
gerenciamento 47
perfil de descoberta
criação 34
perfis de descoberta
cópia 36
edição 36
exclusão 36
execução 36
gerenciamento 36
perguntas frequentes 134
Perguntas frequentes 134
permissões
noções básicas 58

permissões de impressão colorida
configuração 73
pesquisa de DNS reverso 151
pesquisa de nome do host
pesquisa reversa 151
pesquisa salva personalizada
criação 49
pesquisas salvas
acesso 151
cópia 53
edição 53
exclusão 53
execução 49
gerenciamento 53
Ponto de distribuição de certificação
configuração 84
portas
configuração 151
noções básicas 160
práticas recomendadas 13
programação
criação 145
programações
edição 146
exclusão 146
gerenciamento 146
proteção das comunicações da impressora no parque de impressão 59
proteção das impressoras 60
proteção das impressoras usando as configurações padrão 56
Protocolo de registro de certificado simples
ativação 109
protocolos
noções básicas 160
publicação do CRL 116

R

recurso de gerenciamento automático de certificados 76
registros
exibição 143
exportação 144
limpeza 143
reinicialização da impressora 61
rejeição de solicitações de certificado sem senha de desafio na CA do OpenXPKI 114
remoção de impressoras 67
remoção de informações e referências do usuário 149
requisitos
conectividade de rede 88
sistema 88
requisitos de banco de dados 15
requisitos de conectividade 88
requisitos de conectividade de rede 88
requisitos de delegação 91
requisitos de sistema 88
requisitos do servidor da Web 15
requisitos do sistema do usuário 15
revogação de certificados 116, 163

S

segurança da impressora
configuração 59
senha
alteração 24
reconfiguração 154
senha da chave de certificado
disponibilização para openXPKI 125
Senha de desafio
desativação no servidor Microsoft CA 87
Serviço SCEP
ativação 109
servidor da web
configuração 124
servidor da Web
requisitos 15
servidores CA raiz
instalação 81
servidores CA subordinados
instalação 83
servidores de CEP e CES
criação de certificados SSL 89
servidores do Serviço de registro de dispositivo de rede
configuração 85
Servidores NDES
configuração 85
servidores suportados 15
Servidor LDAP
ativação da autenticação 31
sistema do usuário
requisitos 15
sistemas operacionais suportados 15
solicitações de certificado no Microsoft CA
aprovação automática 163
solicitações de certificado no OpenXPKI CA
aprovação automática 110, 128
solicitações de certificado sem senha de desafio
rejeição na AC do OpenXPKI 114
solução de problemas
a aplicação de configurações com vários aplicativos falha na primeira tentativa, mas é bem-sucedida nas tentativas seguintes 156
a emissão de certificado falhou ao usar o servidor OpenXPKI CA 157
a página fica carregando infinitamente 155
ca-signer-1 está off-line 159
erro de conector aninhado sem classe 158
erro de Perl 158
erro interno do servidor 157
falha na aplicação de configurações com certificado da impressora 157
informação incorreta da impressora 155
não é possível aprovar certificados manualmente 158
não foi possível descobrir uma impressora de rede 155
O MVE não reconhece uma impressora como segura 156
o prompt de login não é exibido 158
o usuário administrador esqueceu a senha 154
o usuário esqueceu a senha 154
vault-1 está off-line 159
status da impressora
atualização 61

status da tarefa
  exibição 143
symlinks
  criação 106

T

tarefas
  interrupção 143
Terminais EST
  configuração para vários realms 129
teste de ações 137

U

upgrade para a versão mais recente do MVE 25
usuários
  adição 30
  edição 30
  exclusão 30
  gerenciamento 30
usuário “executar como”
  configuração 20

V

vários certificados ativos com o mesmo assunto
  ativação 131
vault-1 está off-line
  solução de problemas 159
verificação da conformidade da impressora com uma configuração 63
Verificação de conformidade do dispositivo
  gerenciamento 39
versões do TLS
  personalização 151
visão geral
  configuração do acesso do usuário 29
  configuração do servidor CA raiz 81
  configuração do servidor CA subordinado 83
  exibição do status e do histórico das tarefas 143
  gerenciamento de alertas da impressora 135
  gerenciamento de configurações 68
  Markvision Enterprise 12
  painel de segurança 38
visão geral da configuração do acesso do usuário 29
visão geral da configuração do servidor CA raiz 81
visão geral da configuração do servidor CA subordinado 83
visão geral do gerenciamento de alertas da impressora 135
visualização da lista de impressoras 40
visualização da listagem de impressoras
  alteração 46
visualização das informações da impressora 43
visualização do Embedded Web Server da impressora 61
visualização dos registros 143
visualização do status da tarefa 143
visualização do status e visão geral do histórico das tarefas 143