Markvision Enterprise

Version 4.2

Administratorhandbuch

September 2022 **www.lexmark.com**

Inhalt

Änderungsverlauf

August 2022

- Zusatzinformationen zu folgenden Themen:
  - Enrollment over Secure Transport (EST)-Protokoll, wie in RFC 7030 definiert
  - Sicherheits-Dashboard
  - Automatische Zuweisung von Schlüsselwörtern während der Erkennung
  - Unterstützung für E-Mails über SSL/TLS
  - Unterstützung für Windows Server 2022
- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Verwalten von Zertifikaten unter Verwendung von Microsoft CA über Microsoft Certificate Enrollment Web Services (MSCEWS)
  - Konfigurieren des OpenXPKI CA-Servers
  - Verwalten von MVE-Konfigurationen

März 2022

- Aktualisierte Informationen zu den unterstützten Druckermodellen.
- Zusätzliche Informationen zum Erstellen eines Clientzertifikats.

Mai 2021

- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Verwalten der Microsoft Certificate Authority (CA)
  - Konfigurieren von Markvision™ Enterprise (MVE) für die automatische Zertifikatsverwaltung
  - Konfigurieren der Microsoft Enterprise Certificate Authority (CA) unter Verwendung des Network Device Enrollment Service (NDES)
- Zusatzinformationen zu folgenden Themen:
  - Verwalten von Zertifikaten unter Verwendung von Microsoft CA über Microsoft Certificate Enrollment Web Services (MSCEWS)
  - Erstellen eines SSL-Zertifikats für Certificate Enrollment Policy Web Service-Server (CEP) und Certificate Enrollment Web Service-Server (CES)
  - Authentifizierungsmethoden für CEP und CES
  - Benanntes Gerätezertifikat

November 2020

- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Unterstützte Datenbanken

- Zusatzinformationen zu folgenden Themen:
  - Verwalten und Bereitstellen von Konfigurationen
  - Sichern und Wiederherstellen der Datenbank
  - Verwalten von Zertifikaten mit OpenXPKI und Microsoft Certificate Authority
- Zusätzlicher Support für Folgendes:
  - Verwalten und Bereitstellen von Konfigurationen für eine Gruppe von Druckermodellen
  - Erstellen benutzerdefinierter Datenbanknamen

Februar 2020

- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Unterstützte Server
  - Unterstützte Datenbanken
  - Gültiger MVE-Upgradepfad
- Zusatzinformationen zu folgenden Themen:
  - Anweisungen für Best Practices
  - Anweisungen zur Verwaltung automatisierter Zertifikate
  - Standardmäßige erweiterte Sicherheitskomponenten und deren Einstellungen
  - Andere Möglichkeiten zum Sichern von Druckern
  - Beispielszenarien

Juni 2019

- Aktualisierte Informationen zu folgenden Themen:
  - Fußnoten zu Druckermodellen hinzugefügt, für die Zertifikate erforderlich sind
  - Zuweisen von DBO-Rechten beim Einrichten der Datenbank
  - Gültiger Upgradepfad beim Upgrade auf Version 3.4
  - Dateien, die beim Sichern und Wiederherstellen der Datenbank benötigt werden
  - LDAP-Server-Authentifizierungseinstellungen
  - Zertifikatgültigkeitsstatus, Datumsangaben und Zeitzonenparameter werden den Einstellungen für Suchkriterien hinzugefügt.
  - Konfigurieren der Berechtigungen und Funktionszugriffssteuerungen in den Sicherheitseinstellungen des Druckers
  - Auswählen einer Firmware-Datei aus der Ressourcenbibliothek beim Aktualisieren der Druckerfirmware
  - Auswählen des Startdatums, der Start- und Pausenzeit sowie der Wochentage beim Aktualisieren der Druckerfirmware
  - Verwalten von Konfigurationen
- Zusatzinformationen zu folgenden Themen:
  - Bedeutung des Druckersicherheitsstatus
  - Konfigurieren erweiterter Sicherheitskomponenten
  - Erstellen einer erweiterten Sicherheitskomponente von einem Drucker
  - Erstellen einer druckbaren Version der Konfigurationseinstellungen
  - Hochladen einer Druckerflottenzertifizierungsstelle

  - Entfernen von Benutzerinformationen und Verweisen
  - Bedeutung von Berechtigungen und Funktionszugriffssteuerungen
  - Schritte zur Fehlerbehebung, wenn das Durchsetzen von Konfigurationen mit mehreren Anwendungen fehlschlägt
  - Schritte zur Fehlerbehebung, wenn ein Admin-Benutzer das Kennwort vergessen hat

August 2018

- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Einrichten der Datenbank
  - Aktualisieren auf MVE 3.3
  - Häufig gestellte Fragen
  - Erstellen einer Aktion
  - Erstellen eines Zeitplans
- Zusatzinformationen zu folgenden Themen:
  - Einrichten eines Dömänenbenutzerkontos
  - Exportieren von Protokollen
  - Schritte zur Fehlerbehebung, wenn MVE gesicherte Drucker nicht erkennt

Juli 2018

- Aktualisierte Informationen zur Aktualisierung auf MVE 3.2.

April 2018

- Aktualisierte Informationen zu folgenden Themen:
  - Unterstützte Druckermodelle
  - Einrichten der Datenbank
  - Sichern und Wiederherstellen von Datenbankdateien
  - Die URL für den Zugriff auf MVE
  - Grundlagen zu Variableneinstellungen
- Zusatzinformationen zu folgenden Themen:
  - Konfigurieren der Druckerzertifikate
  - Anhalten von Aufgaben
  - Aktualisieren der Druckerfirmware

September 2017

- Aktualisierte Informationen zu folgenden Themen:
  - Systemvoraussetzungen
  - Kommunikation zwischen MVE und den Formulardruckermodellen 2580, 2581, 2590 und 2591 von Lexmark™
  - Manuelles Verwerfen von Microsoft SQL Server-Datenbanken
  - Sichern und Wiederherstellen von Datenbankdateien

  - Erforderliche Sicherheitseinstellungen für Funktionszugriffssteuerungen beim Bereitstellen von Firmware- und Lösungsdateien für Drucker
  - Unterstützung für Lizenzen beim Bereitstellen von Anwendungen
  - Druckerwarnungen und die zugehörigen Maßnahmen
  - Druckerstatus automatisch wiederherstellen
  - Zuordnung von Ereignissen und Schlüsselwörtern

Juni 2017

- Erste Dokumentversion für MVE 3.0

Übersicht

Grundlagen zu Markvision Enterprise

Markvision Enterprise (MVE) ist ein webbasiertes Dienstprogramm zur Druckerverwaltung für IT-Mitarbeiter.

MVE ermöglicht das effiziente Verwalten einer großen Flotte von Druckern in einem Unternehmen mithilfe der folgenden Funktionen:

- Eine Druckerflotte suchen, organisieren und verfolgen. Sie können eine Druckerprüfung durchführen, um Daten wie Status, Einstellungen und Zubehör zu erfassen.
- Konfigurationen erstellen und Druckern zuweisen.
- Firmware, Druckerzertifikate, CA-Zertifikate und Anwendungen den Druckern bereitstellen.
- Druckerereignisse und Warnungen überwachen.

Dieses Dokument bietet Informationen zu Konfiguration und Verwendung der Anwendung sowie zur Fehlerbehebung dafür.

Dieses Dokument richtet sich an Administratoren.

Erste Schritte

Best Practices

In diesem Thema werden die empfohlenen Schritte beschrieben, um MVE bei der effektiven Verwaltung Ihrer Flotte zu verwenden.

1. Installieren Sie MVE in Ihrer Umgebung.
   a. Erstellen Sie einen Server mit der neuesten Windows Server-Umgebung.

      Verwandte Inhalte:
      Web-Server-Anforderungen

   b. Erstellen Sie ein Domänenbenutzerkonto, das keinen Administratorzugriff hat.

      Verwandte Inhalte:
      Einrichten einer Benutzeranmeldung

   c. Erstellen Sie eine Microsoft SQL Server-Datenbank, richten Sie die Verschlüsselung ein, und gewähren Sie dem neuen Benutzerkonto Zugriff auf die Datenbanken.

      Verwandte Inhalte:
      - **Datenbankanforderungen**
      - **Einrichten der Datenbank**

   d. Installieren Sie MVE unter Verwendung des Domänenbenutzerkontos und des SQL-Servers mit Windows-Authentifizierung.

      Verwandte Inhalte:
      Installation von MVE

2. Richten Sie MVE ein, und suchen und organisieren Sie dann Ihre Flotte.
   a. Signieren Sie das Serverzertifikat.

      Verwandte Inhalte:
      - **Signieren des MVE-Zertifikats**
      - **Einrichten von MVE zur automatischen Verwaltung von Zertifikaten**

   b. Richten Sie die LDAP-Einstellungen ein.

      Verwandte Inhalte:
      - **Aktivieren der LDAP-Serverauthentifizierung**
      - **Installieren von LDAP-Zertifikaten**

   c. Stellen Sie eine Verbindung mit einem E-Mail-Server her.

      Verwandte Inhalte:
      Konfigurieren der E-Mail-Einstellungen

   d. Suchen Sie Ihre Flotte.

      Verwandte Inhalte:
      Erkennen von Druckern

   e. Planen Sie Prüfungen und Statusaktualisierungen.

Verwandte Inhalte:

- **Überprüfen von Druckern**
- **Aktualisieren des Druckerstatus**

f Richten Sie grundlegende Einstellungen wie Kontaktnamen, Standorte, Asset-Tags und Zeitzonen ein.

g Organisieren Sie Ihre Flotte. Verwenden Sie Schlüsselwörter, zum Beispiel Standorte, um die Drucker zu kategorisieren.

Verwandte Inhalte:

- **Zuweisen von Stichwörtern zu Druckern**
- **Erstellen eines gespeicherten Suchvorgangs**

3 Sichern Sie Ihre Flotte.

a Sichern Sie den Druckerzugriff mit den standardmäßigen erweiterten Sicherheitskomponenten.

Verwandte Inhalte:

- **Sichern von Druckern unter Verwendung der Standardkonfigurationen**
- **Bedeutung von Berechtigungen und Funktionszugriffssteuerungen**
- **Andere Möglichkeiten, Ihre Drucker zu schützen**

b Erstellen Sie eine gesicherte Konfiguration, die Zertifikate enthält.

Verwandte Inhalte:

- **Erstellen einer Konfiguration**
- **Importieren von Dateien in die Ressourcenbibliothek**

c Setzen Sie die Konfiguration für Ihre aktuelle Flotte durch.

Verwandte Inhalte:

- **Zuweisen von Konfigurationen zu Druckern**
- **Durchsetzen von Konfigurationen**

d Planen Sie Durchsetzungen und Konformitätsprüfungen.

Verwandte Inhalte:

Erstellen eines Zeitplans

e Fügen Sie Konfigurationen zu Suchprofilen hinzu, um neue Drucker zu sichern.

Verwandte Inhalte:

Erstellen von Suchprofilen

f Signieren Sie Druckerzertifikate.

Verwandte Inhalte:

Signieren des MVE-Zertifikats

4 Halten Sie Ihre Firmware auf dem neuesten Stand.

Verwandte Inhalte:

Aktualisieren der Drucker-Firmware

5 Installieren und konfigurieren Sie Anwendungen.

Verwandte Inhalte:

- **Erstellen einer Konfiguration**
- **Importieren von Dateien in die Ressourcenbibliothek**

6 Überwachen Sie Ihre Flotte.

Verwandte Inhalte:

Erstellen eines gespeicherten Suchvorgangs

Systemvoraussetzungen

MVE ist wie ein Webserver installiert, auf den auf jedem Computer im Netzwerk über einen Web-Browser zugegriffen werden kann. MVE verwendet außerdem eine Datenbank zum Speichern von Informationen über die Druckerflotte. Folgende Listen stellen die Anforderungen für Web-Server, Datenbank und Benutzersystem dar:

Web-Server-Anforderungen

Prozessor	Mindestens 2 GHz Dual-Core-Prozessor mit Hyper-Threading Technology (HTT)
RAM	Mindestens 4 GB
Festplattenlaufwerk	Mindestens 60 GB

Hinweis: MVE Lexmark Document Distributor (LDD-) und das Gerätebereitstellungs-Dienstprogramm (DDU) können nicht auf demselben Server ausgeführt werden.

Unterstützte Server

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

  Hinweis: MVE unterstützt die Virtualisierung der unterstützten Server in einer lokalen Umgebung.

Datenbankanforderungen

Unterstützte Datenbanken

- Firebird® Datenbank (integriert)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

  Hinweis: Die empfohlene Mindestgröße der Datenbank beträgt 60 GB für die Zuteilung von 20 MB für FRAMEWORK und von 4,5 MB für MONITOR und QUARTZ. Weitere Informationen finden Sie unter "Einrichten der Datenbank" auf Seite 19.

Benutzer-Systemvoraussetzungen

Unterstützte Webbrowser

- Microsoft Edge
- Mozilla Firefox (neueste Version)
- Google Chrome™ (neueste Version)
- Apple Safari (neueste Version)

Bildschirmauflösung

Mindestens 1.280 x 768 Pixel

Unterstützte Sprachen

- Brasilianisches Portugiesisch
- English
- Französisch
- Deutsch
- Italienisch
- Vereinfachtes Chinesisch
- Spanisch

Unterstützte Druckermodelle

- 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]
- Lexmark Formulardrucker 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] Eine Aktualisierung des Druckerzertifikats ist erforderlich. In dieser Version wird durch ein Sicherheits- und Leistungs-Update der Java-Plattform Support für manche Algorithmen zur Zertifikatsregistrierung wie beispielsweise MD5 und SHA1 entfernt. Diese Änderung verhindert die Kompatibilität von MVE mit einigen Druckern. Weitere Informationen erhalten Sie in den **Hilfeinformationen**.

[2] SNMPv3-Unterstützung muss auf dem Drucker aktiviert sein.

[3] Wenn ein erweitertes Sicherheitskennwort für den Drucker festgelegt wird, kann MVE den Drucker nicht unterstützen.

[4] MVE kann nicht mit den Lexmark-Formulardruckermodellen 2580, 2581, 2590 und 2591 kommunizieren, wenn diese den Status "Nicht bereit" aufweisen. Die Kommunikation funktioniert nur, wenn MVE zuvor mit dem Drucker im Status "Bereit" kommuniziert hat. Der Drucker kann im Status "Nicht bereit" sein, wenn Fehler- oder Warnmeldungen vorliegen, wie wenn z. B. das Verbrauchsmaterial erschöpft ist. Um den Status zu ändern, beheben Sie die Ursache der Fehler- oder Warnmeldung, und drücken anschließend auf **Bereit**.

Einrichten der Datenbank

Sie können entweder Firebird oder Microsoft SQL Server als Backend-Datenbank verwenden. Die folgende Tabelle kann Ihnen bei der Wahl der zu verwendenden Datenbank helfen.

	Firebird	Microsoft SQL Server
Server-Installation	Muss auf demselben Server wie MVE installiert sein.	Kann von einem beliebigen Server aus ausgeführt werden.
Kommunikation	Auf localhost begrenzt.	Kommuniziert über einen statischen Port oder eine dynamische benannte Instanz. SSL/TLS-Kommunikation mit einem gesicherten Microsoft SQL-Server wird unterstützt.
Leistung	Zeigt Leistungsprobleme bei großen Flotten.	Zeigt die beste Leistung für große Flotten.
Größe der Datenbank	Die Standardgrößen für Datenbanken betragen 6 MB für FRAMEWORK und 1 MB für MONITOR und QUARTZ. Die FRAMEWORK-Tabelle wächst mit jedem hinzugefügten Drucker-Datensatz um 1 KB.	Die Standardgrößen für Datenbanken betragen 20 MB für FRAMEWORK und 4,5 MB für MONITOR und QUARTZ. Die FRAMEWORK-Tabelle wächst mit jedem hinzugefügten Drucker-Datensatz um 1 KB.
Konfiguration	Automatische Konfiguration während der Installation.	Erfordert eine Einrichtung im Vorfeld der Installation.

Bei Verwendung von Firebird wird Firebird vom MVE Installationsprogramm installiert und konfiguriert, ohne dass eine weitere Konfiguration erforderlich wäre.

Wenn Sie Microsoft SQL Server verwenden, müssen Sie vor der Installation von MVE die folgenden Schritte ausführen:

- Erlauben Sie die automatische Ausführung der Anwendung.
- Richten Sie die Netzwerkbibliotheken so ein, dass sie TCP/IP-Sockets verwenden.
- Richten Sie die folgenden Datenbanken ein:

Hinweis: Im Folgenden sind die standardmäßigen Datenbanknamen aufgeführt. Sie können auch benutzerdefinierte Datenbanknamen angeben.

  - FRAMEWORK
  - MONITOR
  - QUARTZ
- Bei Verwendung einer benannten Instanz legen Sie fest, dass der Microsoft SQL Server-Browser automatisch gestartet werden soll. Andernfalls legen einen statischen Port auf die TCP/IP-Sockets.
- Erstellen Sie ein Benutzerkonto mit db-Owner-Rechten (Datenbankbesitzer-Rechten) in Bezug auf alle drei Datenbanken, die MVE verwendet, und richten Sie die Datenbank ein. Wenn der Benutzer ein Microsoft SQL Server-Konto ist, müssen Sie den Microsoft SQL Server und die Windows-Authentifizierungsmodi auf dem Microsoft SQL Server aktivieren.

  Hinweis: Wenn Markvision Enterprise (MVE), welches zur Verwendung von MS SQL Server konfiguriert wurde, deinstalliert wird, werden die erstellten Tabellen oder Datenbanken nicht gelöscht. Nach der Deinstallation müssen die Datenbanken von FRAMEWORK, MONITOR und QUARTZ manuell verschoben werden.
- Weisen Sie dem Datenbankbenutzer die DBO-Rechte zu, und legen Sie anschließend das DBO-Schema als Standardschema fest.

Einrichten einer Benutzeranmeldung

Während der Installation können Sie festlegen, ob MVE als lokales Systemkonto oder als Domänenbenutzerkonto ausgeführt wird. Die Ausführung von MVE als Domänenbenutzerkonto bietet eine sicherere Installation. Das Domänenbenutzerkonto verfügt über beschränkte Berechtigungen im Vergleich zu einem lokalen Systemkonto.

	Ausführung als Domänenbenutzerkonto	Ausführung im lokalen System
Berechtigungen im lokalen System	• Gesamten Zugriff wie folgt festlegen: – *$MVE_INSTALL*/tomcat/logs – *$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 – *$MVE_INSTALL*/apps/dm-mve/download Dabei ist *$MVE_INSTALL* das Installationsverzeichnis. • Windows-Berechtigung: LOGON_AS_A_SERVICE	Administrator-Berechtigungen
Datenbank-Verbindungsauthentifizierung	• Windows-Authentifizierung mit Microsoft SQL Server • SQL-Authentifizierung	SQL-Authentifizierung
Konfiguration	Ein Domänenbenutzer muss vor der Installation konfiguriert werden.	Automatische Konfiguration während der Installation

Wenn Sie MVE als Domänenbenutzerkonto einrichten, erstellen Sie den Benutzer auf derselben Domäne wie der des MVE-Servers.

Installation von MVE

1. Laden Sie die ausführbare Datei in einen Pfad herunter, der keine Leerzeichen enthält.
2. Führen Sie die Datei als Administrator aus und folgen Sie den Anweisungen auf dem Computerbildschirm.

Hinweise:

- Passwörter werden gehasht und sicher gespeichert. Stellen Sie sicher, dass Sie Ihre Kennwörter nicht vergessen, oder speichern Sie sie an einem sicheren Ort, da gespeicherte Passwörter nicht entschlüsselt werden können.
- Wenn Sie sich über die Windows-Authentifizierung mit dem Microsoft SQL Server verbinden, wird keine Verifizierung während der Installation versucht. Stellen Sie sicher, dass der vorgesehene Benutzer des MVE Windows-Dienstes, ein entsprechendes Konto in der Microsoft SQL Server-Instanz besitzt. Der angegebene Benutzer muss db-Owner-Rechte für die Datenbanken FRAMEWORK, MONITOR, und QUARTZ besitzen.

Installieren von MVE im Hintergrund

Datenbankeinstellungen für die Installation im Hintergrund

Einstellung	Beschreibung	Wert
--help	Zeigt die Liste der gültigen Optionen an.	
--version	Zeigt die Produktinformationen an.	
--unattendedmodeui <unattendedmodeui>	Die Benutzeroberfläche für den unbeaufsichtigten Modus.	Standard: **keine** Zugelassen: • **keine** • **minimal** • **minimalWithDialogs**
--optionfile <optionfile>	Die Datei mit den Installationsoptionen.	Standard:
--debuglevel <debuglevel>	Die Debuginformationsebene der Verbosität.	Standard: **2** Zugelassen: • **0** • **1** • **2** • **3** • **4**

Einstellung	Beschreibung	Wert
--mode <mode>	Der Installationsmodus.	Standard: **win32** Zugelassen: • **win32** • **unbeaufsichtigt**
--debugtrace <debugtrace>	Der Name der Debugdatei.	Standard:
--installer-language <installer-language>	Die Sprachauswahl.	Standard: **de** Zugelassen: • **de** • **es** • **de** • **fr** • **it** • **pt_BR** • **zh_CN**
--encryptionKey <encryptionKey>	Der Kodierungsschlüssel.	Kodierungsschlüssel: Standard:
--prefix <prefix>	Das Installationsverzeichnis.	Standard: **C:\Programme**
--mveLexmark_runas <mveLexmark_runas>	Die Benutzeroptionen für "Ausführen als".	Standard: **LOCAL_SYSTEM** Zugelassen: • **LOCAL_SYSTEM** • **SPECIFIC_USER**
--serviceRunAsUsername <serviceRunAsUsername>	Der Benutzername für "Ausführen als".	Benutzername: Standard:
--serviceRunAsPassword <serviceRunAsPassword>	Das Benutzerkennwort für "Ausführen als".	Kennwort: Standard:
--mveLexmark_database <mveLexmark_database>	Der Datenbanktyp.	Standard: Zugelassen: • **FIREBIRD** • **SQL_SERVER**
--firebirdUsername <firebirdUsername>	Der Benutzername der Firebird-Datenbank.	Benutzername: Standard:
--firebirdPassword <firebirdPassword>	Das Kennwort der Firebird-Datenbank.	Kennwort: Standard:
--firebirdFWDbName <firebirdFWDbName>	Der Name der Firebird-Datenbank für FRAMEWORK.	Datenbanknamen: Standard: **FRAMEWORK**
--firebirdMNDbName <firebirdMNDbName>	Der Firebird-Datenbankname für MONITOR.	Standard: **MONITOR**
--firebirdQZDbName <firebirdQZDbName>	Der Firebird-Datenbankname für QUARTZ.	Standard: **QUARTZ**

Einstellung	Beschreibung	Wert
--databaseIPAddress <databaseIPAddress>	Die IP-Adresse oder der Hostname der Datenbank.	IP-Adresse oder Hostname: Standard:
--databasePort <databasePort>	Die Anschlussnummer der Datenbank.	Anschlussnummer: Standard:
--instanceName <instanceName>	Der Instanzname.	Instanzname: Standard:
--instanceIdentifier <instanceIdentifier>	Die Instanz.	Standard: **databasePort** Zugelassen: • **databasePort** • **instanceName**
--databaseUsername <databaseUsername>	Der Benutzername der Datenbank.	Benutzername: Standard:
--databasePassword <databasePassword>	Das Kennwort der Datenbank.	Kennwort: Standard:
--sqlServerAuthenticationMethod <sqlServerAuthenticationMethod>	Die Authentifizierungsmethode für den Microsoft SQL-Server.	Standard: **sqlServerDbAuthentication** Zugelassen: • **sqlServerDbAuthentication** • **sqlServerWindowsAuthentication**
--fWDbName <fWDbName>	Der Datenbankname für FRAMEWORK.	Datenbanknamen: Standard: **FRAMEWORK**
--mNDbName <mNDbName>	Der Datenbankname für MONITOR.	Standard: **MONITOR**
--qZDbName <qZDbName>	Der Datenbankname für QUARTZ.	Standard: **QUARTZ**
--mveAdminUsername <mveAdminUsername>	Der Benutzername des Administrators.	Benutzername: Standard: **admin**
--mveAdminPassword <mveAdminPassword>	Das Kennwort des Administrators.	Kennwort: Standard:

Zugreifen auf MVE

Verwenden Sie die Anmeldeinformationen, die Sie bei der Installation erstellt haben, um auf MVE zuzugreifen. Sie können auch andere Anmeldemethoden, z. B. LDAP, Kerberos oder andere lokale Konten, einrichten. Weitere Informationen finden Sie unter "Einrichten des Benutzerzugriffs" auf Seite 29.

1. Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: **https://*MVE_SERVER*/mve/**, wobei ***MVE_SERVER*** der Hostname oder die IP-Adresse der auf dem Server gehosteten MVE-Software ist.
2. Akzeptieren Sie gegebenenfalls den Haftungsausschluss.
3. Geben Sie Ihre Benutzeranmeldeinformationen ein.
4. Klicken Sie auf **Anmelden**.

Hinweise:

- Stellen Sie sicher, dass Sie nach der Anmeldung das Standard-Administratorpasswort, das während der Installation verwendet wurde, ändern. Weitere Informationen finden Sie unter "Ändern des Passworts" auf Seite 24.
- Der Benutzer wird automatisch abgemeldet, wenn MVE mehr als 30 Minuten nicht verwendet wird.

Ändern der Sprache

1. Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: **`https://MVE_SERVER/mve/`**, wobei ***`MVE_SERVER`*** der Hostname oder die IP-Adresse der auf dem Server gehosteten MVE-Software ist.
2. Akzeptieren Sie gegebenenfalls den Haftungsausschluss.
3. Wählen Sie in der oberen rechten Ecke der Seite eine Sprache aus.

Ändern des Passworts

1. Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: **`https://MVE_SERVER/mve/`**, wobei ***`MVE_SERVER`*** der Hostname oder die IP-Adresse der auf dem Server gehosteten MVE-Software ist.
2. Akzeptieren Sie gegebenenfalls den Haftungsausschluss.
3. Geben Sie Ihre Benutzeranmeldeinformationen ein.
4. Klicken Sie auf **Anmelden**.
5. Klicken Sie in der oberen rechten Ecke der Seite auf Ihren Benutzernamen, und klicken Sie dann auf **Passwort ändern**.
6. Ändern Sie das Passwort.

Warten der Anwendung

Aktualisieren auf MVE 4.2

Führen Sie vor Beginn der Aktualisierung Folgendes aus:

- Sichern Sie die Datenbank-, Anwendungs- und Eigenschaftsdateien. Weitere Informationen finden Sie unter "Sichern und Wiederherstellen der Datenbank" auf Seite 26.
- Geben Sie bei Bedarf benutzerdefinierte Datenbanknamen an.

Wenn Sie ein Upgrade von Version 1.x durchführen, führen Sie zunächst ein Upgrade auf Version 2.0, dann auf Version 3.3 und dann auf Version 4.0 durch, bevor Sie auf Version 4.2 aktualisieren. Die Richtlinienmigration wird nur bei einem Upgrade auf MVE 2.0 durchgeführt.

Gültiger Upgradepfad	**3.3** auf **4.0** auf **4.2**
Ungültiger Upgradepfad	**1.6.x** auf **4.2** **2.0** auf **4.2**

1. Sichern Sie Ihre Datenbank- und Anwendungsdateien. Bei jeder Aktualisierung oder Deinstallation besteht das Risiko eines nicht zu behebenden Datenverlusts. Sie können die Sicherungsdateien verwenden, um die Anwendung auf ihren vorherigen Status zurückzusetzen, falls das Upgrade fehlschlägt.

   Warnung—Mögliche Schäden: Beim Aktualisieren von MVE ändert sich die Datenbank. Stellen Sie keine von einer älteren Version erstellte Datenbanksicherung wieder her.

   Hinweis: Weitere Informationen finden Sie unter "Sichern und Wiederherstellen der Datenbank" auf Seite 26.

2. Laden Sie die ausführbare Datei in ein temporäres Verzeichnis herunter.
3. Führen Sie die Datei als Administrator aus, und folgen Sie den Anweisungen auf dem Computerbildschirm.

   Hinweise:

   - Beim Upgrade auf MVE 2.0 werden Richtlinien, die Druckern zugewiesen sind, für jedes Druckermodell in eine einzige Konfiguration migriert. Wenn beispielsweise Richtlinien für Faxen, Kopieren, Papier und Drucken einem X792-Drucker zugewiesen sind, werden diese Richtlinien in einer X792-Konfiguration zusammengefasst. Dies gilt nicht für Richtlinien, die keinem Drucker zugewiesen sind. MVE erstellt eine Protokolldatei, in der die erfolgreiche Migration der Richtlinien in eine Konfiguration bestätigt wird. Weitere Informationen finden Sie unter "Wo befinden sich die Protokolldateien?" auf Seite 153.
   - Stellen Sie nach der Aktualisierung sicher, dass Sie den Browsercache leeren, bevor Sie erneut auf die Anwendung zugreifen.
   - Wenn Sie MVE auf Version 3.5 oder höher aktualisieren, werden die erweiterten Sicherheitskomponenten aus den Konfigurationen ausgeklammert, in denen sie sich befinden. Wenn mindestens eine erweiterte Sicherheitskomponente identisch ist, werden die Komponenten zu einer Komponente zusammengefasst. Die erstellte erweiterte Sicherheitskomponente wird automatisch zur Bibliothek der erweiterten Sicherheitskomponenten hinzugefügt.

Sichern und Wiederherstellen der Datenbank

Hinweis: Bei der Durchführung von Sicherungs- und Wiederherstellungsvorgängen kann es zu Datenverlust kommen. Stellen Sie sicher, dass die Schritte ordnungsgemäß ausgeführt werden.

Sichern der Datenbank- und Anwendungsdateien

Wir empfehlen Ihnen, Ihre Datenbank regelmäßig zu sichern.

1. Stoppen Sie den Firebird- und den Markvision Enterprise-Dienst.
   a. Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **`services.msc`** ein.
   b. Klicken Sie mit der rechten Maustaste auf **Firebird Guardian - DefaultInstance**, und klicken Sie anschließend auf **Stopp**.
   c. Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Stopp**.
2. Navigieren Sie zu dem Ordner, in dem Markvision Enterprise installiert ist.

   Beispiel: **`C:\Programme\`**
3. Sichern Sie die Anwendungs- und Datenbankdateien.

Sichern der Anwendungsdateien

Kopieren Sie folgende Dateien in ein sicheres Repository:

- 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

Hinweis: Stellen Sie sicher, dass diese Dateien ordnungsgemäß gespeichert sind. Ohne die Verschlüsselungsschlüssel in der Datei mve_Encryption.jceks können Daten, die in einem verschlüsselten Format in der Datenbank und im Dateisystem gespeichert sind, nicht wiederhergestellt werden.

Sichern der Datenbank-Dateien

Führen Sie einen der folgenden Schritte aus:

Hinweis: Die folgenden Dateien verwenden die standardmäßigen Datenbanknamen. Diese Anweisungen gelten auch für benutzerdefinierte Datenbanknamen.

- Wenn Sie eine Firebird-Datenbank verwenden, kopieren Sie die folgenden Dateien in ein sicheres Repository. Diese Dateien müssen regelmäßig gesichert werden, um Datenverlust vorzubeugen.
  - Lexmark\Markvision Enterprise\firebird\security2.fdb

Wenn Sie benutzerdefinierte Datenbanknamen verwenden, aktualisieren Sie Folgendes:

- 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

- Wenn Sie Microsoft SQL Server verwenden, erstellen Sie eine Sicherung für FRAMEWORK, MONITOR und QUARTZ.

  Weitere Informationen erhalten Sie bei Ihrem SQL-Server-Administrator.

4. Starten Sie den Firebird-Dienst und den Markvision Enterprise-Dienst erneut.
   a. Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **`services.msc`** ein.
   b. Klicken Sie mit der rechten Maustaste auf **Firebird Guardian – DefaultInstance**, und klicken Sie anschließend auf **Neu starten**.
   c. Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Neu starten**.

Wiederherstellen von Datenbank- und Anwendungsdateien

Warnung—Mögliche Schäden: Beim Aktualisieren von MVE kann sich die Datenbank ändern. Stellen Sie keine Datenbanksicherung wieder her, die von einer älteren Version erstellt wurde.

1. Beenden Sie den Markvision Enterprise-Dienst.

   Weitere Informationen finden Sie in Schritt 1 unter "Sichern der Datenbank- und Anwendungsdateien" auf Seite 26.

2. Navigieren Sie zu dem Ordner, in dem Markvision Enterprise installiert ist.

   Beispiel: **`C:\Programme\`**

3. Stellen Sie die Anwendungsdateien wieder her.

   Ersetzen Sie die folgenden Dateien durch die während des Sicherungsprozesses gespeicherten Dateien:

   - 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

   Hinweis: Sie können eine Datenbanksicherung in einer neuen MVE-Installation nur wiederherstellen, wenn es sich bei der neuen MVE-Installation um die gleiche Version handelt.

4. Stellen Sie die Datenbankdateien wieder her.

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie eine Firebird-Datenbank verwenden, ersetzen Sie die folgenden Dateien, die Sie während des Sicherungsvorgangs gespeichert haben:

  Hinweis: Die folgenden Dateien verwenden die standardmäßigen Datenbanknamen. Diese Anweisung gilt auch für benutzerdefinierte Datenbanknamen.

  - Lexmark\Markvision Enterprise\firebird\security2.fdb

    Wenn Sie benutzerdefinierte Datenbanknamen verwenden, werden auch die folgenden Dateien wiederhergestellt:

    - 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
- Bei Verwendung von Microsoft SQL Server wenden Sie sich an Ihren Microsoft SQL Server-Administrator.

5. Starten Sie den Markvision Enterprise-Dienst erneut.

   Weitere Informationen finden Sie in Schritt 4 unter "Sichern der Datenbank- und Anwendungsdateien" auf Seite 26.

Aktualisieren der Installationsprogramm-Einstellungen nach der Installation

Mit dem Markvision Enterprise-Kennwortdienstprogramm können Sie, ohne Neuinstallation von MVE, die Microsoft SQL Server-Einstellungen aktualisieren, die während der Installation konfiguriert wurden. Mit diesem Dienstprogramm können Sie auch Benutzeranmeldeinformationen des Domänenkontos aktualisieren, wie etwa Benutzernamen und Kennwort. Sie können das Dienstprogramm auch verwenden, um ein weiteres Administratorkonto zu erstellen, wenn Sie Ihre vorherigen Administrator-Anmeldeinformationen vergessen haben.

1. Navigieren Sie zu dem Ordner, in dem Markvision Enterprise installiert ist.

   Beispiel: **`C:\Program Files\`**

2. Starten Sie die Datei **mvepwdutility-windows.exe** im Verzeichnis Lexmark\Markvision Enterprise\.

3. Wählen Sie eine Sprache aus und klicken Sie dann auf **OK** > **Weiter**.

4. Befolgen Sie dann die Anweisungen auf dem Bildschirm.

Einrichten des Benutzerzugriffs

Übersicht

Mit MVE können Sie interne Benutzer direkt dem MVE-Server hinzufügen oder die bei einem LDAP-Server registrierten Benutzerkonten verwenden. Weitere Informationen über das Hinzufügen von internen Benutzern finden Sie unter "Verwalten von Benutzern" auf Seite 30. Weitere Informationen zum Verwenden von LDAP-Benutzerkonten finden Sie unter "Aktivieren der LDAP-Server-Authentifizierung" auf Seite 31.

Beim Hinzufügen von Benutzern müssen Rollen zugewiesen werden. Weitere Informationen finden Sie unter "Informationen zu Benutzerrollen" auf Seite 29.

Während der Authentifizierung überprüft das System die Benutzeranmeldeinformationen der internen Benutzer auf dem MVE-Server. Wenn MVE den Benutzer nicht authentifizieren kann, wird ein neuer Versuch anhand der im LDAP-Server registrierten Benutzer durchgeführt. Wenn der Benutzername sowohl im MVE- als auch im LDAP-Server vorhanden ist, wird das MVE-Passwort verwendet.

Informationen zu Benutzerrollen

MVE-Benutzern können eine oder mehrere Rollen zugewiesen werden. Abhängig von der Rolle können Benutzer folgende Aufgaben ausführen:

- **Admin**: Zugreifen auf und Durchführen von Aufgaben in allen Menüs. Verfügt außerdem über Administratorrechte, zum Beispiel das Hinzufügen von Benutzern zum System oder das Konfigurieren von Systemeinstellungen. Nur Benutzer mit einer Admin-Rolle können laufende Aufgaben anhalten, unabhängig davon, welcher Benutzertyp die Aufgaben gestartet hat.
- **Drucker**
  - Suchprofile verwalten.
  - Den Druckerstatus einstellen.
  - Eine Prüfung durchführen.
  - Kategorien und Stichwörter verwalten.
  - Eine Prüfung, einen Datenexport und eine Druckersuche planen.
- **Konfigurationen**
  - Konfigurationen verwalten, einschließlich Importieren und Exportieren von Konfigurationsdateien.
  - Dateien in die Ressourcenbibliothek hochladen.
  - Druckern Konfigurationen zuweisen und durchsetzen.
  - Übereinstimmungsprüfung und Konfigurationsdurchsetzung planen.
  - Stellen Sie Dateien für Drucker bereit.
  - Aktualisieren der Drucker-Firmware
  - Erzeugen Sie Signieraufforderungen für Druckerzertifikate.
  - Laden Sie Signieraufforderungen für Druckerzertifikate herunter.
- **Event Manager**
  - Aktionen und Ereignissen verwalten.
  - Geräten Ereignisse zuweisen.
  - Testaktionen.

- **Service Desk**
  - Druckerstatus aktualisieren.
  - Drucker neu starten.
  - Übereinstimmungsprüfung ausführen.
  - Konfigurationen auf Drucker durchsetzen.

Hinweise:

- Alle Benutzer können in MVE die Druckerinformationsseite anzeigen und gespeicherte Suchvorgänge und Ansichten verwalten.
- Weitere Informationen über das Zuweisen von Benutzerrollen finden Sie unter "Verwalten von Benutzern" auf Seite 30.

Verwalten von Benutzern

1. Klicken Sie in der oberen rechten Ecke der Seite auf  .
2. Klicken Sie auf **Benutzer**, und wählen Sie dann eine der folgenden Möglichkeiten aus:

Benutzer hinzufügen

a. Klicken Sie auf **Erstellen**.

b. Geben Sie Benutzernamen, Benutzer-ID und Passwort ein.

c. Wählen Sie die Rollen aus.

Hinweis: Weitere Informationen finden Sie unter "Informationen zu Benutzerrollen" auf Seite 29.

d. Klicken Sie auf **Benutzer erstellen**.

Benutzer bearbeiten

a. Wählen Sie eine Benutzer-ID aus.

b. Konfigurieren Sie die Einstellungen.

c. Klicken Sie auf **Änderungen speichern**.

Benutzer löschen

a. Wählen Sie einen oder mehrere Benutzer aus.

b. Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Hinweis: Ein Benutzerkonto wird nach drei hintereinander fehlgeschlagenen Anmeldeversuchen gesperrt. Nur ein Administrator kann das Benutzerkonto reaktivieren. Wenn der Administrator gesperrt wird, wird er vom System automatisch nach fünf Minuten reaktiviert.

Aktivieren der LDAP-Server-Authentifizierung

LDAP ist ein standardbasiertes, plattformübergreifendes und erweiterbares Protokoll, das direkt über TCP/IP ausgeführt wird. Es wird für den Zugriff auf spezielle Datenbanken (Verzeichnisse) verwendet.

Um zu vermeiden, dass mehrere Anmeldeinformationen verwaltet werden müssen, können Benutzer-IDs und Kennwörter mithilfe des firmeneigenen LDAP-Servers authentifiziert werden.

Voraussetzung dafür ist, dass der LDAP-Server Benutzergruppen enthält, die den erforderlichen Benutzerrollen entsprechen. Weitere Informationen finden Sie unter "Informationen zu Benutzerrollen" auf Seite 29.

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **LDAP**, und wählen Sie anschließend **LDAP für Authentifizierung aktivieren** aus.
3. In dem Feld Hostname des LDAP-Servers wird die IP-Adresse oder der Hostname des LDAP-Servers angezeigt, auf dem die Authentifizierung stattfindet.

   Hinweis: Wenn die Kommunikation zwischen MVE- und LDAP-Server verschlüsselt werden soll, verwenden Sie den vollqualifizierten Domänennamen (FQDN).
4. Geben Sie die Server-Anschlussnummer entsprechend dem ausgewählten Verschlüsselungsprotokoll an.
5. Wählen Sie das Verschlüsselungsprotokoll aus.
   - **Keine**
   - **TLS**: ein Sicherheitsprotokoll, das die Kommunikation zwischen einem Server und einem Client mittels Datenverschlüsselung und Zertifikatauthentifizierung schützt. Wenn diese Option ausgewählt ist, wird ein START_TLS-Befehl an den LDAP-Server gesendet, nachdem die Verbindung hergestellt worden ist. Verwenden Sie diese Einstellung, wenn Sie eine sichere Kommunikation über Port 389 wünschen.
   - **SSL/TLS**: Ein Sicherheitsprotokoll, das die Kommunikation zwischen einem Server und einem Client mithilfe von Kryptografie mit öffentlichem Schlüssel authentifiziert. Verwenden Sie diese Option, wenn Sie eine gesicherte Kommunikation ab dem Beginn der LDAP-Bindung wünschen. Diese Option wird in der Regel für Port 636 oder andere gesicherte LDAP-Anschlüsse verwendet.
6. Wählen Sie den Bindungstyp aus.
   - **Einfach**: Der MVE-Server legt die angegebenen Anmeldeinformationen gegenüber dem LDAP-Server offen, um dessen Suchfunktion zu verwenden.
     a. Geben Sie den Verbindungsbenutzernamen ein.
     b. Geben Sie das Verbindungskennwort ein, und bestätigen Sie anschließend das Kennwort.
   - **Kerberos**: Zur Konfiguration der Einstellungen gehen Sie folgendermaßen vor:
     a. Geben Sie den Verbindungsbenutzernamen ein.
     b. Geben Sie das Verbindungskennwort ein, und bestätigen Sie anschließend das Kennwort.
     c. Klicken Sie auf **Datei auswählen**, und navigieren Sie zur Datei "krb5.conf".
   - **SPNEGO**: Zur Konfiguration der Einstellungen gehen Sie folgendermaßen vor:
     a. Geben Sie den Dienstprinzipalnamen ein.
     b. Klicken Sie auf **Datei auswählen**, und navigieren Sie zur Datei "krb5.conf".
     c. Klicken Sie auf **Datei auswählen**, und navigieren Sie zur Kerberos-Schlüsseltabellendatei.

     Diese Option wird nur für die Konfiguration des Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) zur Unterstützung der Single-Sign-On-Funktionalität verwendet.

7 Konfigurieren Sie im Abschnitt Erweiterte Optionen Folgendes:

- **Suchbasis**: der definierte Name (DN) des Root-Knotens. In der Hierarchie des LDAP-Community-Servers muss dieser Knoten der Vorgänger des Benutzer- und Gruppenknotens sein. Beispiel: **`dc=mvetest,dc=com`**.

  Hinweis: Wenn Sie einen Root-DN angeben, stellen Sie sicher, dass der Ausdruck nur **`dc`** und **`o`** enthält. Wenn **`ou`** oder **`cn`** für den Vorgänger der Benutzer- oder Gruppenknoten angegeben ist, verwenden Sie **`ou`** oder **`cn`** in den Ausdrücken "Benutzersuchbasis" und "Gruppensuchbasis".
- **Benutzersuchbasis**: der Knoten im LDAP-Community-Server, in dem das Benutzerobjekt enthalten ist. Dieser Knoten befindet sich unterhalb des Root-DNs, in dem alle Benutzerknoten aufgeführt sind. Beispiel: **`ou=people`**.
- **Filter für Benutzersuche**: der Parameter zur Suche nach einem Benutzerobjekt im LDAP-Community-Server. Beispiel: **`(uid={0})`**.

  Beispiele für zulässige mehrere Bedingungen und komplexe Ausdrücke

Anmelden mit	Geben Sie im Feld Filter für Benutzersuche Folgendes ein:
Gemeinsamer Name	`(CN={0})`
Anmeldename	`(sAMAccountName={0})`
Benutzerprinzipalname	`(userPrincipalName={0})`
Telefonnummer	`(telephoneNumber={0})`
Anmeldename oder gemeinsamer Name	`(|(sAMAccountName={0})(CN={0}))`

  Hinweis: Das einzig gültige Muster lautet **`{0}`**. Das bedeutet, dass MVE nach dem Anmeldenamen des MVE-Benutzers sucht.
- **Benutzerbasisobjekt und gesamten SubTree durchsuchen**: Das System durchsucht alle Knoten unter der Benutzersuchbasis.
- **Gruppensuchbasis**: Der Knoten im LDAP-Community-Server, der die den MVE-Rollen entsprechenden Benutzergruppen enthält. Dieser Knoten befindet sich unterhalb des Root-DNs, in dem alle Gruppenknoten aufgeführt sind. Beispiel: **`ou=group`**.
- **Gruppensuchfilter**: Der Parameter für die Suche nach einem Benutzer innerhalb einer Gruppe, die einer Rolle in MVE entspricht.

  Hinweis: Nur die Muster **`{0}`** und **`{1}`** können verwendet werden. Bei Verwendung von **`{0}`** sucht MVE nach dem DN des LDAP-Benutzers. Bei Verwendung von **`{1}`** sucht MVE nach dem Anmeldenamen des MVE-Benutzers.
- **Gruppenrollenattribut**: Geben Sie das LDAP-Attribut für den vollständigen Namen der Gruppe ein. Ein LDAP-Attribut hat eine bestimmte Bedeutung und definiert eine Zuordnung zwischen dem Attribut und einem Feldnamen. Das LDAP-Attribut **`cn`** ist beispielsweise dem Feld Vollständiger Name zugeordnet. Das LDAP-Attribut **`commonname`** ist auch dem Feld Vollständiger Name zugeordnet. Im Allgemeinen sollte dieses Attribut auf dem Standardwert **`cn`** belassen werden.
- **Benutzerbasisobjekt und gesamten SubTree durchsuchen**: Das System durchsucht alle Knoten unter der Gruppensuchbasis.

8 Geben Sie im Abschnitt Zuordnung von LDAP-Gruppen und MVE-Rollen die Namen der LDAP-Gruppen ein, die den MVE-Rollen entsprechen.

Hinweise:

- Weitere Informationen finden Sie unter "Informationen zu Benutzerrollen" auf Seite 29.

- Sie können eine LDAP-Gruppe mehreren MVE-Rollen zuweisen. Sie können auch mehr als eine LDAP-Gruppe in ein Rollenfeld eingeben, indem Sie das Senkrechtstrich-Zeichen (|) verwenden, um mehrere Gruppen voneinander zu trennen. Um beispielsweise die Gruppen **admin** und **assets** in die Admin-Rolle einzuschließen, geben Sie **admin|assets** in das Rollenfeld LDAP-Gruppen für Admin ein.
- Wenn Sie nur eine Admin-Rolle und keine anderen MVE-Rollen verwenden möchten, lassen Sie die Felder leer.

9 Klicken Sie auf **Änderungen speichern**.

Installieren von LDAP-Serverzertifikaten

Um eine verschlüsselte Kommunikation zwischen dem MVE-Server und dem LDAP-Server einzurichten, muss MVE dem LDAP-Serverzertifikat vertrauen. Wenn MVE in der MVE-Architektur eine Authentifizierung mit einem LDAP-Server durchführt, ist MVE der Client und der LDAP-Server ist der Peer.

1 Klicken Sie in der oberen rechten Ecke der Seite auf .

2 Klicken Sie auf **LDAP**, und konfigurieren Sie dann die LDAP-Einstellungen. Weitere Informationen finden Sie unter "Aktivieren der LDAP-Server-Authentifizierung" auf Seite 31.

3 Klicken Sie auf **LDAP testen**.

4 Geben Sie einen gültigen LDAP-Benutzernamen mit Passwort ein, und klicken Sie dann auf **Test starten**.

5 Überprüfen Sie das Zertifikat auf seine Gültigkeit, und akzeptieren Sie es dann.

Erkennen von Druckern

Erstellen eines Suchprofils

Verwenden Sie ein Suchprofil zum Suchen nach Druckern in Ihrem Netzwerk, und fügen Sie diese zum System hinzu. Führen Sie in einem Suchprofil einen der folgenden Schritte aus, um eine Liste von IP-Adressen oder Hostnamen ein- oder auszuschließen:

- Einträge einzeln hinzufügen
- Importieren von Einträgen mithilfe einer TXT- oder CSV-Datei

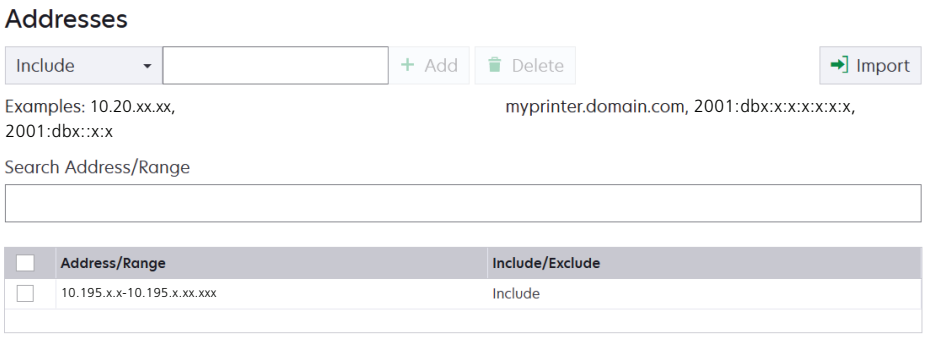
Sie können einem kompatiblen Druckermodell auch automatisch eine Konfiguration zuweisen und diese durchsetzen. Eine Konfiguration muss Printer Settings, Anwendungen, Lizenzen, Firmware und CA-Zertifikate enthalten, die den Druckern bereitgestellt werden können.

1. Klicken Sie im Menü Drucker auf **Suchprofile** > **Erstellen**.
2. Geben Sie im Abschnitt Allgemein einen eindeutigen Namen für das Suchprofil und seine Beschreibung ein, und konfigurieren Sie anschließend Folgendes:
   - **Zeitsperre**: So lange wartet das System auf eine Druckerantwort.
   - **Erneute Versuche**: So oft soll das System versuchen, mit einem Drucker zu kommunizieren.
   - **Gefundene Drucker automatisch verwalten**: Neu gefundene Drucker werden automatisch auf den Staus "Verwaltet" gesetzt, und der Status "Neu" wird während der Suche übersprungen.
3. Führen Sie im Abschnitt Adressen eine der folgenden Aktionen durch:

Adressen hinzufügen

a. Wählen Sie **Einschließen** oder **Ausschließen** aus.

b. Geben Sie die IP-Adresse, den Hostnamen, das Subnetz oder den IP-Adressbereich ein.



Fügen Sie nur jeweils einen Eintrag hinzu. Geben Sie die Adressen mithilfe der folgenden Formate ein:

- **`10.195.10.1`** (einzelne IPv4-Adresse)
- **`meindrucker.beispiel.com`** (einzelner Hostname)
- **`10.195.10.3–10.195.10.255`** (IPv4-Adressbereich)
- **`10.195.*.*`** (Platzhalter)
- **`10.195.10.1/22`** (IPv4-Classless-Inter-Domain-Routing- oder CIDR-Schreibweise)
- **`2001:db8:0:0:0:0:2:1`** (vollständige IPv6-Adresse)
- **`2001:db8::2:1`** (gekürzte IPv6-Adresse)

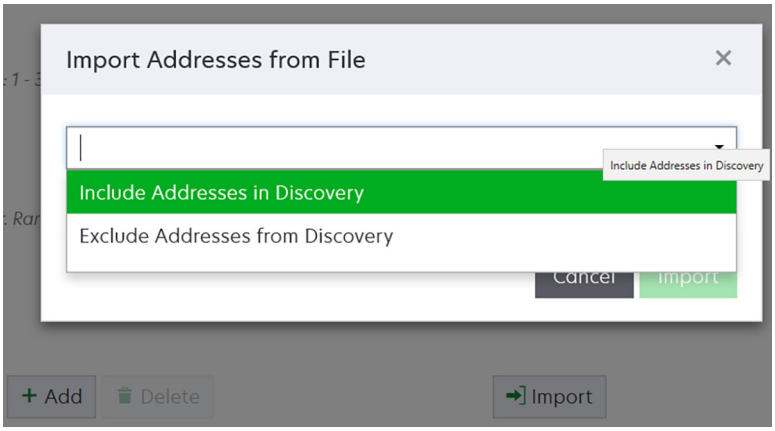
Hinweis: Wenn separate Suchprofile für die IPv6- und die IPv4-Adresse für den gleichen Drucker erstellt werden, wird die zuletzt gefundene Adresse angezeigt. Wird beispielsweise für einen Drucker erst eine IPv6-Adresse und anschließend noch eine IPv4-Adresse gefunden, wird nur die IPv4-Adresse in der Druckerliste angezeigt.

c Klicken Sie auf **Hinzufügen**.

Importieren der Adressen

a Klicken Sie auf **Importieren**.

b Wählen Sie aus, ob IP-Adressen während der Suche ein- oder ausgeschlossen werden sollen.



c Navigieren Sie zu der Textdatei, die eine Liste der Adressen enthält. Jede Adresse muss in einer separaten Zeile eingetragen werden.

Beispiel-Textdatei

```
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 Klicken Sie auf **Importieren**.

4 Wählen Sie im Abschnitt SNMP die Option **Version 1**, **Version 2c** oder **Version 3** aus, und stellen Sie anschließend die Zugriffsberechtigungen ein.

Hinweis: Um Drucker zu identifizieren, die SNMP-Version 3 verwenden, erstellen Sie einen Benutzernamen und ein Benutzerkennwort im Embedded Web Server des Druckers, und starten Sie anschließend den Drucker neu. Wenn keine Verbindung hergestellt werden kann, suchen Sie erneut nach den Druckern. Weitere Informationen finden Sie im *Embedded Web Server Administratorhandbuch*.

5 Falls erforderlich, wählen Sie im Abschnitt Anmeldeinformationen eingeben die von den Druckern verwendete Authentifizierungsmethode aus, und geben Sie anschließend die Anmeldeinformationen ein.

Hinweis: Mit dieser Funktion können Sie während der Suche die Kommunikation mit gesicherten Druckern herstellen. Die korrekten Anmeldeinformationen müssen angegeben werden, um Aufgaben auf den gesicherten Druckern auszuführen, zum Beispiel Prüfung, Statusaktualisierung und Firmware-Aktualisierung.

6 Bei Bedarf können Sie einem Druckermodell über den Abschnitt Konfigurationen zuweisen eine Konfiguration zuweisen. Informationen zum Erstellen einer Konfiguration finden Sie unter "Erstellen einer Konfiguration" auf Seite 69.

7 Bei Bedarf können Sie einem Druckermodell über den Abschnitt Schlüsselwörter zuweisen ein Schlüsselwort zuweisen. Informationen zum Zuweisen von Schlüsselwörtern zu Druckern finden Sie unter "Zuweisen von Stichwörtern zu Druckern" auf Seite 66.

Hinweise:

- Alle Drucker, die über dieses Profil erkannt werden, werden mit den neuen Schlüsselwörtern zugewiesen.
- Die neuen Schlüsselwörter werden der bestehenden Liste von Stichwörtern hinzugefügt, die bereits einem Drucker zugewiesen sind.

8 Klicken Sie auf **Profil speichern** oder auf **Profil speichern und ausführen**.

Hinweis: Eine Suche kann so geplant werden, dass sie in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Verwalten von Suchprofilen

1 Klicken Sie im Menü "Drucker" auf **Suchprofile**.

2 Gehen Sie wie folgt vor:

Bearbeiten eines Profils

a Wählen Sie ein Profil aus, und klicken Sie dann auf **Bearbeiten**.

b Konfigurieren Sie die Einstellungen.

c Klicken Sie auf **Profil speichern** oder **Profil speichern und ausführen**.

Profil kopieren

a Wählen Sie ein Profil aus, und klicken Sie dann auf **Kopieren**.

b Konfigurieren Sie die Einstellungen.

c Fügen Sie die IP-Adressen hinzu. Weitere Informationen finden Sie unter "Adressen hinzufügen" auf Seite 34.

d Klicken Sie auf **Profil speichern** oder **Profil speichern und ausführen**.

Löschen eines Profils

a Wählen Sie ein oder mehrere Profile aus.

b Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Profil ausführen

a Wählen Sie ein oder mehrere Profile aus.

b Klicken Sie auf **Ausführen**. Überprüfen Sie den Suchstatus über das Menü "Aufgaben".

Beispielszenario: Erkennen von Druckern

Firma ABC ist ein großes Fertigungsunternehmen, das in einem neunstöckigen Gebäude residiert. Das Unternehmen hat gerade 30 neue Lexmark Drucker gekauft, die auf die neun Stockwerke verteilt sind. Als IT-Mitarbeiter müssen Sie diese neuen Drucker zu MVE hinzufügen. Die Drucker sind bereits mit dem Netzwerk verbunden, aber Sie kennen nicht alle IP-Adressen.

Sie möchten die folgenden neuen Drucker in der Buchhaltung sichern.

10.194.55.60
10.194.56.77
10.194.55.71
10.194.63.27
10.194.63.10

Beispielimplementierung

1. Erstellen Sie ein Suchprofil für die Drucker in der Buchhaltung.
2. Fügen Sie die fünf IP-Adressen hinzu.
3. Erstellen Sie eine Konfiguration, die die angegebenen Drucker sichert.
4. Nehmen Sie die Konfigurationen in das Suchprofil auf.
5. Speichern Sie das Profil, und führen Sie es aus.
6. Erstellen Sie ein weiteres Suchprofil für die übrigen Drucker.
7. Fügen Sie die IP-Adressen mit einem Platzhalter ein. Verwenden Sie Folgendes: **10.194.*.***
8. Schließen Sie die fünf Drucker-IP-Adressen in der Buchhaltung aus.
9. Speichern Sie, und führen Sie dann das Profil aus.

Verwalten des Sicherheits-Dashboards

Übersicht

Im Sicherheits-Dashboard können Sie den Zustand der Sicherheitseinstellungen des Geräts anzeigen. Es ist eine visuelle Darstellung verschiedener Sicherheitseinstellungen, wie Ports, Protokolle, Festplattenverschlüsselungsstatus, Geräteadministratorkonten und Standardzertifikatstatus. Es bietet einen Überblick über die Sicherheitslage Ihrer Flotte, sodass Administratoren die Einstellungen identifizieren und korrigieren können, die nicht den Vorgaben entsprechen.

Zugriff auf das Sicherheits-Dashboard

1. Klicken Sie im MVE-Webportal auf **Dashboard**.

   Hinweis: Das Sicherheits-Dashboard ist die Standard-Landing Page für Admin-Benutzer.

2. Klicken Sie auf eine der folgenden Optionen:
   - **Geräte-Sicherheitsinformationen**
   - **Gerätekonformitätsprüfung**

Verwalten der Geräte-Sicherheitsinformationen

Dieses Widget fasst die Sicherheitsansicht der Flotte zusammen.

1. Klicken Sie auf einen beliebigen Balken des Diagramms, um das Fenster Geräte-Sicherheitsinformationen zu öffnen.
2. Bewegen Sie den Mauszeiger über die Balken, um die folgenden Details anzuzeigen:
   - Anschlussnummer
   - Anzahl der zugeordneten Drucker
   - Gibt an, ob die Druckereinstellungen geöffnet/aktiviert sind
3. Klicken Sie auf **Drucken**, um ein druckbares Format der Detailansicht anzuzeigen.

Hinweise:

- Das Fenster „Geräte-Sicherheitsinformationen“ bietet dem Benutzer eine Funktion zur genauen Suche an.
- Durch Klicken auf ein beliebiges Balkenelement im Diagramm kann der Benutzer zu einer gefilterten Ansicht der Druckerlistenseite navigieren. Weitere Informationen finden Sie unter "Anzeigen der Druckerliste" auf Seite 40.

Verwalten der Gerätekonformitätsprüfung

Dieses Widget fasst die detaillierte Ansicht der Übereinstimmungsprüfung der Flotte zusammen.

1. Klicken Sie auf einen beliebigen Abschnitt des Kreisdiagramms, um das Fenster Gerätekonformitätsprüfung aufzurufen.
2. Wenden Sie im linken Fensterbereich den Filter Zeitraum an.

   Hinweis: Der Standardbereich beträgt 7 Tage.
3. Klicken Sie auf **Drucken**, um ein druckbares Format der Detailansicht anzuzeigen.

Hinweise:

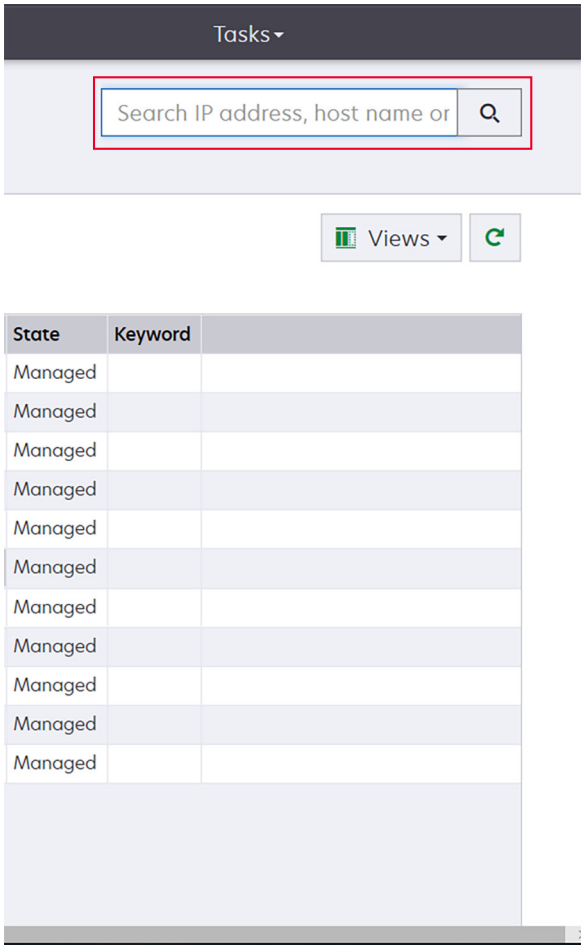
- Das Fenster Gerätekonformitätsprüfung bietet dem Benutzer eine Funktion zur genauen Suche.
- Durch Klicken auf einen beliebigen Abschnitt des Kreisdiagramms kann der Benutzer zu einer gefilterten Ansicht der Druckerlistenseite navigieren. Weitere Informationen finden Sie unter "Anzeigen der Druckerliste" auf Seite 40.

Anzeigen von Druckern

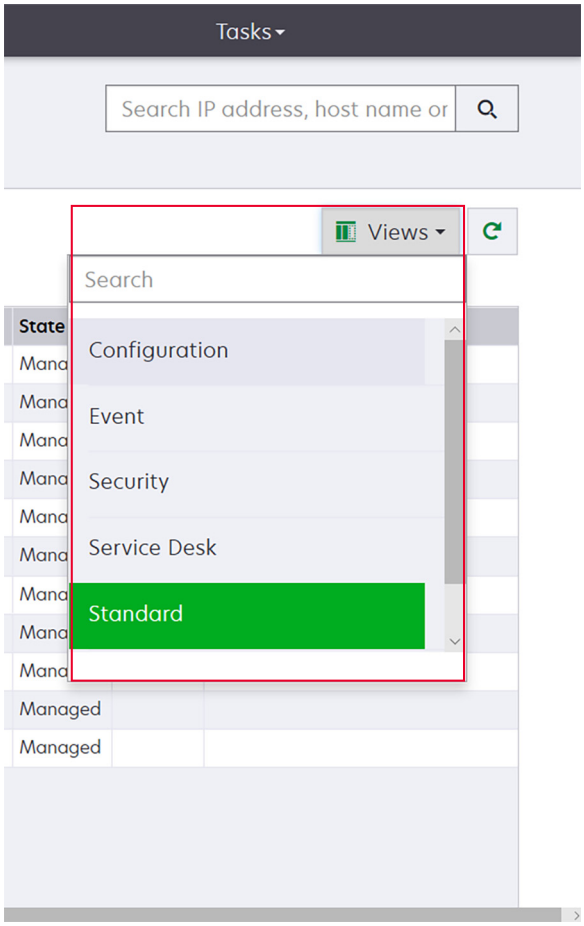
Anzeigen der Druckerliste

Die Druckerlistenseite ist die standardmäßige Startseite beim Zugriff auf MVE. Die Tabelle zeigt die Liste der Drucker, die in MVE hinzugefügt werden.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Gehen Sie auf der Seite Druckerliste wie folgt vor:
   - Um nach bestimmten Druckern zu suchen, führen Sie einen der folgenden Schritte aus:
     - Suchen Sie mithilfe des Suchfeldes nach einer IP-Adresse, einem Hostnamen, einem Systemnamen, oder einer Seriennummer.

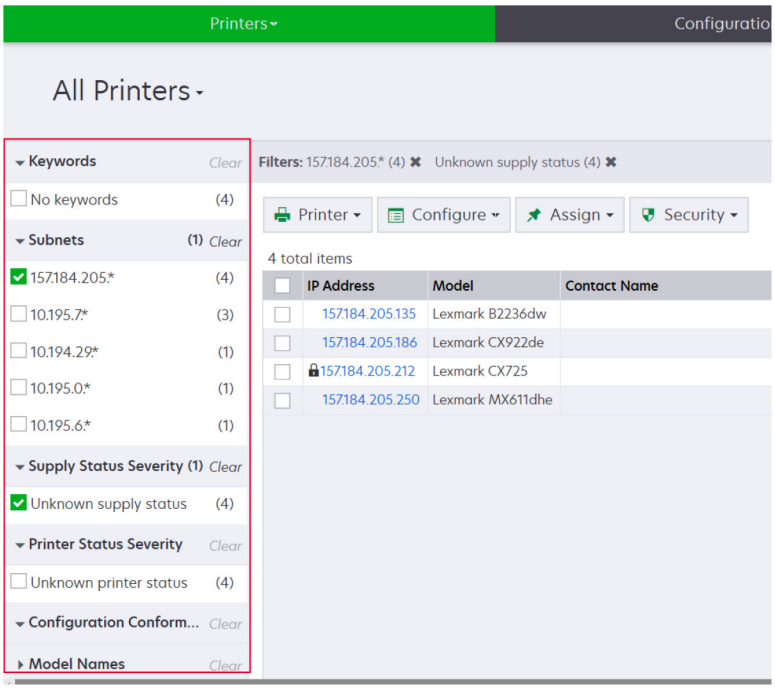


– Ändern Sie die Druckerlistenansicht. Weitere Informationen finden Sie unter "Druckerlistenansicht ändern" auf Seite 46.

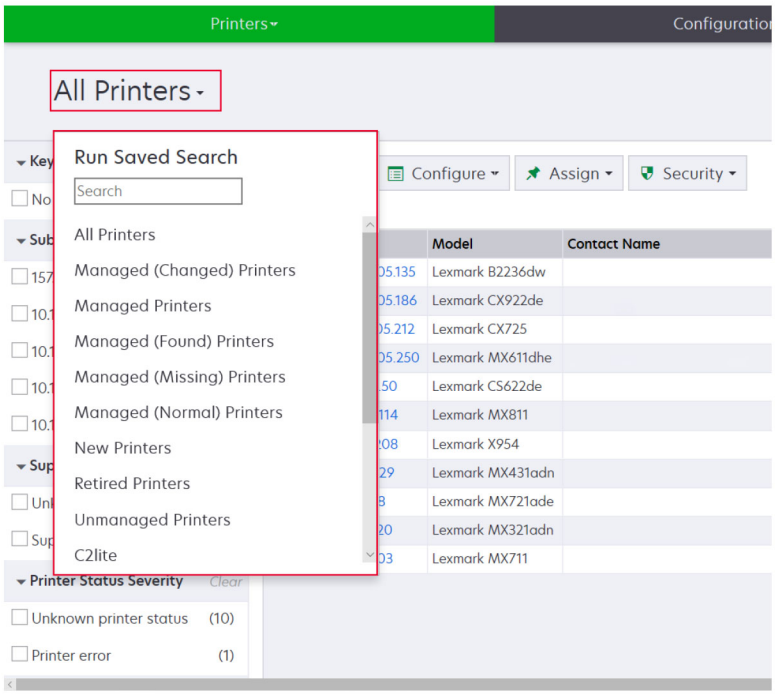


Hinweis: Bei Verwendung des Suchfeldes sucht die Anwendung nach allen Druckern im System. Die ausgewählten Filter und gespeicherten Suchvorgänge werden ignoriert. Bei der Ausführung eines gespeicherten Suchvorgangs werden die darin angegebenen Kriterien verwendet. Die ausgewählten Filter und die im Suchfeld eingegebene IP-Adresse bzw. der Host-Name werden ignoriert. Anhand der Filter können die aktuellen Suchergebnisse eingegrenzt werden.

– Verwenden Sie die Filter.



– Führen Sie einen gespeicherten Suchvorgang aus. Weitere Informationen finden Sie unter "Ausführen eines gespeicherten Suchvorgangs" auf Seite 49.



- Klicken Sie zum Sortieren der Drucker in der Druckerlistentabelle auf eine beliebige Spaltenüberschrift. Die Drucker werden gemäß der ausgewählten Spaltenüberschrift sortiert.

- Um sich weitere Informationen zu den Druckern anzeigen zu lassen, ändern Sie die Größe der Spalten. Platzieren Sie den Cursor auf den vertikalen Rand der Spaltenüberschrift, und ziehen Sie den Rand nach links oder rechts.

Anzeigen der Druckerinformationen

Um eine vollständige Liste mit Informationen anzuzeigen, stellen Sie sicher, dass am Drucker eine Geräteprüfung durchgeführt wurde. Weitere Informationen finden Sie unter "Überprüfen von Druckern" auf Seite 61.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Klicken Sie auf die IP-Adresse des Druckers.
3. Beachten Sie folgende Informationen:
   - **Status**: Der Druckerstatus.
   - **Verbrauchsmaterialien**: Die Einzelheiten des Verbrauchsmaterials und der verbleibende Vorrat in Prozent.
   - **Identifikation**: Die Informationen zur Druckernetzwerk-Identifikation.

     Hinweis: Die Zeitzoneninformation ist nur auf bestimmten Druckermodellen verfügbar.
   - **Datumsangaben**: Das Datum, an dem der Drucker zum System hinzugefügt wurde, das Suchdatum und das letzte Prüfdatum.
   - **Firmware**: Die Eigenschaften und Code-Version der Drucker-Firmware.
   - **Funktionen**: Die Druckerfunktionen.
   - **Speicheroptionen**: Die Festplattengröße und freier Speicherplatz im Benutzer-Flash.
   - **Einzugsoptionen**: Die Einstellungen für die verfügbaren Fächer.
   - **Ausgabeoptionen**: Die Einstellungen für die verfügbaren Ablagen.
   - **eSF-Anwendungen**: Angaben über die auf dem Drucker installierten eSF-Anwendungen (Embedded Solutions Framework).
   - **Druckerstatistiken**: Die spezifischen Werte für die einzelnen Druckereigenschaften.
   - **Details ändern**: Die Informationen über Änderungen am Drucker.

     Hinweis: Diese Informationen sind nur für Drucker verfügbar, für die der Zustand "Verwaltet (geändert)" festgelegt wurde. Weitere Informationen finden Sie unter "Informationen zu Lebenszyklus-Statusarten von Druckern" auf Seite 47.
   - **Druckeranmeldeinformationen**: Die Anmeldeinformationen, die in der dem Drucker zugewiesenen Konfiguration verwendet wurden.
   - **Druckerzertifikat**: Die Eigenschaften der folgenden Druckerzertifikate.
     - **Standard**
     - **HTTPS**
     - **802.1x**
     - **IPSec**

     Hinweise:

     - Diese Informationen sind nur bei manchen Druckermodellen verfügbar.
     - Der Gültigkeitsstatus Läuft bald ab gibt das Ablaufdatum an, das im Abschnitt Zertifizierungsstelle unter Systemkonfiguration festgelegt wurde.

- **Konfigurationseigenschaften**: Die Eigenschaften der Konfiguration, die dem Drucker zugewiesen wurde.
- **Aktive Warnungen**: Die Druckerwarnungen, die zu löschen sind.
- **Zugewiesene Ereignisse**: Die dem Drucker zugewiesenen Ereignisse.

Exportieren von Druckerdaten

MVE ermöglicht Ihnen das Exportieren der Druckerinformationen, die in Ihrer aktuellen Ansicht verfügbar sind.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Drucker** > **Daten exportieren**.

   Hinweise:

   - Die exportierten Daten werden in einer CSV-Datei gespeichert.
   - Das Exportieren von Daten kann so geplant werden, dass es in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Verwalten von Ansichten

Die Funktion Ansichten ermöglicht das Anpassen der Informationen, die auf der Seite "Druckerliste" angezeigt wird.

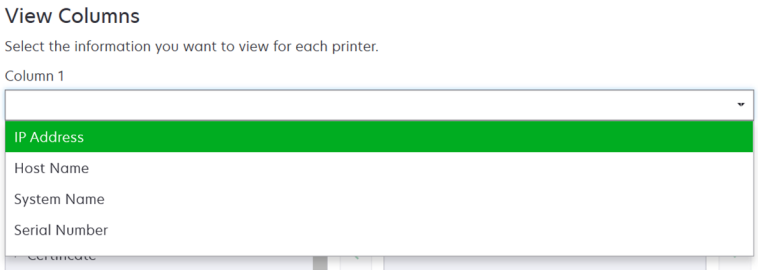
1. Klicken Sie im Menü Drucker auf **Ansichten**.
2. Wählen Sie eine der folgenden Möglichkeiten:

Erstellen einer Ansicht

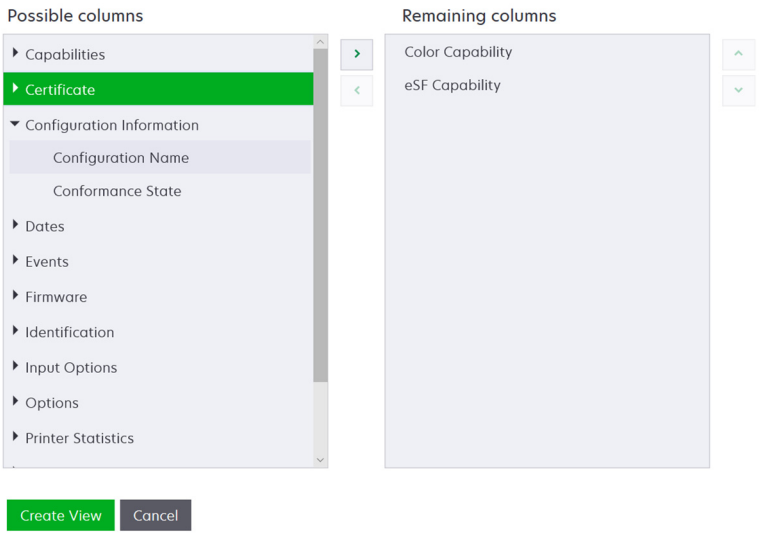
a. Klicken Sie auf **Erstellen**.

b. Geben Sie einen eindeutigen Namen für die Ansicht und ihre Beschreibung ein.

c. Wählen Sie im Menü Spalte 1 im Abschnitt Spalten anzeigen die Bezeichner-Spalte aus.



d Wählen Sie im Abschnitt Mögliche Spalten die Informationen aus, die Sie als Spalte anzeigen möchten, und klicken Sie dann auf **>**.



- **Funktionen**: Zeigt an, ob die ausgewählten Funktionen auf dem Drucker unterstützt werden.
- **Zertifikat**: Zeigt das Erstellungsdatum des Druckerzertifikats, den Anmeldestatus, das Ablaufdatum, das Verlängerungsdatum, die Überarbeitungsnummer, das Zertifikatsthema, die Gültigkeit und den Signaturstatus an.
- **Konfigurationsinformationen**: Zeigt konfigurationsrelevante Druckerinformationen wie Übereinstimmung, Konfigurationsname und Status an.
- **Datumsangaben**: Zeigt die letzte Prüfung, die letzte Übereinstimmungsprüfung, die letzte Suche und das Datum an, an dem der Drucker dem System hinzugefügt wurde.
- **Ereignisse**: Zeigt ereignisrelevante Druckerinformationen an.
- **Firmware**: Zeigt Firmware-relevante Informationen wie die Firmware-Version an.
- **Identifikation**: Zeigt Informationen über den Drucker wie IP-Adresse, Hostname und Seriennummer an.
- **Einzugsoptionen**: Zeigt Informationen zu den Zuführungsoptionen wie Fachgröße und Medienart an.
- **Optionen**: Zeigt Informationen über die Druckeroptionen wie Festplatte und Flash-Laufwerk an.
- **Druckerstatistik**: Zeigt Informationen über die Druckerverwendung an, beispielsweise die Anzahl der gedruckten oder gescannten Seiten und die Gesamtanzahl der gefaxten Aufträge.
- **Lösungen**: Zeigt die auf dem Drucker installierten eSF-Anwendungen und deren Versionsnummern an.
- **Status**: Zeigt den Status von Drucker und Verbrauchsmaterialien an.
- **Verbrauchsmaterialien**: Zeigt Informationen zu Verbrauchsmaterialien an.
- **Druckeranschlüsse**: Zeigt Informationen zu Anschlüssen an.

  Hinweis: Die Option **Unbekannt** im Anschlusswert bedeutet, dass entweder der Anschluss nicht auf dem Drucker vorhanden ist oder MVE den Anschluss nicht abrufen kann.
- **Druckersicherheitsoptionen**: Zeigt TLS- und Cipher-Informationen an.

e Klicken Sie auf **Ansicht erstellen**.

Bearbeiten einer Ansicht

a Wählen Sie eine Ansicht aus.

b Klicken Sie auf **Bearbeiten**, und bearbeiten Sie dann die Einstellungen.

c Klicken Sie auf **Änderungen speichern**.

Kopieren einer Ansicht

a Wählen Sie eine Ansicht aus.

b Klicken Sie auf **Kopieren**, und konfigurieren Sie dann die Einstellungen.

c Klicken Sie auf **Ansicht erstellen**.

Löschen von Ansichten

a Wählen Sie eine oder mehrere Ansichten aus.

b Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Festlegen einer Standardansicht

a Wählen Sie eine Ansicht aus.

b Klicken Sie auf **Als Standard festlegen**.

Die folgenden Ansichten wurden vom System erzeugt und können weder bearbeitet noch gelöscht werden:

- Konfiguration
- Druckerliste
- Ereignis
- Sicherheit
- Service Desk
- Standard

Druckerlistenansicht ändern

Weitere Informationen finden Sie unter "Verwalten von Ansichten" auf Seite 44.

1 Klicken Sie im Menü "Drucker" auf **Druckerliste**.

2 Klicken Sie auf **Ansichten**, und wählen Sie anschließend einen Typ aus.

Filtern von Druckern über die Suchleiste

Beachten Sie folgende Hinweise, wenn Sie über die Suchleiste nach Druckern suchen.

- Für die Suche nach einer IP-Adresse, bitte die komplette IP-Adresse oder den IP-Adressbereich angeben.

  Beispiel:

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

- Wenn der Suchstring keine volle IP-Adresse ist, werden die Drucker entsprechend ihrer Hostnamen, Systemnamen, oder Seriennummer gesucht.
- Der Unterstrich (_) kann als Platzhalterzeichen verwendet werden.

Verwalten von Schlüsselwörtern

Mit Schlüsselwörtern können Sie benutzerdefinierte Tags erstellen und sie Druckern zuweisen.

1. Klicken Sie im Menü Drucker auf **Schlüsselwörter**.
2. Führen Sie einen der folgenden Schritte aus:
   - Hinzufügen, Bearbeiten oder Löschen einer Kategorie.

     Hinweis: In Kategorien werden Schlüsselwörter zu Gruppen zusammengefasst.
   - Hinzufügen, Bearbeiten oder Löschen eines Schlüsselworts.

Informationen zum Zuweisen von Schlüsselwörtern zu Druckern finden Sie unter "Zuweisen von Stichwörtern zu Druckern" auf Seite 66.

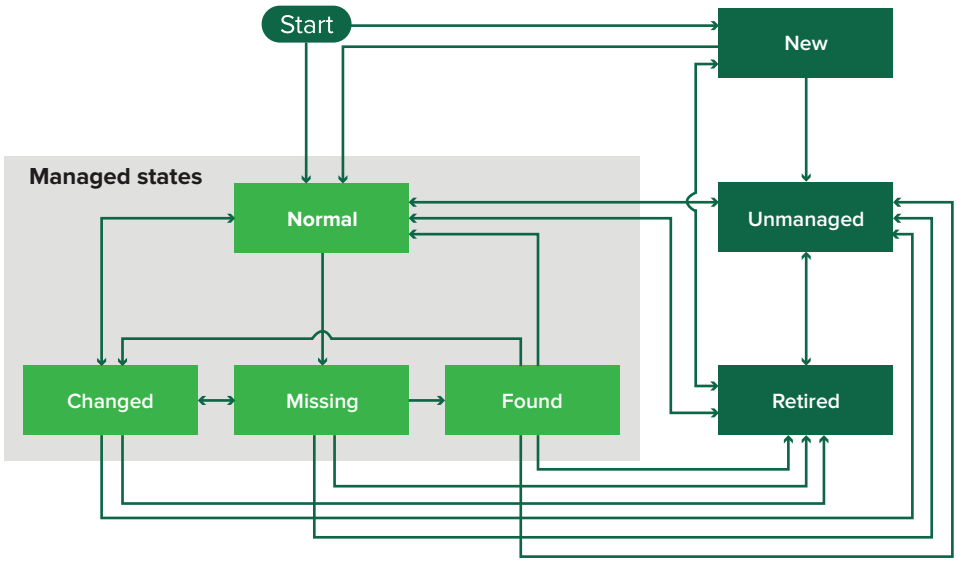
Verwenden gespeicherter Suchvorgänge

Informationen zu Lebenszyklus-Statusarten von Druckern

Vom System erzeugte gespeicherte Suchvorgänge zeigen die Drucker in folgenden Lebenszyklus-Statusarten:

- **Alle Drucker**: Alle Drucker im System
- **Verwaltete Drucker**: Angezeigte Drucker können eine der folgenden Statusarten aufweisen:
  - Verwaltet (normal)
  - Verwaltet (geändert)
  - Verwaltet (fehlt)
  - Verwaltet (gefunden)
- **Verwaltete (geänderte) Drucker**: Drucker im System, deren Eigenschaften seit der letzten Überprüfung geändert wurden.
  - Kennzeichnung
  - Hostname
  - Kontaktname
  - Kontaktstandort
  - Speichergröße
  - Beidseitig
  - Verbrauchsmaterial (ohne Ebenen)
  - Einzugsoptionen
  - Ausgabeoptionen
  - eSF-Anwendungen
  - Standardruckerzertifikat
- **Verwaltete (gefundene) Drucker**: Drucker, die als fehlend gemeldet wurden, jetzt aber gefunden wurden.

- **Verwaltete (fehlende) Drucker**: Drucker, mit denen das System nicht kommunizieren konnte.
- **Verwaltete (normale) Drucker**: Drucker im System, deren Eigenschaften seit der letzten Überprüfung unverändert sind.
- **Neue Drucker**: Geräte, die neu gefunden wurden und nicht automatisch auf den Staus "Verwaltet" gesetzt wurden.
- **Stillgelegte Drucker**: Drucker, die nicht mehr im System aktiv sind.
- **Nicht verwaltete Drucker**: Drucker, die für im System ausgeführte Aktivitäten als ausgeschlossen gekennzeichnet wurden.



Anfangsstatus	Endstatus	Übergang
Starten	Normal	Gefunden.[1]
Starten	Neu	Gefunden.[2]
Beliebig	Normal, Nicht verwaltet oder Stillgelegt	Manuell ("Fehlt" ändert sich nicht in "Normal").
Stillgelegt	Normal	Gefunden.[1]
Stillgelegt	Neu	Gefunden.[2]
Normal, Fehlend oder Gefunden	Geändert	Neue Adresse, wenn gefunden.
Normal	Geändert	Überprüfungseigenschaften stimmen nicht mit Datenbankeigenschaften überein.
Normal, Geändert oder Gefunden	Fehlt	Nicht gefunden bei Prüfung oder Aktualisierungsstatus.
Geändert	Normal	Überprüfungseigenschaften stimmen mit Datenbankeigenschaften überein.
Fehlt	Gefunden	Gefunden, Prüfung oder Aktualisierungsstatus.
Gefunden	Normal	Gefunden, Prüfung oder Aktualisierungsstatus.

[1] Die Einstellung "Gefundene Drucker automatisch verwalten" ist im Suchprofil aktiviert.

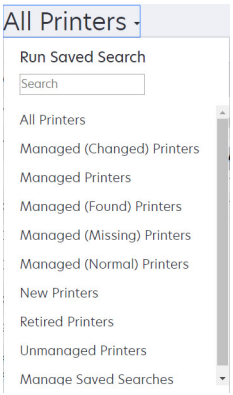
[2] Die Einstellung "Gefundene Drucker automatisch verwalten" ist im Suchprofil deaktiviert.

Ausführen eines gespeicherten Suchvorgangs

Eine gespeicherte Suche ist ein gespeicherter Parametersatz, der die neuesten Druckerinformationen zurückgibt, die den Parametern entsprechen.

Sie können eine benutzerdefinierte gespeicherte Suche erstellen und ausführen oder die vom System erzeugten und gespeicherten Standardsuchvorgänge ausführen. Vom System erzeugte gespeicherte Suchvorgänge zeigen die Drucker in folgenden Lebenszyklus-Statusarten: Weitere Informationen finden Sie unter "Informationen zu Lebenszyklus-Statusarten von Druckern" auf Seite 47.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie im Drop-down-Menü einen gespeicherten Suchvorgang aus.



Erstellen eines gespeicherten Suchvorgangs

Verwenden von Filtern

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie im linken Bereich der Seite die Filter aus.

   Hinweis: Die ausgewählten Filter werden oberhalb der Suchergebnis-Kopfzeile aufgeführt.
3. Klicken Sie auf **Speichern**, und geben Sie dann einen eindeutigen Namen für den gespeicherten Suchvorgang und seine Beschreibung ein.
4. Klicken Sie auf **Gespeicherten Suchvorgang erstellen**.

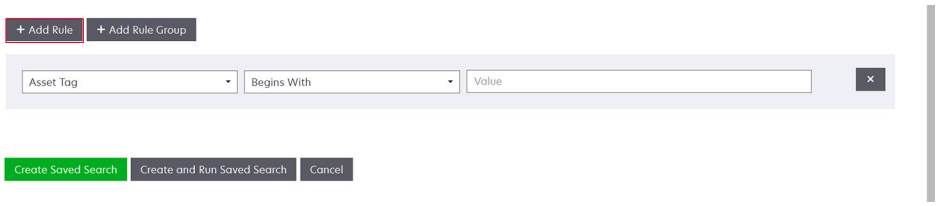
Verwenden der Seite "Gespeicherter Suchvorgang"

1. Klicken Sie im Menü Drucker auf **Gespeicherte Suchvorgänge** > **Erstellen**.
2. Geben Sie im Abschnitt Allgemein einen eindeutigen Namen für den gespeicherten Suchvorgang und seine Beschreibung ein.
3. Geben Sie im Abschnitt Regeln und Regelgruppen im Menü Übereinstimmung an, ob die Suchergebnisse allen oder beliebigen Regeln entsprechen müssen.
4. Führen Sie einen der folgenden Schritte aus:

Regel hinzufügen

a Klicken Sie auf **Regel hinzufügen**.

b Legen Sie den Parameter, Vorgang und Wert für Ihre Suchregel fest. Weitere Informationen finden Sie unter "Informationen zu Einstellungen für Suchkriterien" auf Seite 50.



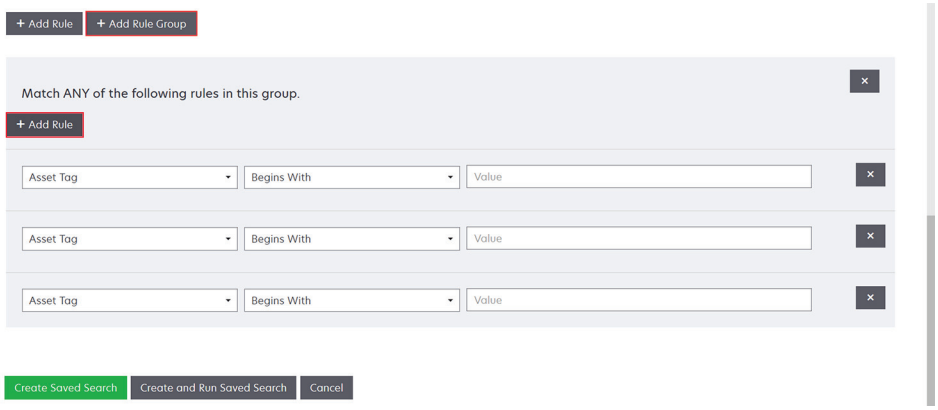
Regelgruppe hinzufügen

Eine Regelgruppe kann eine Kombination von Regeln enthalten. Wenn das Menü Übereinstimmung auf **BELIEBIGE Regeln und Regelgruppen** eingestellt ist, sucht das System nach Druckern, die beliebigen Regeln in der Regelgruppe entsprechen. Wenn das Menü Übereinstimmung auf **ALLE Regeln und Regelgruppen** eingestellt ist, sucht das System nach Druckern, die allen Regeln in der Regelgruppe entsprechen.

a Klicken Sie auf **Regelgruppe hinzufügen**.

b Legen Sie den Parameter, Vorgang und Wert für Ihre Suchregel fest. Weitere Informationen finden Sie unter "Informationen zu Einstellungen für Suchkriterien" auf Seite 50.

c Klicken Sie auf **Regel hinzufügen**, um eine weitere Regel hinzuzufügen.



5 Klicken Sie auf **Gespeicherten Suchvorgang erstellen** oder **Gespeicherten Suchvorgang erstellen und ausführen**.

Informationen zu Einstellungen für Suchkriterien

Suchen Sie nach Druckern mittels einem oder mehreren der folgenden Parameter:

Parameter	Beschreibung
Gerätenummer	Der Wert der Einstellung "Asset-Tag" auf dem Drucker.
Zertifikatserstellungsdatum[1]	Ruft das Datum ab, an dem das Zertifikat erstellt wurde.
Zertifikatsanmeldestatus[1]	Der Anmeldestatus des Zertifikats.
Ablaufdatum des Zertifikats[1]	Das Datum, an dem das Zertifikat abläuft.

Parameter	Beschreibung
Verlängerungsdatum des Zertifikats[1]	Das Datum, an dem das Zertifikat erneuert wird.
Zertifikatsprüfnummer[1]	Die Prüfnummer des Zertifikats.
Zertifikatssignaturstatus[1]	Der Status des Zertifikats.
Zertifikatsgültigkeitsstatus[1]	Die Gültigkeit des Zertifikats. **Hinweis:** Der Status Läuft bald ab zeigt an, dass das Zertifikat innerhalb von 30 Tagen abläuft.
Unterstützung des Farbdrucks	Der Drucker druckt in Farbe oder Schwarzweiß.
Konfiguration	Der dem Drucker zugewiesene Konfigurationsname.
Konfigurationskonformität	Der Konformitätsstatus des Druckers in Hinblick auf die zugewiesene Konfiguration.
Kontaktstandort	Der Wert der Einstellung "Kontaktstandort" auf dem Drucker.
Kontaktname	Der Wert der Einstellung "Kontaktname" auf dem Drucker.
Kopieren	Der Drucker unterstützt die Kopierfunktion.
Datum: Zu System hinzugefügt	Das Datum, an dem der Drucker zum System hinzugefügt wurde.
Datum: Zuletzt überprüft	Das Datum, an dem der Drucker zuletzt überprüft wurde.
Datum: Letzte Konformitätsprüfung	Das Datum, an dem die Konformität der Druckerkonfiguration zuletzt überprüft wurde.
Datum: Zuletzt gesucht	Das Datum, an dem der Drucker zuletzt erkannt wurde.
Festplattenverschlüsselung	Der Drucker ist für Festplattenverschlüsselung konfiguriert.
Löschen der Festplatte	Der Drucker ist für das Löschen der Festplatte konfiguriert.
Duplexmodus	Der Drucker unterstützt zweiseitigen Druck.
eSF-Funktion	Der Drucker unterstützt das Verwalten von eSF-Anwendungen.
eSF-Informationen	Die auf dem Drucker installierten Informationen über die eSF-Anwendung, wie beispielsweise Name, Status und Version.
Ereignisname	Der Name der zugewiesenen Ereignisse.
Faxname	Der Wert der Einstellung "Faxname" auf dem Drucker.
Faxnummer	Der Wert der Einstellung "Faxnummer" auf dem Drucker.
Fax-Empfang	Der Drucker unterstützt den Fax-Empfang.
Firmware-informationen	Informationen zu der auf dem Drucker installierten Firmware. • **Name**: Der Name der Firmware. Beispiel: **`Base`** oder **`Kernel`**. • **Version**: Die Version der Drucker-Firmware.
Hostname	Der Hostname des Druckers.
IP-Adresse	Die IP-Adresse des Druckers. **Hinweis:** Sie können in den letzten drei Oktetten ein Sternchen eingeben, um nach mehreren Einträgen zu suchen. Beispielsweise **`123.123.123.*`**, **`123.123.*.*`**, **`123.*.*.*`**, **`2001:db8::2:1`** und **`2001:db8:0:0:0:0:2:1`**.
Schlüsselwort	Die zugewiesenen Schlüsselwörter.
Insgesamt gedruckte Seiten	Der Wert der insgesamt gedruckten Seiten des Druckers.

Parameter	Beschreibung
MAC-Adresse	Die MAC-Adresse des Druckers.
Wartungszähler	Der Wert des Druckerwartungszählers.
Hersteller	Der Name des Druckerherstellers.
Kennzeichnungstechnologie	Die vom Drucker unterstützte Kennzeichnungstechnologie.
Unterstützung der MFP-Funktion	Beim Drucker handelt es sich um ein Multifunktionsgerät (MFP).
Modell	Der Name des Druckermodells.
Modulare Seriennummer	Die modulare Seriennummer.
Druckerstatus	Der Druckerstatus. Beispielsweise **`Bereit`**, **`Papierstau`**, **`Fach 1 fehlt`**.
Schweregrad Druckerstatus	Der Wert des Druckerstatus mit dem höchsten Schweregrad. Beispielsweise **`Unbekannt`**, **`Bereit`**, **`Warnung`** oder **`Fehler`**.
Profil	Der Drucker unterstützt Profile.
Scan to E-mail	Der Drucker unterstützt Scan to E-mail.
Scan to Fax	Der Drucker unterstützt Scan to Fax
Scan to Fax	Der Drucker unterstützt Scan to Fax
Sicherer Kommunikationsstatus	Der Gerätesicherheits- bzw. Authentifizierungsstatus.
Seriennummer	Die Seriennummer des Druckers.
Zustand	Der aktuelle Druckerstatus in der Datenbank.
Verbrauchsmaterialstatus	Der Verbrauchsmaterialstatus des Druckers.
Schweregrad Verbrauchsmaterialstatus	Der Wert des Druckerstatus mit dem höchsten Schweregrad für Verbrauchsmaterialien. Beispielsweise **`Unbekannt`**, **`OK`**, **`Warnung`** oder **`Fehler`**.
Systemname	Der Systemname des Druckers.
Zeitzone	Die Zeitzone der Region, in der sich der Drucker befindet.
TLI	Der Wert der Einstellung "TLI" auf dem Drucker.

[1]Zertifikatsparameter gelten für die folgenden Gerätezertifikate:

- **Standard**
- **HTTPS**
- **802.1x**
- **IPSec**

Verwenden Sie bei der Suche nach Druckern die folgenden Operatoren:

- **Entspricht genau**: Ein Parameter entspricht einem festgelegten Wert.
- **Entspricht nicht**: Ein Parameter entspricht nicht einem festgelegten Wert.
- **Enthält**: Ein Parameter enthält einen festgelegten Wert.
- **Enthält nicht**: Ein Parameter enthält einen festgelegten Wert nicht.
- **Beginnt mit**: Ein Parameter beginnt mit einem festgelegten Wert.
- **Endet mit**: Ein Parameter endet mit einem festgelegten Wert.

- **Datum**
  - **Älter als**: Ein Parameter für die Suche nach Tagen vor den angegebenen Tagen.
  - **Innerhalb der letzten**: Ein Parameter für die Suche innerhalb der vor dem heutigen Tag angegebenen Tage.
  - **Innerhalb der nächsten**: Ein Parameter für die Suche innerhalb der nach dem heutigen Tag angegebenen Tage.

Hinweis: Für die Suche nach Druckern, die Parameter mit leeren Werten haben, verwenden Sie **_EMPTY_OR_NULL_**. Wenn Sie beispielsweise nach Druckern suchen, bei denen Faxname leer ist, geben Sie im Feld Wert den Wert **_EMPTY_OR_NULL_** ein.

Verwalten von gespeicherten Suchvorgängen

1. Klicken Sie im Menü "Drucker" auf **Gespeicherte Suchvorgänge**.
2. Gehen Sie wie folgt vor:

Gespeicherte Suchvorgänge bearbeiten

a. Wählen Sie einen gespeicherten Suchvorgang aus, und klicken Sie dann auf **Bearbeiten**.

Hinweis: Vom System generierte, gespeicherte Suchvorgänge können nicht bearbeitet werden. Weitere Informationen finden Sie unter "Informationen zu Lebenszyklus-Statusarten von Druckern" auf Seite 47.

b. Konfigurieren Sie die Einstellungen.

c. Klicken Sie auf **Änderungen speichern** oder **Speichern und Ausführen**.

Gespeicherte Suchvorgänge kopieren

a. Wählen Sie einen gespeicherten Suchvorgang aus, und klicken Sie dann auf **Kopieren**.

b. Konfigurieren Sie die Einstellungen.

c. Klicken Sie auf **Gespeicherten Suchvorgang erstellen** oder **Gespeicherten Suchvorgang erstellen und ausführen**.

Gespeicherte Suchvorgänge löschen

a. Wählen Sie mindestens einen gespeicherten Suchvorgang aus.

Hinweis: Vom System generierte, gespeicherte Suchvorgänge können nicht gelöscht werden. Weitere Informationen finden Sie unter "Informationen zu Lebenszyklus-Statusarten von Druckern" auf Seite 47.

b. Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Beispielszenario: Überwachung der Tonerstände Ihrer Flotte

Als IT-Mitarbeiter von Unternehmen ABC müssen Sie die Druckerflotte organisieren, um sie einfach zu überwachen. Sie möchten den Tonerverbrauch der Drucker überwachen, um festzustellen, ob das Verbrauchsmaterial ausgetauscht werden muss.

Beispielimplementierung

1. Erstellen Sie einen gespeicherten Suchvorgang, der die Drucker abruft, für deren Verbrauchsmaterialien es Fehler oder Warnungen gibt.

   Beispielregel für Ihre gespeicherte Suche

   Parameter: **Schweregrad Verbrauchsmaterialstatus**

   Vorgang: **Ist nicht**

   Wert: **Verbrauchsmaterial OK**

2. Erstellen Sie eine Ansicht, die den Verbrauchsmaterialstatus, die Kapazität und den Verbrauchsstand für jeden Drucker anzeigt.

   Beispielspalten, die in der Verbrauchsmaterialansicht angezeigt werden

   Verbrauchsmaterialstatus

   Tonerkassette Schwarz, Kapazität

   Tonerkassette Schwarz, Verbrauchsstand

   Tonerkassette Cyan, Kapazität

   Tonerkassette Cyan, Verbrauchsstand

   Tonerkassette Magenta, Kapazität

   Tonerkassette Magenta, Verbrauchsstand

   Tonerkassette Gelb, Kapazität

   Tonerkassette Gelb, Verbrauchsstand

3. Führen Sie die gespeicherte Suche unter Verwendung der Ansicht aus.

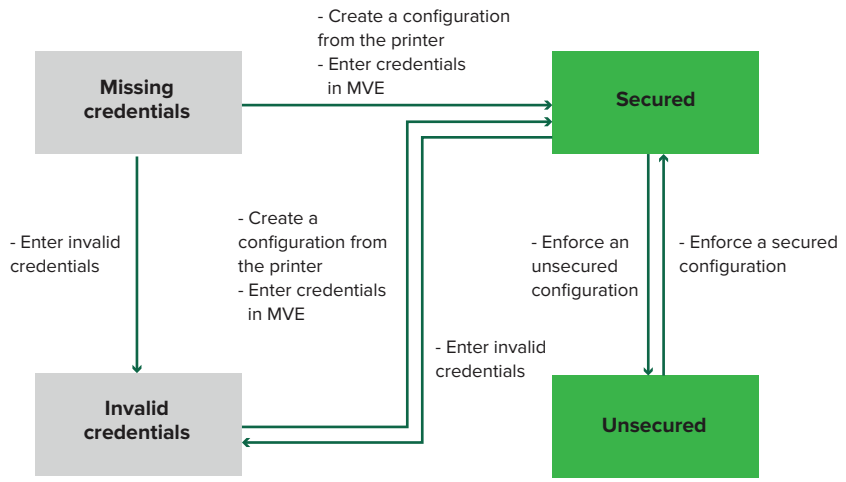
   Hinweis: Die in der Druckerlistenansicht angezeigten Informationen basieren auf der letzten Prüfung. Führen Sie eine Prüfung und eine Statusaktualisierung durch, um den aktuellen Druckerstatus abzurufen.

Sichern der Druckerkommunikation

Bedeutung des Druckersicherheitsstatus

Während der Suche kann sich der Drucker in einem der folgenden Sicherheitsstatus befinden:

- **Ungesichert**: MVE benötigt keine Anmeldeinformationen, um mit dem Gerät zu kommunizieren.
- **Gesichert**: MVE benötigt Anmeldeinformationen, und diese wurden angegeben.
- **Fehlende Anmeldeinformationen**: MVE benötigt Anmeldeinformationen, diese wurden aber nicht angegeben.
- **Ungültige Anmeldeinformationen**: MVE benötigt Anmeldeinformationen, jedoch wurden falsche Anmeldeinformationen angegeben.



Ein Drucker befindet sich im Status Ungültige Anmeldeinformationen, wenn die Anmeldeinformationen während der Suche, Prüfung, Statusaktualisierung, Konformitätsprüfung oder Konfigurationsdurchsetzung ungültig sind.

Der Drucker befindet sich nur dann im Status Ungesichert, wenn während der Suche keine Anmeldeinformationen erforderlich sind.

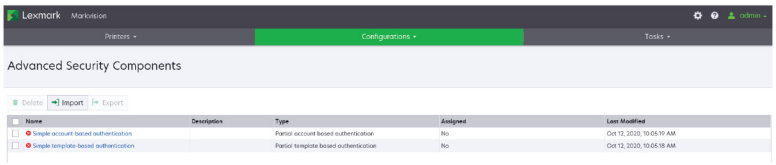
Erzwingen Sie zum Ändern des Status von Ungesichert in Gesichert eine gesicherte Konfiguration.

Um einen Drucker aus dem Status Fehlende Anmeldeinformationen oder Ungültige Anmeldeinformationen zu verschieben, geben Sie die Anmeldeinformationen manuell in MVE ein, oder erstellen Sie eine Konfiguration vom Drucker.

Sichern von Druckern unter Verwendung der Standardkonfigurationen

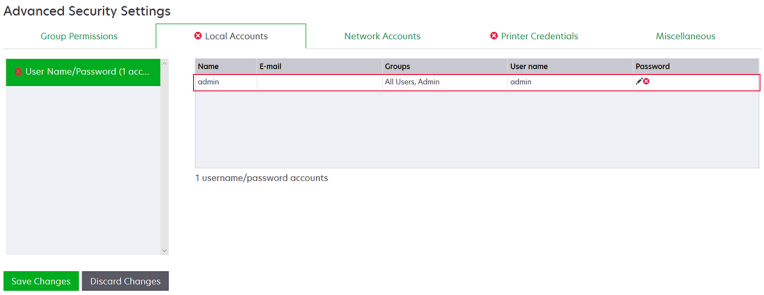
Bei einigen Druckermodellen gibt es keinen Standardadministrator-Benutzer. Gastbenutzer haben offenen Zugriff und sind nicht angemeldet. Diese Einrichtung gewährt Benutzern Zugriff auf alle Druckerberechtigungen und Zugriffssteuerungen. MVE behandelt dieses Risiko durch Standardkonfigurationen. Nach einer Neuinstallation werden automatisch zwei erweiterte Sicherheitskomponenten erstellt. Jede Komponente enthält die Standardsicherheitseinstellungen und das vorkonfigurierte lokale Administratorkonto. Sie können diese Sicherheitskomponenten beim Erstellen einer Konfiguration verwenden und anschließend die Konfiguration auf den neuen Druckern bereitstellen und durchsetzen.

Klicken Sie im Menü Konfigurationen auf **Alle erweiterten Sicherheitskomponenten**.

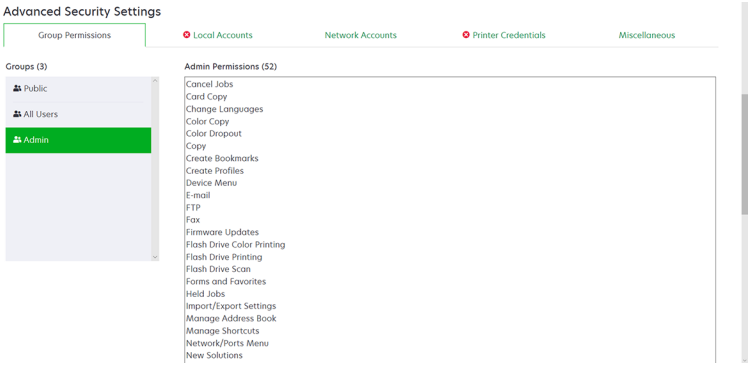


Einfache kontobasierte Authentifizierung

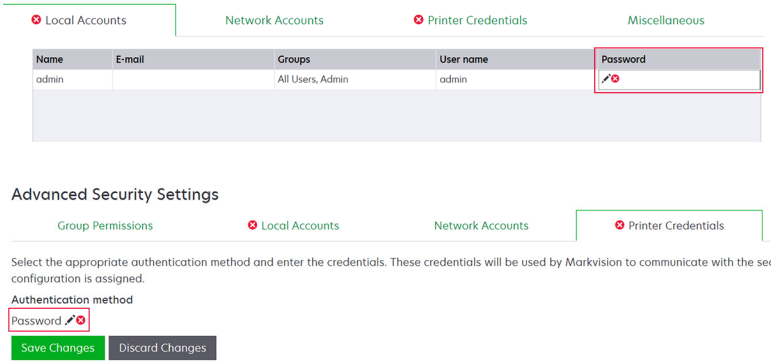
Diese Sicherheitskomponente enthält ein lokales Konto (Benutzername/Passwort) mit dem Namen **admin**.



Das **Administratorkonto** ist ein Mitglied der Admin-Gruppe, zu deren Berechtigungen Funktionszugriffssteuerungen und Berechtigungen gehören, um den Drucker zu sichern und den öffentlichen Zugriff einzuschränken. Weitere Informationen finden Sie unter "Bedeutung von Berechtigungen und Funktionszugriffssteuerungen" auf Seite 58.

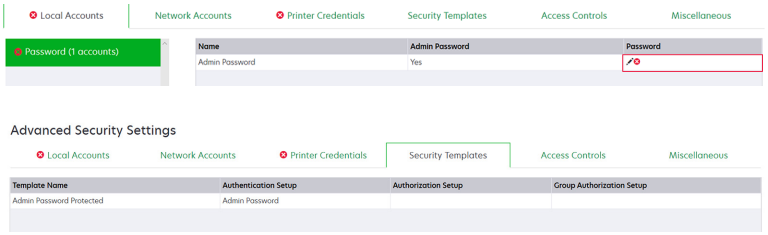


Stellen Sie vor dem Hinzufügen dieser Komponente zu einer Konfiguration sicher, dass Sie das **Administratorkennwort** und die Anmeldeinformationen des Druckers festgelegt haben.



Einfache vorlagenbasierte Authentifizierung

Diese Sicherheitskomponente enthält eine Sicherheitsvorlage namens Admin kennwortgesichert, die mit einem lokalen Kennwortkonto konfiguriert ist.

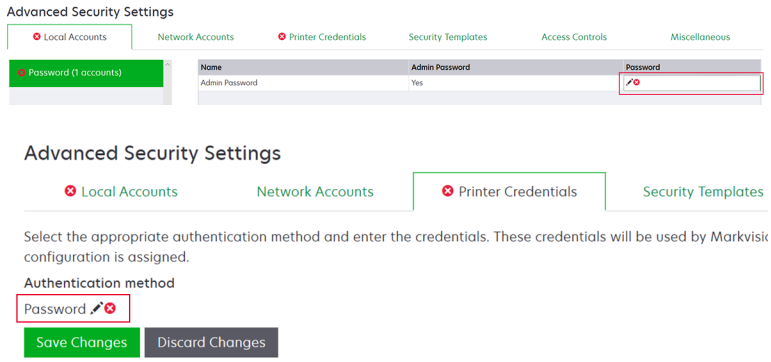


Diese Sicherheitsvorlage wird auf die folgenden Zugriffssteuerungen angewendet:

- Firmware-Aktualisierungen
- Remote-Verwaltung
- Sicherheitsmenü, standortfern

Die übrigen Zugriffssteuerungen sind auf **Keine Sicherheit** eingestellt. Sie können jedoch immer die anderen Druckerverwaltungsmenüs so einstellen, dass die Sicherheitsvorlage für mehr Schutz verwendet wird. Weitere Informationen zu den Zugriffssteuerungen finden Sie unter "Bedeutung von Berechtigungen und Funktionszugriffssteuerungen" auf Seite 58.

Achten Sie darauf, vor dem Hinzufügen dieser Komponente zu einer Konfiguration das Kennwort und die Anmeldeinformationen des Druckers festzulegen.



Bedeutung von Berechtigungen und Funktionszugriffssteuerungen

Drucker können so konfiguriert werden, dass der öffentliche Zugriff auf Verwaltungsmenüs und Geräteverwaltungsfunktionen eingeschränkt wird. Bei neueren Druckermodellen können Berechtigungen für den Zugriff auf Druckerfunktionen über verschiedene Authentifizierungsmethoden gesichert werden. Bei älteren Druckermodellen kann eine Sicherheitsvorlage auf eine Funktionszugriffssteuerung (Function Access Control, FAC) angewendet werden.

Um mit diesen gesicherten Druckern zu kommunizieren und diese zu verwalten, benötigt MVE je nach Druckermodell bestimmte Berechtigungen oder FACs.

In der folgenden Tabelle wird erläutert, welche Druckerverwaltungsfunktionen in MVE verwaltet werden können und welche Berechtigungen oder FACs erforderlich sind.

Beachten Sie, dass MVE die Authentifizierungsinformationen benötigt, wenn die Remote-Verwaltung gesichert ist. Wenn andere Verwaltungsmenüs und Geräteverwaltungsberechtigungen oder FACs gesichert sind, muss die Remote-Verwaltung ebenfalls gesichert sein. Andernfalls kann MVE die Funktionen nicht ausführen.

Diese Berechtigungen und Funktionszugriffssteuerungen sind in MVE als standardmäßige erweiterte Sicherheitskomponenten vordefiniert und können problemlos in einer Konfiguration verwendet werden. Weitere Informationen finden Sie unter "Sichern von Druckern unter Verwendung der Standardkonfigurationen" auf Seite 56.

Wenn Sie die erweiterten Standardsicherheitskomponenten nicht verwenden, stellen Sie sicher, dass diese Berechtigungen und Funktionszugriffssteuerungen im Drucker manuell konfiguriert sind. Weitere Informationen finden Sie unter "Konfigurieren der Druckersicherheit" auf Seite 59.

Berechtigungen oder FACs	Beschreibung
Remote-Verwaltung	Die Möglichkeit, Einstellungen per Fernzugriff zu lesen und zu schreiben. Wenn andere in dieser Tabelle aufgeführte Berechtigungen oder FACs gesichert sind, muss die Remote-Verwaltung ebenfalls gesichert sein.
Firmware-Aktualisierungen	Die Möglichkeit, Firmware über jede beliebige Methode zu aktualisieren.
Konfiguration der Anwendungen	Die Möglichkeit, Anwendungen auf dem Drucker zu installieren oder zu entfernen und Dateien mit Anwendungseinstellungen an den Drucker zu senden.
Alle Einstellungen importieren/exportieren oder **Konfigurationsdatei importieren/exportieren**	Die Möglichkeit, Konfigurationsdateien an den Drucker zu senden.
Menü "Sicherheit" oder **Remote-Sicherheitsmenü**	Die Möglichkeit, Anmeldemethoden zu verwalten und Druckersicherheitsoptionen zu konfigurieren.

Um neuere Druckermodelle in MVE zu sichern, deaktivieren Sie den öffentlichen Zugriff auf die Berechtigungen für die Remote-Verwaltung und das Menü "Sicherheit". Wenden Sie bei älteren Druckermodellen eine Sicherheitsvorlage auf die FAC Remote-Verwaltung an.

Konfigurieren der Druckersicherheit

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Klicken Sie auf die IP-Adresse des Druckers, und klicken Sie anschließend auf **Embedded Web Server öffnen**.
3. Klicken Sie auf **Einstellungen** oder **Konfiguration**.
4. Führen Sie je nach Druckermodell einen der folgenden Schritte aus:
   - Klicken Sie auf **Sicherheit** > **Anmeldemethoden**, und gehen Sie wie folgt vor:

     ### Für neuere Druckermodelle

     a. Erstellen Sie im Abschnitt Sicherheit eine Anmeldemethode.
     b. Klicken Sie neben der Anmeldemethode auf **Gruppen/Berechtigungen verw.** oder **Berechtigungen verw.**
     c. Erweitern Sie die **Verwaltungsmenüs**, und wählen Sie anschließend das Menü **Sicherheit** aus.
     d. Erweitern Sie die **Geräteverwaltung**, und wählen Sie die folgenden Berechtigungen aus:
        - **Remote-Verwaltung**
        - **Firmware-Aktualisierungen**
        - **Konfiguration der Anwendungen**
        - **Alle Einstellungen importieren/exportieren**
     e. Klicken Sie auf **Speichern**.
     f. Klicken Sie im Abschnitt Öffentlich auf **Berechtigungen verwalten**.
     g. Erweitern Sie die **Verwaltungsmenüs**, und löschen dann die Auswahl des Menüs **Sicherheit**.
     h. Erweitern Sie **Geräteverwaltung**, und löschen Sie dann die Auswahl für **Remote-Verwaltung**.
     i. Klicken Sie auf **Speichern**.

   - Klicken Sie auf **Sicherheit** > **Sicherheitseinstellung** oder **Sicherheitseinstellung bearbeiten**, und gehen Sie dann wie folgt vor:

     ### Für ältere Druckermodelle

     a. Erstellen Sie im Abschnitt Erweiterte Sicherheitseinrichtung einen Baustein und eine Sicherheitsvorlage.
     b. Klicken Sie auf **Zugriffssteuerungen**, und erweitern Sie die **Verwaltungsmenüs**.
     c. Wählen Sie im Remote-Sicherheitsmenü die Sicherheitsvorlage aus.
     d. Erweitern Sie **Verwaltung**, und wählen Sie dann die Sicherheitsvorlage für die folgenden Funktionszugriffssteuerungen aus:
        - **Konfiguration der Anwendungen**
        - **Remote-Verwaltung**
        - **Firmware-Aktualisierungen**
        - **Konfigurationsdatei importieren/exportieren**
     e. Klicken Sie auf **Übernehmen**.

Sichern der Kommunikation in der Druckerflotte

1. Suchen Sie einen gesicherten Drucker. Weitere Informationen finden Sie unter "Erkennen von Druckern" auf Seite 34.

   Hinweise:

   - Ein Drucker ist gesichert, wenn  daneben angezeigt wird. Weitere Informationen zum Sichern eines Druckers finden Sie im **Hilfedokument**.
   - Weitere Informationen zum Druckersicherheitsstatus finden Sie unter "Bedeutung des Druckersicherheitsstatus" auf Seite 55.

2. Erstellen Sie eine Konfiguration über einen Drucker. Weitere Informationen finden Sie unter "Erstellen einer Konfiguration über einen Drucker" auf Seite 72.
3. Weisen Sie die Konfiguration der Druckerflotte zu. Weitere Informationen finden Sie unter "Zuweisen von Konfigurationen zu Druckern" auf Seite 62.
4. Setzen Sie die Konfiguration durch. Weitere Informationen finden Sie unter "Durchsetzen von Konfigurationen" auf Seite 63. Neben dem gesicherten Drucker wird ein Vorhängeschloss-Symbol angezeigt.

Andere Möglichkeiten, Ihre Drucker zu schützen

Weitere Informationen zur Konfiguration für Sicherheitseinstellungen von Druckern finden Sie im *Administratorhandbuch zu Embedded Web Server* für Ihren Drucker.

Überprüfen Sie Ihre Drucker auf die folgenden Einstellungen:

- Festplattenverschlüsselung ist aktiviert.
- Folgende Anschlüsse sind eingeschränkt:
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- Die Standard-Ziffernliste ist die OWASP-Ziffernzeichenfolge "B.".

Verwalten von Druckern

Neustarten des Druckers

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Klicken Sie auf die IP-Adresse des Druckers.
3. Klicken Sie auf **Drucker neu starten**.

Anzeigen des Embedded Web Servers des Druckers

Der Embedded Web Server ist eine im Drucker integrierte Software, mit der eine Bedienkonsole bereitgestellt wird, über die das Konfigurieren des Druckers von jedem Webbrowser aus möglich ist.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Klicken Sie auf die IP-Adresse des Druckers.
3. Klicken Sie auf **Embedded Web Server öffnen**.

Überprüfen von Druckern

Bei einer Prüfung werden Informationen der Drucker im Status "Verwaltet" erfasst und dann im System gespeichert. Führen Sie regelmäßige Prüfungen durch, um sicherzustellen, dass die Informationen im System aktuell sind.

1. Klicken Sie im Menü "Drucker" auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Drucker** > **Überwachung**.

   Hinweis: Die Durchführung einer Prüfung kann in regelmäßigen Abständen geplant werden. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Aktualisieren des Druckerstatus

Mit der Funktion "Status aktualisieren" können Sie den Druckerstatus aktualisieren, während sie gleichzeitig Informationen bereitstellt. Um sicherzustellen, dass der Druckerstatus und die Verbrauchsmaterialinformationen aktuell sind, aktualisieren Sie den Status regelmäßig.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Drucker** > **Status aktualisieren**.

   Hinweis: Eine Status-Aktualisierung kann so geplant werden, dass sie in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Einstellen des Druckerstatus

Weitere Informationen zu Druckerstatus finden Sie unter "Informationen zu Lebenszyklus-Statusarten von Druckern" auf Seite 47.

1. Klicken Sie im Menü "Drucker" auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Drucker**, und wählen Sie dann eine der folgenden Optionen aus:
   - **Status auf "Verwaltet" setzen**— Der Drucker wird in sämtliche Aktivitäten, die im System ausgeführt werden können, einbezogen.
   - **Status auf "Nicht Verwaltet" setzen**— Der Drucker wird von sämtlichen Aktivitäten, die im System ausgeführt werden können, ausgeschlossen.
   - **Status auf "Nicht verwendet" setzen**— Der Drucker wird aus dem Netzwerk entfernt. Das System behält die Druckerinformationen, geht aber nicht davon aus, das Gerät wieder im Netzwerk zu entdecken.

Zuweisen von Konfigurationen zu Druckern

Stellen Sie zunächst sicher, dass eine Konfiguration für den Drucker erstellt wurde. Durch das Zuweisen einer Konfiguration zu einem Drucker kann das System Übereinstimmungsprüfung und Durchsetzung ausführen. Weitere Informationen finden Sie unter "Erstellen einer Konfiguration" auf Seite 69.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Konfigurationen zuweisen**.
4. Wählen Sie im Abschnitt Konfiguration eine Konfiguration aus.

   Hinweis: Wenn das System auf **Markvision verwenden, um Gerätezertifikate zu verwalten** eingestellt ist, wählen Sie die Option **Ausgewählten Geräten vertrauen** aus. Mit dieser Bestätigung können Benutzer überprüfen, ob es sich bei den Druckern um echte Geräte und nicht um vorgetäuschte Geräte handelt.
5. Klicken Sie auf **Konfigurationen zuweisen**.

Aufheben der Zuweisung von Konfigurationen

1. Klicken Sie im Menü "Drucker" auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Zuweisen der Konfigurationen aufheben**.
4. Klicken Sie auf **Zuweisen der Konfigurationen aufheben**.

Durchsetzen von Konfigurationen

MVE führt eine Übereinstimmungsprüfung am Drucker durch. Wenn einige Einstellungen nicht übereinstimmen, ändert MVE diese Einstellungen des Druckers. Im Anschluss an die Einstellungsänderungen führt MVE eine abschließende Übereinstimmungsprüfung durch. Zum Abschluss von Updates, die einen Neustart des Druckers erfordern, beispielsweise Firmware-Aktualisierungen, ist möglicherweise eine zweite Durchsetzung nötig.

Stellen Sie zunächst sicher, dass dem Drucker eine Konfiguration zugewiesen ist. Weitere Informationen finden Sie unter "Zuweisen von Konfigurationen zu Druckern" auf Seite 62.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Konfigurationen durchsetzen**.

Hinweise:

- Wenn sich der Drucker in einem Fehlerstatus befindet, werden einige Einstellungen möglicherweise nicht aktualisiert.
- Damit MVE Firmware- und Lösungsdateien für einen Drucker bereitstellen kann, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen auf **Keine Sicherheit** eingestellt werden. Wenn Sicherheit angewandt wird, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen die gleiche Sicherheitsvorlage verwenden wie die Funktionszugriffssteuerung für die Remote-Verwaltung. Weitere Informationen finden Sie unter "Bereitstellen von Dateien für Drucker" auf Seite 64.
- Eine Durchsetzung kann so geplant werden, dass sie in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Prüfen der Druckerübereinstimmung mit einer Konfiguration

Während einer Übereinstimmungsprüfung prüft MVE die Druckereinstellungen und überprüft, ob sie der zugewiesenen Konfiguration entsprechen. Während dieses Vorgangs nimmt MVE keine Änderungen am Drucker vor.

Stellen Sie zunächst sicher, dass dem Drucker eine Konfiguration zugewiesen ist. Weitere Informationen finden Sie unter "Zuweisen von Konfigurationen zu Druckern" auf Seite 62.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Übereinstimmung prüfen**.

   Hinweise:

   - Sie können die Ergebnisse auf der Statusseite der Aufgabe anzeigen.
   - Eine Übereinstimmungsprüfung kann so geplant werden, dass sie in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Bereitstellen von Dateien für Drucker

Sie können folgende Dateien für den Drucker bereitstellen:

- **CA-Zertifikate**—**.cer** - oder **.pem** -Dateien, die zum vertrauenswürdigen Druckerspeicher hinzugefügt werden.
- **Konfigurationpaket**—**.zip** -Dateien, die über einen unterstützten Drucker exportiert oder direkt von Lexmark erhalten werden.
- **Firmware-Aktualisierung**—Eine **.fls** -Datei, die an den Drucker geflasht wird.
- **Generische Datei**—Beliebige Datei, die Sie an den Drucker senden möchten.
  - **Raw Socket**—Über Port 9100 gesendet. Der Drucker behandelt dies wie alle anderen Druckdaten.
  - **FTP**—Datei über FTP senden. Diese Bereitstellungsmethode wird bei gesicherten Druckern nicht unterstützt.
- **Drucker-Zertifikat**—Ein signiertes Zertifikat, das als Standard-Zertifikat auf dem Drucker installiert ist.
- **Universelle Konfigurationsdatei (UCF)**—Eine Konfigurationsdatei, die von einem Drucker exportiert wurde.
  - **Webdienst**—Der HTTPS-Webdienst wird verwendet, wenn das Druckermodell diesen unterstützt. Andernfalls verwendet der Drucker den HTTP-Webdienst.
  - **FTP**—Datei über FTP senden. Diese Bereitstellungsmethode wird bei gesicherten Druckern nicht unterstützt.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Datei für Drucker bereitstellen**.
4. Klicken Sie auf **Datei auswählen**, und navigieren Sie dann zur Datei.
5. Wählen Sie einen Dateityp aus, und wählen Sie dann eine Bereitstellungsmethode aus.
6. Klicken Sie auf **Datei bereitstellen**.

Hinweise:

- Damit MVE Firmware- und Lösungsdateien für einen Drucker bereitstellen kann, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen auf **Keine Sicherheit** eingestellt werden. Wenn Sicherheit angewandt wird, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen die gleiche Sicherheitsvorlage verwenden wie die Funktionszugriffssteuerung für die Remote-Verwaltung.
- Eine Datei-Bereitstellung kann so geplant werden, dass sie in regelmäßigen Abständen stattfindet. Weitere Informationen finden Sie unter "Erstellen eines Zeitplans" auf Seite 147.

Aktualisieren der Drucker-Firmware

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.
3. Klicken Sie auf **Konfigurieren** > **Firmwareaktualisierung zu Druckern**.

4 Wählen Sie eine Firmware-Datei aus der Ressourcenbibliothek aus, oder klicken Sie auf **Datei auswählen**, und navigieren Sie dann zur Firmware-Datei.

   Hinweis: Weitere Informationen zum Hinzufügen von Firmware-Dateien zur Bibliothek finden Sie unter "Importieren von Dateien in die Ressourcenbibliothek" auf Seite 76.

5 Falls erforderlich, können Sie eine Zeit für die Aktualisierung wählen, indem Sie **Aktualisierungsfenster festlegen** auswählen und dann die Start- und Unterbrechungszeit und die Wochentage festlegen.

   Hinweis: Die Firmware wird innerhalb der angegebenen Start- und Unterbrechungszeit an die Drucker gesendet. Die Aufgabe wird nach der Unterbrechungszeit angehalten, und zur nächsten Startzeit bis zum Abschluss weitergeführt.

6 Klicken Sie auf **Firmware aktualisieren**.

Hinweis: Damit MVE die Drucker-Firmware aktualisieren kann, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen auf **Keine Sicherheit** eingestellt sein. Wenn Sicherheit angewandt wird, muss die Funktionszugriffssteuerung für Firmware-Aktualisierungen die gleiche Sicherheitsvorlage verwenden wie die Funktionszugriffssteuerung für die Remote-Verwaltung. In diesem Fall muss MVE den Drucker sicher verwalten. Weitere Informationen finden Sie unter "Sichern der Druckerkommunikation" auf Seite 55.

Deinstallieren von Anwendungen auf Druckern

MVE kann nur Anwendungen deinstallieren, die dem System im Package Builder-Format hinzugefügt wurden. Weitere Informationen zum Hochladen von Anwendungen zum System finden Sie unter "Importieren von Dateien in die Ressourcenbibliothek" auf Seite 76.

1 Klicken Sie im Menü Drucker auf **Druckerliste**.

2 Wählen Sie einen oder mehrere Drucker aus.

3 Klicken Sie auf **Konfigurieren** > **Apps auf Druckern deinstallieren**.

4 Wählen Sie die Anwendungen aus.

5 Klicken Sie auf **Apps deinstallieren**.

Zuweisen von Ereignissen zu Druckern

Durch das Zuweisen von Ereignissen zu Druckern kann MVE die zugehörige Aktion ausführen, sobald eine der zugehörigen Warnungen auf dem zugewiesenen Drucker auftritt. Weitere Informationen zum Erstellen von Ereignissen finden Sie unter "Verwalten von Druckerwarnungen" auf Seite 137.

Hinweis: Ereignisse können nur ungesicherten Druckern zugewiesen werden.

1 Klicken Sie im Menü "Drucker" auf **Druckerliste**.

2 Wählen Sie einen oder mehrere Drucker aus.

3 Klicken Sie auf **Zuweisen** > **Ereignisse**.

4 Wählen Sie ein oder mehrere Ereignisse aus.

Hinweis: Wenn einigen der ausgewählten Drucker bereits das Ereignis zugewiesen wurde, wird ein Bindestrich im Kontrollkästchen angezeigt. Wenn Sie den Bindestrich dort stehen lassen, wird das Ereignis nicht verändert. Wenn Sie dieses Kontrollkästchen aktivieren, wird das Ereignis allen ausgewählten Druckern zugewiesen. Wenn Sie das Kontrollkästchen deaktivieren, wird die Zuordnung des Ereignisses zu den Druckern, denen es zuvor zugewiesen war, aufgehoben.

5 Klicken Sie auf **Ereignisse zuweisen**.

Zuweisen von Stichwörtern zu Druckern

Durch das Zuweisen von Stichwörtern zu Druckern können Sie Ihre Drucker organisieren. Weitere Informationen zum Erstellen von Stichwörtern finden Sie unter "Verwalten von Schlüsselwörtern" auf Seite 47.

1 Klicken Sie im Menü "Drucker" auf **Druckerliste**.

2 Wählen Sie einen oder mehrere Drucker aus.

3 Klicken Sie auf **Zuweisen** > **Stichwörter**.

4 Wählen Sie ggf. im Menü "Anzeigen" eine Kategorie aus.

5 Wählen Sie ein oder mehrere Stichwörter aus.

Hinweis: Stichwörter werden nach Kategorien aufgeführt. Wenn einigen der ausgewählten Drucker bereits ein Schlüsselwort zugewiesen wurde, wird ein Bindestrich im Kontrollkästchen angezeigt. Wenn Sie den Bindestrich stehen lassen, wird das Schlüsselwort den ausgewählten Druckern nicht zugeordnet oder die Zuordnung wird aufgehoben. Wenn Sie dieses Kontrollkästchen aktivieren, wird das Schlüsselwort allen ausgewählten Druckern zugewiesen. Wenn Sie das Kontrollkästchen deaktivieren, wird die Zuordnung des Schlüsselworts zu den Druckern, denen es zuvor zugewiesen war, aufgehoben.

6 Klicken Sie auf **Stichwörter zuweisen**.

Eingeben von Anmeldeinformationen für gesicherte Drucker

Gesicherte Drucker können erkannt und integriert werden. Um mit diesen Druckern zu kommunizieren, können Sie entweder eine Konfiguration erzwingen oder die Anmeldeinformationen direkt in MVE eingeben.

Hinweis: Ein Drucker ist gesichert, wenn daneben angezeigt wird.

Um die Anmeldeinformationen einzugeben, verfahren Sie wie folgt:

1 Klicken Sie im Menü Drucker auf **Druckerliste**.

2 Wählen Sie einen oder mehrere gesicherte Drucker aus.

3 Klicken Sie auf **Sicherheit** > **Anmeldeinformationen eingeben**.

4 Wählen Sie die Authentifizierungsmethode aus, und geben Sie dann die Anmeldeinformationen ein.

5 Klicken Sie auf **Anmeldeinformationen eingeben**.

Hinweis: Integrierte Drucker, die gesichert sind, für die aber nicht die richtigen Anmeldeinformationen in MVE gespeichert sind, werden unter dem Filter Kommunikationen als Fehlende Anmeldeinformationen gekennzeichnet. Nach Eingabe der richtigen Anmeldeinformationen werden die Drucker als Gesichert gekennzeichnet.

Manuelles Konfigurieren von Standarddruckerzertifikaten

Wenn MVE nicht die Funktion zur automatischen Zertifikatsverwaltung verwendet, kann es Ihnen helfen, das Standarddruckerzertifikat für eine Druckerflotte zu signieren. MVE sammelt die Anforderungen der Druckerflotte zum Signieren von Zertifikaten und stellt nach dem Signieren die signierten Zertifikate für die richtigen Drucker bereit.

Ein Systemadministrator muss Folgendes tun:

1. Erzeugen Sie die Signieranforderungen für Druckerzertifikate.
   a. Klicken Sie im Menü Drucker auf **Druckerliste**.
   b. Wählen Sie einen oder mehrere Drucker aus.
   c. Klicken Sie auf **Sicherheit** > **Signieranforderungen für Druckerzertifikate erzeugen**.

   Hinweis: Sie können bei der Erzeugung von Zertifikatssignieranforderungen einen oder mehrere Drucker auswählen, aber nur maximal ein Satz Anforderungen kann vorhanden sein. Um vorhandene Zertifikatssignieranforderungen nicht zu überschreiben, müssen Sie die Zertifikatssignieranforderungen herunterladen, bevor Sie einen weiteren Satz erzeugen.
2. Warten Sie, bis die Aufgabe beendet ist, und laden Sie anschließend die Signieranforderungen für Druckerzertifikate herunter.
   a. Klicken Sie im Menü Drucker auf **Druckerliste**.
   b. Klicken Sie auf **Sicherheit** > **Herunterladen von Signieranforderungen für Druckerzertifikate**.
3. Verwenden Sie eine vertrauenswürdige Zertifizierungsstelle zum Signieren der Zertifikatssignieranforderungen.
4. Speichern Sie die signierten Zertifikate in einer ZIP-Datei.

   Hinweis: Alle signierten Zertifikate müssen sich im Stammverzeichnis der ZIP-Datei befinden. Andernfalls kann MVE die Datei nicht analysieren.
5. Klicken Sie im Menü Drucker auf **Druckerliste**.
6. Wählen Sie einen oder mehrere Drucker aus.
7. Klicken Sie auf **Konfigurieren** > **Datei für Drucker bereitstellen**.
8. Klicken Sie auf **Datei auswählen**, und navigieren Sie anschließend zur ZIP-Datei.
9. Wählen Sie im Menü Dateityp die Option **Druckerzertifikate** aus.
10. Klicken Sie auf **Datei bereitstellen**.

Entfernen von Druckern

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie einen oder mehrere Drucker aus.

3 Klicken Sie auf **Drucker**.

4 Falls es notwendig ist, das Druckerzertifikat zu entfernen, wählen Sie die Option **Zugeordnete(s) Gerätezertifikat(e) löschen** aus.

Hinweis: Wenn MVE die Gerätezertifikate verwaltet, wird beim Entfernen des Druckerzertifikats das Standardzertifikat vom Drucker gelöscht. Der Drucker erzeugt daraufhin ein neues signiertes Zertifikat.

5 Führen Sie einen der folgenden Schritte aus:

- Um die Druckerinformationen beizubehalten, klicken Sie auf **Drucker stilllegen**.
- Um den Drucker aus Ihrem System zu entfernen, klicken Sie auf **Drucker löschen**.

Verwalten von Konfigurationen

Übersicht

MVE verwendet Konfigurationen zur Verwaltung der Drucker in Ihrer Druckerflotte.

Eine Konfiguration ist eine Zusammenfassung von Einstellungen, die einem Drucker oder einer Gruppe von Druckermodellen zugewiesen und durchgesetzt werden können. Innerhalb einer Konfiguration können Sie Druckereinstellungen ändern und Anwendungen, Lizenzen, Firmware und CA-Zertifikate für die Drucker bereitstellen.

Sie können eine Konfiguration erstellen, die aus Folgendem besteht:

- Grundlegende Druckereinstellungen
- Erweiterte Sicherheitseinstellungen
- Farbdruckberechtigungen

  Hinweis: Diese Einstellung ist nur in Konfigurationen für unterstützte Farbdrucker verfügbar.
- Drucker-Firmware
- Anwendungen
- CA-Zertifikate
- Ressourcendateien

Durch die Verwendung von Konfigurationen haben Sie folgende Möglichkeiten zur Verwaltung der Drucker:

- Weisen Sie den Druckern Konfigurationen zu.
- Durchsetzung von Konfiguration an den Druckern. Die in der Konfiguration angegebenen Einstellungen werden auf die Drucker angewendet. Firmware, Anwendungen, Druckerzertifikat, Anwendungsdateien (.fls) und CA-Zertifikate sind installiert.
- Prüfen Sie, ob die Drucker mit einer Konfiguration übereinstimmen. Wenn keine Übereinstimmung vorhanden ist, kann die Konfiguration am Drucker durchgesetzt werden.

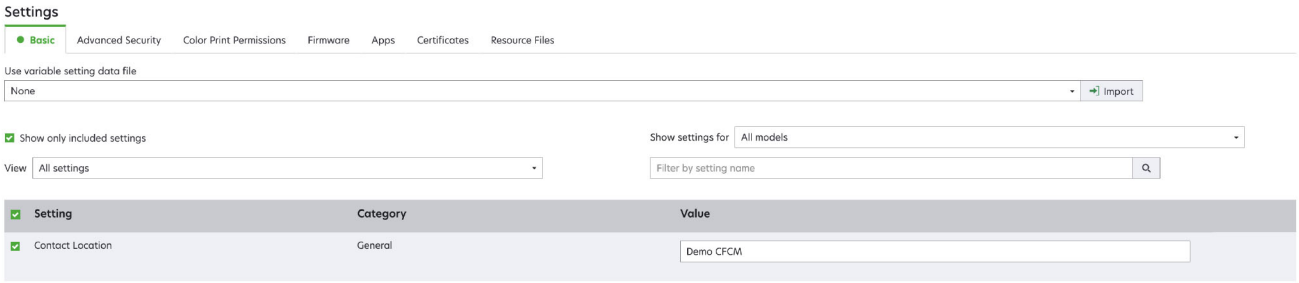
  Hinweis: Die Durchsetzung der Konfiguration und die Übereinstimmungsprüfung können so geplant werden, dass sie in regelmäßigen Abständen stattfinden.
- Wenn der Drucker die Konfigurationseinstellungen unterstützt, die Werte jedoch nicht zutreffen, wird der Drucker als nicht konform angezeigt.

Erstellen einer Konfiguration

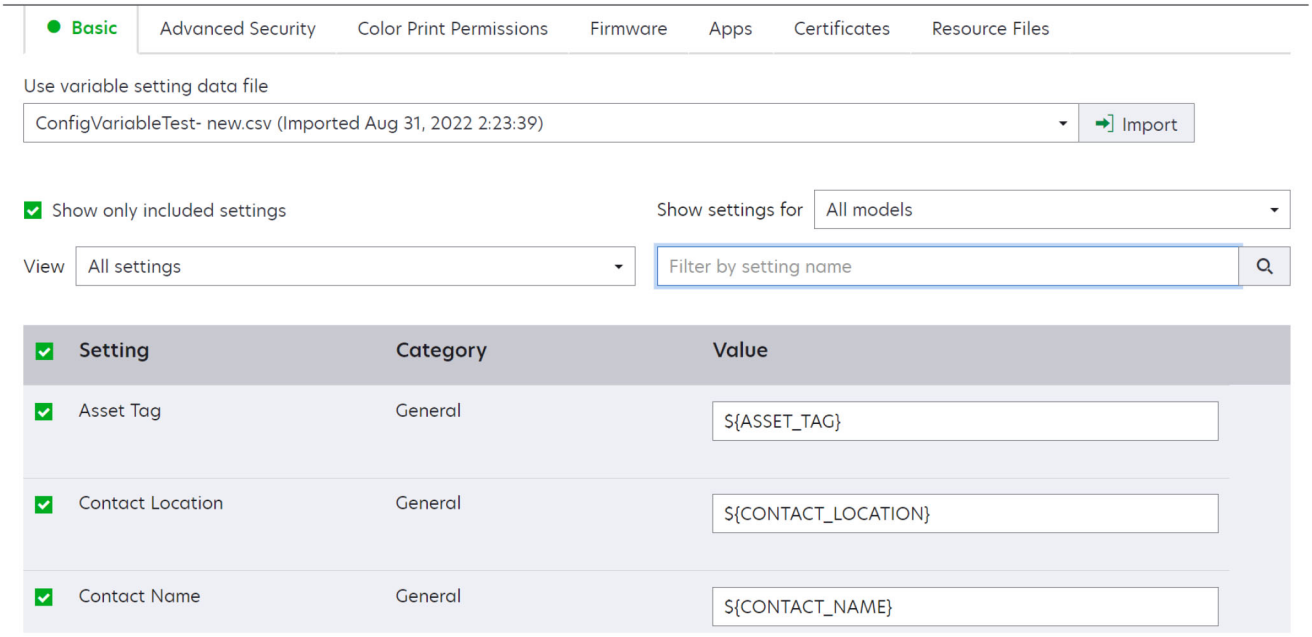
Eine Konfiguration ist eine Zusammenfassung von Einstellungen, die einem Drucker oder einer Gruppe von Druckern zugewiesen und durchgesetzt werden können. Innerhalb einer Konfiguration können Sie Printer Settings ändern und Anwendungen, Lizenzen, Firmware und CA-Zertifikate für Drucker bereitstellen.

1. Klicken Sie im Menü Konfigurationen auf **Alle Konfigurationen** > **Erstellen**.
2. Geben Sie einen eindeutigen Namen für die Konfiguration und ihre Beschreibung ein.
3. Führen Sie in der Einstellungsliste einen oder mehrere der folgenden Schritte aus:
   - Wählen Sie über die Registerkarte Grundeinstellungen eine oder mehrere Einstellungen aus und geben Sie anschließend die Werte an. Handelt es sich bei dem Wert um eine Variableneinstellung, müssen Sie die Kopfzeile mit **`${}`** einschließen. Beispiel: **`${Contact_Name}`**. Um eine Datei mit Variableneinstellungen zu verwenden, wählen Sie die Datei im Menü Variableneinstellungsdatei

verwenden aus, oder importieren Sie die Datei. Weitere Informationen finden Sie unter "Grundlagen zu Variableneinstellungen" auf Seite 73.



– Wählen Sie eine oder mehrere Einstellungen aus und legen Sie dann die Werte fest. Handelt es sich bei dem Wert um eine Variableneinstellung, müssen Sie die Kopfzeile mit **${}** einschließen. Beispiel: **${Contact_Name}**. Um eine Datei mit Variableneinstellungen zu verwenden, wählen Sie die Datei im Menü Variableneinstellungsdatei verwenden aus, oder importieren Sie die Datei. Weitere Informationen finden Sie unter "Grundlagen zu Variableneinstellungen" auf Seite 73.



– Wenn ein oder mehrere Zertifikate zu dieser Konfiguration hinzugefügt werden, können Sie eines der Zertifikate aus dem Dropdown**Wert** auswählen.

- Wählen Sie über die Registerkarte Erweiterte Sicherheit eine erweiterte Sicherheitskomponente aus.

  Hinweise:

  – Informationen zum Erstellen einer erweiterten Sicherheitskomponente finden Sie unter "Erstellen einer erweiterten Sicherheitskomponente von einem Drucker" auf Seite 73.
  – Sie können die erweiterten Sicherheitseinstellungen nur verwalten, wenn Sie eine Konfiguration über einen ausgewählten Drucker erstellen. Weitere Informationen finden Sie unter "Erstellen einer Konfiguration über einen Drucker" auf Seite 72.

- Konfigurieren Sie die Einstellungen über die Registerkarte Farbdruckberechtigungen. Weitere Informationen finden Sie unter "Farbdruckberechtigungen konfigurieren" auf Seite 74.

  Hinweis: Diese Einstellung ist nur in Konfigurationen für unterstützte Farbdrucker verfügbar.
- Wählen Sie auf der Registerkarte Firmware eine Firmware-Datei aus. Wenn mehrere Versionen derselben Firmware in einer Konfiguration vorhanden sind, wird bei der Konformitätsprüfung und Durchsetzung nur die höhere Firmware-Version berücksichtigt. Informationen zum Importieren einer Firmware-Datei finden Sie unter "Importieren von Dateien in die Ressourcenbibliothek" auf Seite 76.
- Wählen Sie auf der Registerkarte Apps mindestens eine bereitzustellende Anwendung aus. Weitere Informationen finden Sie unter "Erstellen eines Anwendungspakets" auf Seite 75.

  Hinweis: MVE unterstützt keine Bereitstellungsanwendungen mit Probe-Lizenzen. Sie können nur freie Anwendungen oder Anwendungen mit Produktionslizenzen bereitstellen.
- Wählen Sie auf der Registerkarte Zertifikate mindestens ein Zertifikat für die Bereitstellung aus. Informationen zum Importieren einer Zertifikatsdatei finden Sie unter "Importieren von Dateien in die Ressourcenbibliothek" auf Seite 76.

  Hinweis: Wählen Sie die Option **Markvision zur Verwaltung von Gerätezertifikaten verwenden** (für MVE) aus, um fehlende, ungültige, widerrufene und abgelaufene Zertifikate zu bewerten. Lassen Sie sie anschließend automatisch ersetzen.

  Wählen Sie eine der folgenden Optionen aus:
  - Standardgerätezertifikat
  - Benanntes Gerätezertifikat

    Hinweis: Standardmäßig kann ein Benutzer 10 benannte Zertifikate pro MVE-Installation und 5 benannte Zertifikate pro MVE-Konfiguration hinzufügen.

  Hinweis: Weitere Informationen finden Sie unter "Konfigurieren von MVE für die automatische Zertifikatsverwaltung" auf Seite 79.
- Wählen Sie auf der Registerkarte Ressourcendateien einen der folgenden Dateitypen für die Bereitstellung aus:
  - **Anwendungsdatei (.fls)**
  - **Konfigurationspaket (.zip)**
  - **Universelle Konfigurationsdatei (.ucf)**

  Hinweise:
  - Jede Option auf der Registerkarte "Ressource" ist nicht auf Konformität geprüft.
  - Es ist nicht ratsam, mehrere UCF- und Konfigurationspakete in einer einzigen Konfiguration zu verwenden.
  - Diese Methode ist nicht auf UCF-Dateien anwendbar, wenn "Scannen im Netzwerk" auf älteren Druckermodellen konfiguriert wird. UCF-Dateien müssen mit der Aktion **Datei für Drucker bereitstellen** bereitgestellt werden.

4 Klicken Sie auf **Konfiguration erstellen**.

Hinweis: Die folgende Liste zeigt die Deploymentsequenz in einer Konfiguration:

- **CA-Zertifikate**
- **Anwendungsdateien**
- **Lösungspaket**
- **Erweiterte Sicherheit**

- **Gerätezertifikate**
- **Grundlegende Einstellungen**
- **UCF- und Konfigurationspaket**
- **Firmware**

Erstellen einer Konfiguration über einen Drucker

Folgende Komponenten sind nicht enthalten:

- Drucker-Firmware
- Anwendungen
- Zertifikate

Zum Hinzufügen von Firmware, Anwendungen und Zertifikaten bearbeiten Sie die Konfiguration in MVE.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie den Drucker aus, und klicken Sie dann auf **Konfigurieren** > **Konfiguration über Drucker erstellen**.
3. Wählen Sie gegebenenfalls **Erweiterte Sicherheitseinstellungen inkludieren** aus, um eine erweiterte Sicherheitskomponente von dem ausgewählten Drucker zu erstellen.
4. Wenn der Drucker gesichert ist, wählen Sie die Authentifizierungsmethode aus, und geben Sie die Anmeldeinformationen ein.
5. Geben Sie einen eindeutigen Namen für die Konfiguration und ihre Beschreibung ein, und klicken Sie auf **Konfiguration erstellen**.
6. Klicken Sie im Menü Konfigurationen auf **Alle Konfigurationen**.
7. Wählen Sie die Konfiguration aus, und klicken Sie dann auf **Bearbeiten**.
8. Passen Sie gegebenenfalls die Einstellungen an.
9. Klicken Sie auf **Änderungen speichern**.

Beispielszenario: Duplizieren einer Konfiguration

Fünfzehn Lexmark MX812-Drucker wurden nach der Erkennung zum System hinzugefügt. Als IT-Mitarbeiter müssen Sie die Einstellungen der vorhandenen Drucker für die neu erkannten Drucker übernehmen.

Hinweis: Sie können auch eine Konfiguration von einem Drucker duplizieren und anschließend die Konfiguration auf einer Gruppe von Druckermodellen erzwingen.

Beispielimplementierung

1. Wählen Sie in der Liste der vorhandenen Drucker einen Lexmark Drucker MX812 aus.
2. Erstellen Sie eine Konfiguration über den Drucker.

   Hinweis: Um die Drucker zu sichern, fügen Sie die erweiterten Sicherheitseinstellungen ein.
3. Weisen Sie den neu ermittelten Druckern die Konfiguration zu, und setzen Sie sie durch.

Erstellen einer erweiterten Sicherheitskomponente von einem Drucker

Erstellen Sie zur Verwaltung der erweiterten Sicherheitseinstellungen eine erweiterte Sicherheitskomponente von einem Drucker. MVE liest alle Einstellungen dieses Druckers und erstellt dann eine Komponente, die die Einstellungen enthält. Die Komponente kann mehreren Konfigurationen für Druckermodelle zugeordnet werden, die über dasselbe Sicherheitssystem verfügen.

1. Klicken Sie im Menü Drucker auf **Druckerliste**.
2. Wählen Sie den Drucker aus, und klicken Sie dann auf **Konfigurieren** > **Erweiterte Sicherheitskomponente von Drucker erstellen**.
3. Geben Sie einen eindeutigen Namen für die Komponente und ihre Beschreibung ein.
4. Wenn der Drucker gesichert ist, wählen Sie die Authentifizierungsmethode aus, und geben Sie die Anmeldeinformationen ein.
5. Klicken Sie auf **Komponente erstellen**.

   Hinweis: Wenn Sie eine Konfiguration mit einer erweiterten Sicherheitskomponente erstellen und durchsetzen, die lokale Konten umfasst, werden die lokalen Konten den Druckern hinzugefügt. Alle vorhandenen lokalen Konten, die im Drucker vorkonfiguriert sind, werden beibehalten.

Erstellen einer druckbaren Version der Konfigurationseinstellungen

1. Bearbeiten Sie eine Konfiguration oder eine erweiterte Sicherheitskomponente.
2. Klicken Sie auf **Druckerfreundliche Version**.

Grundlagen zu dynamischen Einstellungen

- Zu diesen Einstellungen gehören das 802,1x-Gerätezertifikat, das HTTPS-Gerätezertifikat und das IPSec-Gerätezertifikat, die auf der Registerkarte Grundeinstellung einer Konfiguration aufgeführt sind.
- Die Optionen für jede dieser Einstellungen werden mit den Zertifikaten ausgefüllt, die auf der Registerkarte Zertifikat ausgewählt wurden.
- Wenn Sie eine Konfiguration klonen, exportieren oder importieren, werden die vorausgewählten Werte dieser Einstellungen gelöscht. Sie müssen die Werte manuell auswählen.

Grundlagen zu Variableneinstellungen

Variableneinstellungen ermöglichen Ihnen das flottenübergreifende Verwalten von Einstellungen, die für jeden Drucker eindeutig sind, beispielsweise Hostname oder Bestandsetikett. Beim Erstellen oder Bearbeiten einer Konfiguration können Sie eine CSV-Datei auswählen, die mit der Konfiguration verknüpft werden soll.

CSV-Beispielformat:

```
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
```

Die erste Spalte in der Kopfzeile der Variablen-Datei ist ein eindeutiges Drucker-Identifizierungstoken. Bei dem Token muss es sich um eines der Folgenden handeln:

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

Jede nachfolgende Spalte in der Kopfzeile der Variablen-Datei ist ein benutzerdefiniertes "Ersatz"-Token. Auf dieses Token muss innerhalb der Konfiguration mithilfe des ${Header}-Formats verwiesen werden. Es wird beim Durchsetzen der Konfiguration durch die Werte in den nachfolgenden Zeilen ersetzt. Stellen Sie sicher, dass die Token keine Leerzeichen enthalten.

Sie können die CSV-Datei, in der die Variableneinstellungen enthalten sind, beim Erstellen oder Bearbeiten einer Konfiguration importieren. Weitere Informationen finden Sie unter "Erstellen einer Konfiguration" auf Seite 69.

Farbdruckberechtigungen konfigurieren

Mit MVE können Sie den Farbdruck für Host-Computer und bestimmte Benutzer einschränken.

Hinweis: Diese Einstellung ist nur in Konfigurationen für unterstützte Farbdrucker verfügbar.

1. Klicken Sie im Menü "Konfigurationen" auf **Alle Konfigurationen**.
2. Erstellen oder bearbeiten Sie eine Konfiguration.
3. Führen Sie in der Registerkarte "Farbdruckberechtigungen" einen der folgenden Schritte aus:

Farbdruckberechtigungen für Host-Computer konfigurieren

a. Wählen Sie im Menü "Anzeigen" zunächst die Option **Host-Computer** und dann **Farbdruckberechtigungen für Host-Computer einschließen** aus.
b. Klicken Sie auf **Hinzufügen**, und geben Sie dann den Namen des Host-Computers ein.
c. Damit der Host-Computer in Farbe druckt, wählen Sie die Option **Farbdruck zulassen**.
d. Um Benutzern, die sich am Host-Computer anmelden, den Farbdruck zu erlauben, wählen Sie die Option **Benutzerberechtigung überschreiben**.
e. Klicken Sie auf **Speichern und Hinzufügen** oder auf **Speichern**.

Farbdruckberechtigungen für Benutzer konfigurieren

a. Wählen Sie im Menü "Anzeigen" zunächst die Option **Benutzer** und dann **Farbdruckberechtigungen für Benutzer einschließen** aus.
b. Klicken Sie auf **Hinzufügen**, und geben Sie dann den Benutzernamen ein.
c. Wählen Sie **Farbdruck zulassen**.
d. Klicken Sie auf **Speichern und Hinzufügen** oder auf **Speichern**.

Erstellen eines Anwendungspakets

1. Exportieren Sie die Ansicht der Druckerliste über MVE mithilfe der Funktion "Daten exportieren".
   a. Klicken Sie im Menü Drucker auf **Ansichten**.
   b. Wählen Sie **Druckerliste**, und klicken Sie dann auf **Daten exportieren**.
   c. Wählen Sie einen gespeicherten Suchvorgang aus.
   d. Wählen Sie im Menü "Dateityp für Datenexport auswählen" die Option **CSV**.
   e. Klicken Sie auf **Daten exportieren**.
2. Öffnen Sie den Paket-Builder.

   Hinweis: Wenn Sie noch keinen Zugriff auf den Paket-Builder haben, wenden Sie sich an einen Vertriebsmitarbeiter von Lexmark.

   a. Melden Sie sich an bei Paket-Builder unter **cdp.lexmark.com/package-builder**.
   b. Importieren Sie die Druckerliste, und klicken Sie dann auf **Weiter**.
   c. Geben Sie die Paketbeschreibung und dann Ihre E-Mail-Adresse.
   d. Wählen Sie im Menü Produkt eine Anwendung aus, und fügen Sie ggf. Lizenzen hinzu.
   e. Klicken Sie auf **Weiter** > **Fertig stellen**. Der Link zum Herunterladen des Pakets wird an Ihre E-Mail-Adresse gesendet.
3. Laden Sie das Paket herunter.

Hinweise:

- MVE unterstützt keine Bereitstellungsanwendungen mit Probe-Lizenzen. Sie können nur freie Anwendungen oder Anwendungen mit Produktionslizenzen bereitstellen. Wenden Sie sich an einen Vertriebsmitarbeiter von Lexmark, wenn Sie Anwendungscodes benötigen.
- Importieren Sie das Anwendungspaket in die Ressourcenbibliothek, um die Anwendungen zu einer Konfiguration hinzuzufügen. Weitere Informationen finden Sie unter "Importieren von Dateien in die Ressourcenbibliothek" auf Seite 76.

Importieren oder Exportieren einer Konfiguration

Stellen Sie zunächst beim Importieren einer Konfigurationsdatei sicher, dass sie aus einem MVE der gleichen Version exportiert wurde.

1. Klicken Sie im Menü Konfigurationen auf **Alle Konfigurationen**.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Konfigurationsdatei zu importieren, klicken Sie auf **Importieren**, suchen Sie nach der Konfigurationsdatei, und klicken Sie dann auf **Importieren**.
   - Um eine Konfigurationsdatei zu exportieren, wählen Sie eine Konfiguration aus, und klicken Sie dann auf **Exportieren**.

   Hinweise:

   – Beim Exportieren einer Konfiguration sind die Kennwörter ausgeschlossen. Nach dem Importieren müssen die Kennwörter manuell hinzugefügt werden.
   – UCF, Konfigurationspakete und Anwendungsdateien sind nicht Teil einer exportierten Konfiguration.

Importieren von Dateien in die Ressourcenbibliothek

Die Ressourcenbibliothek ist eine Zusammenstellung von Firmware-Dateien, CA-Zertifikaten und Anwendungspaketen, die in MVE importiert werden. Diese Dateien können einer oder mehreren Konfiguration(en) zugeordnet werden.

1. Klicken Sie im Menü Konfigurationen auf **Ressourcenbibliothek**.
2. Klicken Sie auf **Importieren** > **Datei auswählen**, und navigieren Sie anschließend zur Datei.

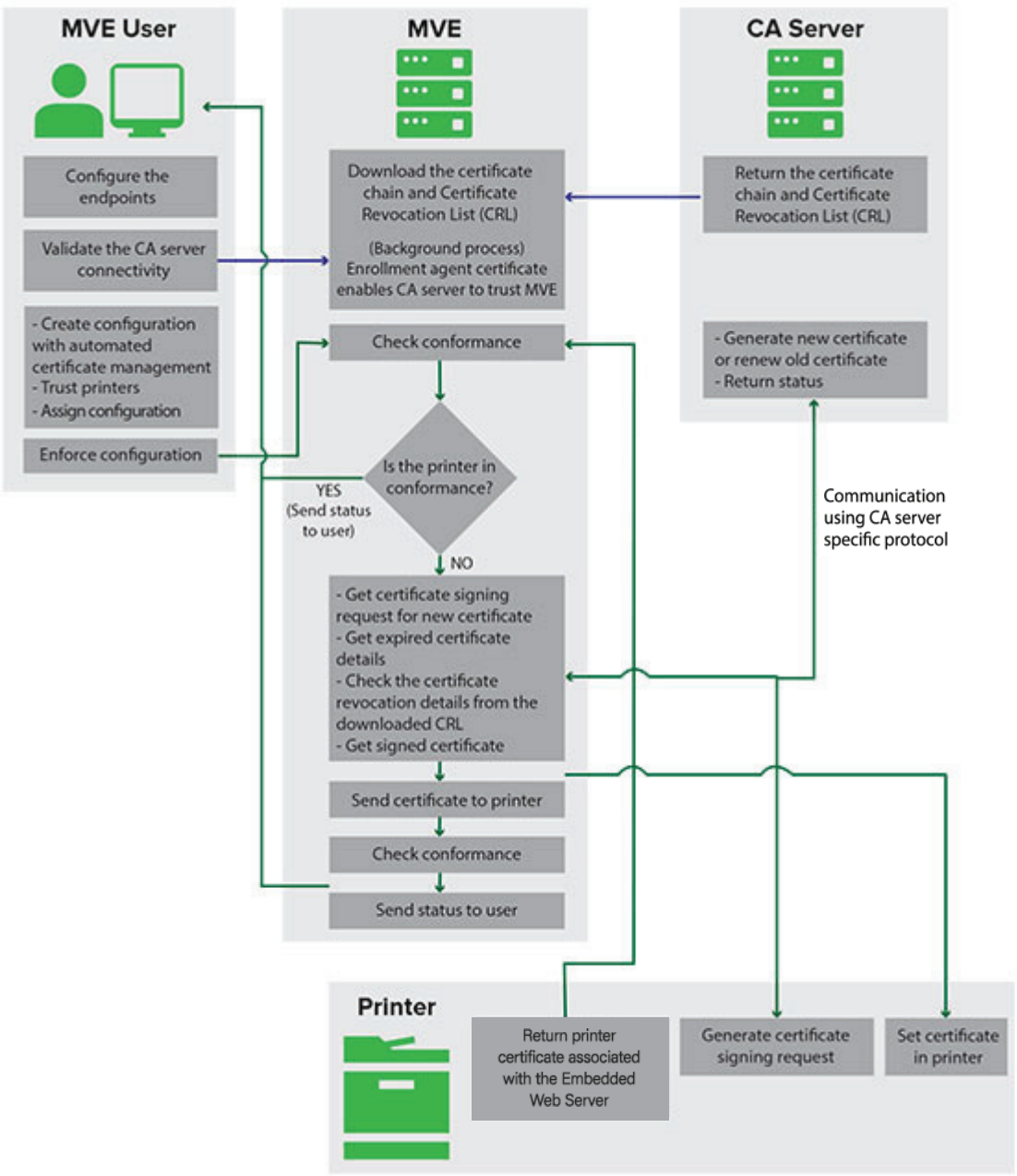
   Hinweis: Nur Firmware-/Anwendungsdateien (.fls), Anwendungs- oder Konfigurationspakete (.zip), CA-Zertifikate (.pem) und universelle Konfigurationsdateien (.ucf) können importiert werden.
3. Klicken Sie auf **Ressource importieren**.

Verwalten von Zertifikaten

Einrichten von MVE zur automatischen Verwaltung von Zertifikaten

Bedeutung der Funktion zur automatisierten Zertifikatsverwaltung

Sie können MVE so konfigurieren, dass Druckerzertifikate automatisch verwaltet werden, und Sie können diese anschließend über die Konfigurationsdurchsetzung auf den Druckern installieren. Das folgende Diagramm beschreibt den End-to-End-Prozess der automatischen Zertifikatsverwaltung.



Die Endpunkte der Zertifizierungsstelle, zum Beispiel der CA-Server und die Serveradresse, müssen in MVE definiert werden.

Die folgenden CA-Server werden unterstützt:

- **OpenXPKI CA**: Benutzer können eines der folgenden Protokolle verwenden:
  - Sicheres Zertifikatverschlüsselungsprotokoll (Secure Certificate Encryption Protocol, SCEP)
  - EST-Anschluss

  Hinweise:

  - EST ist die empfohlene Methode, um eine Verbindung zum OpenXPKI-Server herzustellen.
  - Weitere Informationen zum Konfigurieren von OpenXPKI CA mit dem EST-Protokoll finden Sie unter "Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über EST" auf Seite 119.
  - Weitere Informationen zum Konfigurieren von OpenXPKI CA mit dem SCEP-Protokoll finden Sie unter "Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über SCEP" auf Seite 101.
- **Microsoft CA Enterprise**: Benutzer können eines der folgenden Protokolle verwenden
  - Sicheres Zertifikatverschlüsselungsprotokoll (Secure Certificate Encryption Protocol, SCEP)
  - Microsoft Certificate Enrollment Web Services (MSCEWS)

  Hinweise:

  - MSCEWS ist die empfohlene Methode, um eine Verbindung zum Microsoft CA Enterprise-Server herzustellen.
  - Weitere Informationen zum Konfigurieren von Microsoft CA mit dem MSCEWS-Protokoll finden Sie unter "Verwalten von Zertifikaten mit Microsoft Certificate Authority über MSCEWS" auf Seite 90.
  - Weitere Informationen zum Konfigurieren von Microsoft CA mit dem SCEP-Protokoll finden Sie unter "Verwalten von Zertifikaten mit Microsoft Certificate Authority über SCEP" auf Seite 82.

Die Verbindung zwischen MVE und den CA-Servern muss validiert werden. Während der Validierung kommuniziert MVE mit dem CA-Server, um die Zertifikatskette und die Zertifikatsperrliste (Certificate Revocation List, CRL) herunterzuladen. Das Zertifikat des Anmeldeagenten oder Testzertifikat wird ebenfalls generiert. Mit diesem Zertifikat kann der CA-Server MVE vertrauen.

Weitere Informationen zur Definition der Endpunkte und zur Validierung finden Sie unter "Konfigurieren von MVE für die automatische Zertifikatsverwaltung" auf Seite 79.

Eine Konfiguration, die für die **Verwendung von Markvision zur Verwaltung von Gerätezertifikaten** eingerichtet ist, muss dem Drucker zugewiesen und durchgesetzt werden.

Weitere Informationen finden Sie in den folgenden Themenabschnitten:

- "Erstellen einer Konfiguration" auf Seite 69
- "Durchsetzen von Konfigurationen" auf Seite 63

Während der Durchsetzung überprüft MVE den Drucker auf Konformität.

Für **Standardgerätezertifikat**

- Das Zertifikat wird anhand der Zertifikatskette validiert, die vom CA-Server heruntergeladen wurde.
- Wenn der Drucker nicht konform ist, wird eine Zertifikatssignierungsanforderung (CSR) für den Drucker angefordert.

Für **Benanntes Gerätezertifikat**

- Das Zertifikat wird anhand der Zertifikatskette validiert, die vom CA-Server heruntergeladen wurde.
- MVE erstellt ein selbstsigniertes, benanntes Gerätezertifikat auf dem Gerät.

- Wenn der Drucker nicht konform ist, wird eine CSR für den Drucker angefordert.

Hinweise:

- MVE kommuniziert mit dem CA-Server unter Verwendung eines konfigurierten Protokolls.
- Der CA-Server generiert das neue Zertifikat und sendet das Zertifikat anschließend an den Drucker.
- Wenn ein benanntes Zertifikat im Drucker vorhanden ist, wird kein neues benanntes Zertifikat erstellt, aber für den Drucker wird eine CSR erstellt.

Konfigurieren von MVE für die automatische Zertifikatsverwaltung

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **Zertifizierungsstelle** > **Zertifizierungsstellen-Server verwenden**.

   Hinweis: Die Schaltfläche Zertifizierungsstellen-Server verwenden wird nur angezeigt, wenn die Zertifizierungsstelle zum ersten Mal konfiguriert oder wenn das Zertifikat gelöscht wird.
3. Konfigurieren Sie die Serverendpunkte.
   - **CA-Server**: Der CA-Server (Certificate Authority), der die Druckerzertifikate generiert. Sie können eine der folgenden Optionen auswählen:
     - **OpenXPKI CA**
     - **Microsoft CA- Enterprise**

     Hinweis: Der Benutzer kann auch einen CA-Server konfigurieren, der das **Enrollment over Secure Transport (EST)**-Protokoll unterstützt.

     - Der CA-Server muss das in RFC 7030 definierte EST-Protokoll implementieren.

       Hinweis: Jede Abweichung von der Spezifikation kann zu einer ungültigen Installation führen.
     - EST ist das empfohlene Protokoll für die Verbindung mit dem OpenXPKI CA-Server.

       Hinweis: Der Microsoft CA Enterprise-Server unterstützt das EST-Protokoll nicht.
   - **CA-Serveradresse**: Geben Sie die IP-Adresse oder den Hostnamen Ihres CA-Servers ein. Dieses Feld gilt nur für SCEP- und EST-Protokolle.

     Hinweis: Geben Sie eine der folgenden Optionen ein:

     - Für MSCA-Server (mit SCEP): <Server-IP-Adresse oder Hostname>/certsrv/mscep/mscep.dll
     - Für OpenXPKI-Server (mit SCEP): <Server-IP-Adresse oder Hostname>/scep/scep
     - Geben Sie für EST eine der folgenden Optionen ein:
       - https://172.87.95.240
       - https://estserver.com
       - estserver.com
   - **CA-Server-Kennzeichnung (Optional)** – Wenn der Benutzer einen neuen Bereich erstellt, muss derselbe Bereichsname in dieses Feld eingefügt werden.
   - **CEP-Serveradresse** – Dieses Feld gilt nur für das MSCEWS-Protokoll.

     Hinweis: Geben Sie eine der folgenden Optionen ein:

  - Für die Authentifizierung mit Benutzername und Kennwort: https://democep.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP
  - Für die integrierte Windows-Authentifizierung: https://democep.com/ADPolicyProvider_CEP_Kerberos/service.svc/CEP
  - Für die Clientzertifikat-Authentifizierung: https://democep.com/ADPolicyProvider_CEP_Certificate/service.svc/CEP
- **CA-Server-Hostname** – Geben Sie die IP-Adresse oder den Hostnamen Ihres CA-Servers ein.

  Hinweis: Für das MSCEWS-Protokoll kann der Benutzer beispielsweise **`democa.lexmark.com`** auswählen.
- **CES-Server-Hostname** – Geben Sie die IP-Adresse oder den Hostnamen Ihres CES-Servers ein.

  Hinweis: Für das MSCEWS-Protokoll kann der Benutzer beispielsweise **`democes.lexmark.com`** auswählen.
- **Abfrage-Kennwort**: Das Abfrage-Kennwort, das erforderlich ist, um die Identität von MVE beim CA-Server zu bestätigen. Dieses Kennwort ist nur für OpenXPKI CA erforderlich. Es wird in Microsoft CA Enterprise nicht unterstützt.

Hinweis: Je nach CA-Server müssen Sie den Authentifizierungsmodus des Servers konfigurieren. Führen Sie einen der folgenden Schritte aus:

- Wenn Sie das **EST**-Protokoll auswählen, wählen Sie im Menü **Authentifizierungsmodus des CA-Servers** eine der folgenden Optionen aus:
  - **Authentifizierung mit Benutzername und Kennwort**
  - **Clientzertifikat-Authentifizierung**
- Wenn Sie das **MSCEWS**-Protokoll auswählen, wählen Sie im Menü **Authentifizierungsmodus des CA-Servers** eine der folgenden Optionen aus:
  - **Authentifizierung mit Benutzername und Kennwort**
  - **Clientzertifikat-Authentifizierung**
  - **Integrierte Windows-Authentifizierung**
- **Das SCEP**-Protokoll unterstützt nur den Authentifizierungsmodus **Kennwortabfrage**.

Hinweis: Je nach CA-Server finden Sie in den folgenden Abschnitten weitere Informationen:

- "Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über SCEP" auf Seite 101
- "Verwalten von Zertifikaten mit Microsoft Certificate Authority über SCEP" auf Seite 82
- "Verwalten von Zertifikaten mit Microsoft Certificate Authority über MSCEWS" auf Seite 90
- "Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über EST" auf Seite 119

4 Klicken Sie auf **Änderungen speichern und validieren** > **OK**.

Hinweise:

- Die Option **Änderungen verwerfen** funktioniert nur, wenn die Änderungen noch nicht gespeichert oder gespeichert und validiert wurden.
- Der Benutzer kann Daten nicht aus einer ungültigen Konfiguration heraus wiederherstellen, da MVE den letzten gültigen Status von Konfigurationen nicht speichert. MVE speichert jeweils nur eine einzelne Zertifikatskonfiguration, die gültig sein kann oder nicht.

Hinweise:

- Die Verbindung zwischen MVE und den CA-Servern muss validiert werden. Während der Validierung kommuniziert MVE mit dem CA-Server, um die Zertifikatskette und die Zertifikatsperrliste (Certificate Revocation List, CRL) herunterzuladen. Das Zertifikat des Anmeldeagenten oder Testzertifikat wird ebenfalls generiert. Mit diesem Zertifikat kann der CA-Server MVE vertrauen.
- Sie können eine oder mehrere CEP-Vorlagen auswählen, wenn Sie das MSCEWS-Protokoll verwenden. Gehen Sie folgendermaßen vor:

a Nachdem Sie auf **Änderungen speichern und validieren** geklickt haben, wird das Fenster zur CEP-Vorlagenauswahl angezeigt.

b Wählen Sie eine oder mehrere Vorlagen aus den verfügbaren Vorlagen aus.

- Das Dialogfeld „Zertifizierungsstellen-Server verwenden“ ruft die Zertifikatsrückrufliste ab.
- Ein Dialogfeld bestätigt, dass die Zertifikatsüberprüfung erfolgreich war.

c Sie können die ausgewählten CEP-Vorlagen auf der Konfigurationsseite des CA-Servers anzeigen.

Hinweis: Wenn Sie diese Konfiguration für ein beliebiges Gerät erzwingen, wird ein Zertifikat entsprechend der ausgewählten Vorlage erstellt.

5 Navigieren Sie zurück zur Seite Systemkonfiguration, und überprüfen Sie anschließend das CA-Zertifikat.

Hinweis: Sie können ein CA-Zertifikat auch herunterladen oder löschen.

Konfigurieren von Microsoft Enterprise CA mit NDES

Übersicht

Im folgenden Bereitstellungsszenario basieren alle Berechtigungen auf Berechtigungen, die auf Zertifikatsvorlagen festgelegt sind, die im Domänen-Controller veröffentlicht werden. Die an die Zertifizierungsstelle gesendeten Zertifikatsanforderungen basieren auf Zertifikatsvorlagen.

Stellen Sie bei dieser Einrichtung sicher, dass Sie über Folgendes verfügen:

- Gerät, das die untergeordnete CA hostet
- Gerät, auf dem der NDES-Service gehostet wird
- Domänen-Controller

Erforderliche Benutzer

Erstellen Sie die folgenden Benutzer im Domänen-Controller:

- Service-Administrator
  - Benannt als **SCEPAdmin**
  - Muss Mitglied der Gruppen **lokaler Admin** - und **Enterprise-Admin** sein
  - Muss lokal protokolliert werden, wenn die Installation der NDES-Rolle ausgelöst wird
  - Verfügt über **Registrierungsberechtigung** für die Zertifikatvorlagen
  - Verfügt über **Berechtigung zum Hinzufügen von Vorlagen** für CA
- Dienstkonto
  - Benannt als **SCEPSvc**
  - Muss Mitglied der lokalen Gruppe **IIS_IUSRS** sein

  - Muss ein Domänenbenutzer sein und über **Lese-** und **Registrierungsberechtigungen** für die konfigurierten Vorlagen verfügen
  - Verfügt über **Anforderungsberechtigung** für CA
- CA-Administrator des Unternehmens
  - Benannt als **CAAdmin**
  - Mitglied der **Admin**-Gruppe des Unternehmens
  - Muss Teil der **lokalen Admin**-Gruppe sein

Verwalten von Zertifikaten mit Microsoft Certificate Authority über SCEP

Dieser Abschnitt enthält Anweisungen zu folgenden Themen:

- Konfigurieren der Microsoft Enterprise Certificate Authority (CA) unter Verwendung des Microsoft Network Device Enrollment Service (NDES)
- Erstellen eines Root-CA-Servers

Hinweis: Das Betriebssystem Windows Server 2016 wird für alle Einstellungen in diesem Dokument verwendet.

Übersicht

Der Root-CA-Server ist der Haupt-CA-Server in einer Organisation und die Spitze der PKI-Infrastruktur. Die Root-CA authentifiziert den untergeordneten CA-Server. Dieser Server wird im Allgemeinen im Offlinemodus gehalten, um ein Eindringen zu verhindern und den privaten Schlüssel zu sichern.

Zur Konfiguration des CA-Servers gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass der CA-Server installiert ist. Weitere Informationen finden Sie unter "Installieren des Root-CA-Servers" auf Seite 82.
2. Konfigurieren Sie die Einstellungen für den Zertifizierungsverteilungspunkt und den Zugriff auf die Zertifizierungsstelleninformationen. Weitere Informationen finden Sie unter "Konfigurieren der Einstellungen für den Zertifizierungsverteilungspunkt und den Zugriff auf die Zertifizierungsstelleninformationen" auf Seite 85.
3. Konfigurieren Sie die CRL-Zugänglichkeit. Weitere Informationen finden Sie unter "Konfigurieren der CRL-Zugänglichkeit" auf Seite 86.

Installieren des Root-CA-Servers

1. Klicken Sie im Server-Manager auf **Verwalten** > **Rollen und Funktion hinzufügen**.
2. Klicken Sie auf **Server-Rollen**, wählen Sie **Active Directory-Zertifikatdienste** und alle Funktionen aus, und klicken Sie anschließend auf **Weiter**.
3. Wählen Sie im Abschnitt AD CS-Rollendienste die Option **Zertifizierungsstelle** aus, und klicken Sie anschließend auf **Weiter** > **Installieren**.
4. Klicken Sie nach der Installation auf **Active Directory-Zertifikatdienste auf dem Zielserver konfigurieren**.
5. Wählen Sie im Abschnitt Rollendienste die Option **Zertifizierungsstelle** > **Weiter** aus.

6. Wählen Sie im Abschnitt Einrichtungstyp die Option **Eigenständige Zertifizierungsstelle** aus, und klicken Sie anschließend auf **Weiter**.
7. Wählen Sie im Abschnitt CA-Typ die Option **Root-CA** aus, und klicken Sie anschließend auf **Weiter**.
8. Wählen Sie **Neuen privaten Schlüssel erstellen** aus, und klicken Sie anschließend auf **Weiter**.
9. Wählen Sie im Menü Kryptografieanbieter auswählen die Option **RSA#Microsoft Software Key Storage Provider** aus.
10. Wählen Sie im Menü Schlüssellänge die Option **4096** aus.
11. Wählen Sie aus der Liste mit den Hash-Algorithmen **SHA512** aus, und klicken Sie anschließend auf **Weiter**.
12. Geben Sie in das Feld Gemeinsamer Name für diese CA den Namen des Hosting-Servers ein.
13. Geben Sie in das Feld Suffix des definierten Namens die Domänenkomponente ein.

    Beispiel für Konfiguration des CA-Namens

    Vollqualifizierter Domänenname (FQDN) des Geräts: **`test.dev.lexmark.com`**

    Gemeinsamer Name (CN): **`TEST`**

    Suffix des DN (Distinguished Name): **`DC=DEV,DC=LEXMARK,DC=COM`**
14. Klicken Sie auf **Weiter**.
15. Geben Sie den Gültigkeitszeitraum an, und klicken Sie anschließend auf **Weiter**.

    Hinweis: Im Allgemeinen beträgt der Gültigkeitszeitraum 10 Jahre.
16. Ändern Sie nichts im Fenster "Datenbankspeicherorte".
17. Schließen Sie die Installation ab.

Konfigurieren von Microsoft Enterprise CA mit NDES

Übersicht

Im folgenden Bereitstellungsszenario basieren alle Berechtigungen auf Berechtigungen, die auf Zertifikatsvorlagen festgelegt sind, die im Domänen-Controller veröffentlicht werden. Die an die Zertifizierungsstelle gesendeten Zertifikatsanforderungen basieren auf Zertifikatsvorlagen.

Stellen Sie bei dieser Einrichtung sicher, dass Sie über Folgendes verfügen:

- Gerät, das die untergeordnete CA hostet
- Gerät, auf dem der NDES-Service gehostet wird
- Domänen-Controller

Erforderliche Benutzer

Erstellen Sie die folgenden Benutzer im Domänen-Controller:

- Service-Administrator
  - Benannt als **SCEPAdmin**
  - Muss Mitglied der Gruppen **lokaler Admin** - und **Enterprise-Admin** sein
  - Muss lokal protokolliert werden, wenn die Installation der NDES-Rolle ausgelöst wird

  - Verfügt über **Registrierungsberechtigung** für die Zertifikatvorlagen
  - Verfügt über **Berechtigung zum Hinzufügen von Vorlagen** für CA
- Dienstkonto
  - Benannt als **SCEPSvc**
  - Muss Mitglied der lokalen Gruppe **IIS_IUSRS** sein
  - Muss ein Domänenbenutzer sein und über **Lese-** und **Registrierungsberechtigungen** für die konfigurierten Vorlagen verfügen
  - Verfügt über **Anforderungsberechtigung** für CA

Konfigurieren eines untergeordneten CA-Servers

Übersicht

Der untergeordnete CA-Server ist der Zwischen-CA-Server und immer online. In der Regel führt er die Verwaltung von Zertifikaten durch.

Zur Konfiguration des untergeordneten CA-Servers gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, dass der untergeordnete CA-Server installiert ist. Weitere Informationen finden Sie unter "Installieren des untergeordneten CA-Servers" auf Seite 84.
2. Konfigurieren Sie die Einstellungen für den Zertifizierungsverteilungspunkt und den Zugriff auf die Zertifizierungsstelleninformationen. Weitere Informationen finden Sie unter "Konfigurieren der Einstellungen für den Zertifizierungsverteilungspunkt und den Zugriff auf die Zertifizierungsstelleninformationen" auf Seite 85.
3. Konfigurieren Sie die CRL-Zugänglichkeit. Weitere Informationen finden Sie unter "Konfigurieren der CRL-Zugänglichkeit" auf Seite 86.

Installieren des untergeordneten CA-Servers

1. Melden Sie sich auf dem Server als Domänenbenutzer **CAAdmin** an.
2. Klicken Sie im Server-Manager auf **Verwalten** > **Rollen und Funktion hinzufügen**.
3. Klicken Sie auf **Server-Rollen**, wählen Sie **Active Directory-Zertifikatdienste** und alle Funktionen aus, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie im Abschnitt AD CS-Rollendienste die Optionen **Zertifizierungsstelle** und **Webregistrierung der Zertifizierungsstelle** aus, und klicken Sie anschließend auf **Weiter**.

   Hinweis: Stellen Sie sicher, dass alle Funktionen der Webregistrierung der Zertifizierungsstelle hinzugefügt werden.
5. Behalten Sie im Abschnitt Web-Server-Rolle (ISS) Rollendienste die Standardeinstellungen bei.
6. Klicken Sie nach der Installation auf **Active Directory-Zertifikatdienste auf dem Zielserver konfigurieren**.
7. Wählen Sie im Abschnitt Rollendienste die Optionen **Zertifizierungsstelle** und **Webregistrierung der Zertifizierungsstelle** aus, und klicken Sie anschließend auf **Weiter**.
8. Wählen Sie im Abschnitt Einrichtungstyp die Option **Unternehmens-CA** aus, und klicken Sie anschließend auf **Weiter**.

9. Wählen Sie im Abschnitt CA-Typ die Option **Untergeordnete CA** aus, und klicken Sie anschließend auf **Weiter**.
10. Wählen Sie **Neuen privaten Schlüssel erstellen** aus, und klicken Sie anschließend auf **Weiter**.
11. Wählen Sie im Menü Kryptografieanbieter auswählen die Option **RSA#Microsoft Software Key Storage Provider** aus.
12. Wählen Sie im Menü Schlüssellänge die Option **4096** aus.
13. Wählen Sie aus der Liste mit den Hash-Algorithmen **SHA512** aus, und klicken Sie anschließend auf **Weiter**.
14. Geben Sie in das Feld Gemeinsamer Name für diese CA den Namen des Hosting-Servers ein.
15. Geben Sie in das Feld Suffix des definierten Namens die Domänenkomponente ein.

    Beispiel für Konfiguration des CA-Namens

    Vollqualifizierter Domänenname (FQDN) des Geräts: **`test.dev.lexmark.com`**

    Gemeinsamer Name (CN): **`TEST`**

    Suffix des DN (Distinguished Name): **`DC=DEV,DC=LEXMARK,DC=COM`**
16. Speichern Sie die Anforderungsdatei im Dialogfeld Zertifikatsanforderung, und klicken Sie anschließend auf **Weiter**.
17. Ändern Sie nichts im Fenster "Datenbankspeicherorte".
18. Schließen Sie die Installation ab.
19. Signieren Sie die CA-Anforderung der Root-CA, und exportieren Sie das signierte Zertifikat anschließend im PKCS7-Format.
20. Öffnen Sie die **Zertifizierungsstelle** über die untergeordnete CA.
21. Klicken Sie im linken Bereich mit der rechten Maustaste auf die Zertifizierungsstelle, und klicken Sie anschließend auf **Alle Aufgaben > CA-Zertifikat installieren**.
22. Wählen Sie das signierte Zertifikat aus, und starten Sie anschließend den CA-Dienst.

Konfigurieren der Einstellungen für den Zertifizierungsverteilungspunkt und den Zugriff auf die Zertifizierungsstelleninformationen

Hinweis: Konfigurieren Sie die Zugriffseinstellungen für den Zertifizierungsverteilungspunkt (CDP) und den Zugriff auf die Zertifizierungsstelleninformationen (AIA) für die Zertifikatsrückrufliste (CRL).

1. Klicken Sie im Server-Manager auf **Extras > Zertifizierungsstelle**.
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf die Zertifizierungsstelle, und klicken Sie anschließend auf **Eigenschaften > Erweiterungen**.
3. Wählen Sie im Menü Erweiterung auswählen die Option **CRL Distribution Point (CDP)** aus.
4. Wählen Sie in der Zertifikatsrückrufliste den Eintrag **C:\Windows\system32** aus, und gehen Sie anschließend wie folgt vor:
   a. Aktivieren Sie **CRLs an diesem Speicherort veröffentlichen**.
   b. Deaktivieren Sie **Delta-CRLs an diesem Speicherort veröffentlichen**.
5. Löschen Sie alle anderen Einträge außer **C:\Windows\system32**.

6. Klicken Sie auf **Hinzufügen**.
7. Fügen Sie im Feld Speicherort die Option **http://*serverIP*/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl** hinzu, wobei ***serverIP*** die IP-Adresse des Servers ist.

   Hinweis: Wenn Ihr Server unter Verwendung des FQDN erreichbar ist, verwenden Sie den **<ServerDNSName>** anstelle seiner IP-Adresse.
8. Klicken Sie auf **OK**.
9. Wählen Sie **In die CDP-Erweiterung der ausgegebenen Zertifikate aufnehmen** für den erstellten Eintrag.
10. Wählen Sie im Menü Erweiterung auswählen die Option **Zugriff auf Zertifizierungsstelleninformationen (AIA)** aus.
11. Löschen Sie alle anderen Einträge außer **C:\Windows\system32**.
12. Klicken Sie auf **Hinzufügen**.
13. Fügen Sie im Feld Speicherort die Option **http://*serverIP*/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt**, wobei ***serverIP*** die IP-Adresse des Servers ist.

    Hinweis: Wenn Ihr Server unter Verwendung des FQDN erreichbar ist, verwenden Sie den **<ServerDNSName>** anstelle seiner IP-Adresse.
14. Klicken Sie auf **OK**.
15. Wählen Sie **In die AIA-Erweiterung der ausgegebenen Zertifikate aufnehmen** für den erstellten Eintrag.
16. Klicken Sie auf **Anwenden** > **OK**.

    Hinweis: Starten Sie den Zertifizierungsdienst ggf. neu.
17. Erweitern Sie im linken Bereich die Zertifizierungsstelle, klicken Sie mit der rechten Maustaste auf **Widerrufene Zertifikate**, und klicken Sie anschließend auf **Eigenschaften**.
18. Geben Sie den Wert für CRL-Veröffentlichungsintervall und für Veröffentlichungsintervall für Delta CRLs an, und klicken Sie anschließend auf **Anwenden** > **OK**.
19. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Widerrufene Zertifikate**, klicken Sie auf **Alle Aufgaben**, und veröffentlichen Sie anschließend die CRL, die Neu ist.

Konfigurieren der CRL-Zugänglichkeit

Hinweis: Stellen Sie zu Beginn sicher, dass der Internet Information Services (IIS) Manager installiert ist.

1. Erweitern Sie im IIS-Manager die Zertifizierungsstelle, und erweitern Sie anschließend **Websites**.
2. Klicken Sie mit der rechten Maustaste auf **Standard-Website**, und klicken Sie anschließend auf **Virtuelles Verzeichnis hinzufügen**.
3. Geben Sie im Feld Alias **CertEnroll** ein.
4. Geben Sie im Feld Physischer Pfad **C:\Windows\System32\CertSrv\CertEnroll** ein.
5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf **CertEnroll**, und klicken Sie anschließend auf **Berechtigungen bearbeiten**.

7 Entfernen Sie auf der Registerkarte Sicherheit alle Schreibzugriffe außer für das System.

8 Klicken Sie auf **OK**.

Konfigurieren des NDES-Servers

1 Melden Sie sich auf dem Server als Domänen-Benutzer **SCEPAdmin** an.

2 Klicken Sie im Server-Manager auf **Verwalten > Rollen und Funktion hinzufügen**.

3 Klicken Sie auf **Server-Rollen**, wählen Sie **Active Directory-Zertifikatdienste** und alle Funktionen aus, und klicken Sie anschließend auf **Weiter**.

4 Deaktivieren Sie im Bereich AD CS-Rollendienst die Option **Zertifizierungsstelle**.

5 Wählen Sie **Network Device Enrollment Service** und alle zugehörigen Funktionen aus, und klicken Sie anschließend auf **Weiter**.

6 Behalten Sie im Abschnitt Web-Server-Rolle (ISS) Rollendienste die Standardeinstellungen bei.

7 Klicken Sie nach der Installation auf **Active Directory-Zertifikatdienste auf dem Zielserver konfigurieren**.

8 Wählen Sie im Abschnitt Rollendienste die Option **Network Device Enrollment Service** aus, und klicken Sie anschließend auf **Weiter**.

9 Wählen Sie das Dienstkonto **SCEPSvc** aus.

10 Wählen Sie im Abschnitt CA für NDES entweder **CA-Name** oder **Computername** aus, und klicken Sie anschließend auf **Weiter**.

11 Geben Sie im Abschnitt RA-Informationen die Informationen an, und klicken Sie anschließend auf **Weiter**.

12 Gehen Sie im Abschnitt Kryptografie für NDES folgendermaßen vor:
- Wählen Sie die entsprechenden Signatur- und Kodierungsschlüsselanbieter aus.
- Wählen Sie im Menü Schlüssellänge dieselbe Schlüssellänge wie die des CA-Servers aus.

13 Klicken Sie auf **Weiter**.

14 Schließen Sie die Installation ab.

Sie können jetzt als SCEPSvc-Benutzer über einen Webbrowser auf den NDES-Server zugreifen. Auf dem NDES-Server können Sie den Fingerabdruck des CA-Zertifikats, das Abfrage-Kennwort der Registrierung und den Gültigkeitszeitraum des Abfrage-Kennworts anzeigen lassen.

Zugreifen auf den NDES-Server

Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein:
`http://`*`NDESserverIP`*`/certsrv/mscep_admin`, wobei ***`NDESserverIP`*** die IP-Adresse des NDES-Servers ist.

Konfigurieren von NDES für MVE

Hinweis: Stellen Sie zunächst sicher, dass der NDES-Server ordnungsgemäß funktioniert.

Erstellen einer Zertifikatvorlage

1. Öffnen Sie über die untergeordnete CA (certserv) die **Zertifizierungsstelle**.
2. Erweitern Sie die Zertifizierungsstelle im linken Bereich, klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**, und klicken Sie anschließend auf **Verwalten**.
3. Erstellen Sie in der Zertifikatvorlagen-Konsole eine Kopie des **Web-Servers**.
4. Geben Sie auf der Registerkarte Allgemein **`MVEWebServer`** als Vorlagennamen ein.
5. Geben Sie auf der Registerkarte Sicherheit den Benutzern **SCEPAdmin** und **SCEPSvc** die entsprechenden Berechtigungen.

   Hinweis: Weitere Informationen finden Sie unter "Erforderliche Benutzer" auf Seite 83.
6. Wählen Sie auf der Registerkarte Betreff-Name die Option **In der Anfrage angeben** aus.
7. Öffnen Sie über die untergeordnete CA (certserv) die **Zertifizierungsstelle**.
8. Wählen Sie auf der Registerkarte Erweiterungen **Anwendungsrichtlinien** > **Bearbeiten** aus.
9. Klicken Sie auf **Hinzufügen** >**Client-Authentifizierung** > **OK**.
10. Erweitern Sie die Zertifizierungsstelle im linken Bereich, klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**, und klicken Sie anschließend auf **Neu** > **Zertifikatvorlage zum Ausstellen**.
11. Wählen Sie die neu erstellen Zertifikate aus, und klicken Sie anschließend auf **OK**.

Sie können jetzt über das CA-Web-Registrierungsportal auf die Vorlagen zugreifen.

Zugriff auf die Vorlagen

1. Öffnen Sie einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: **`http://CAserverIP/certsrv/certrqxt.asp`**, wobei ***`CAserverIP`*** die IP-Adresse des CA-Servers ist.
2. Zeigen Sie die Vorlagen im Menü Zertifikatvorlagen an.

Einstellen von Zertifikatvorlagen für NDES

1. Starten Sie auf Ihrem Computer den Registry-Editor.
2. Navigieren Sie zu **HKEY_LOCAL_MACHINE** >**SOFTWARE** >**Microsoft** > **Cryptography** > **MSCEP**.
3. Konfigurieren Sie Folgendes, und legen Sie sie anschließend auf **MVEWebServer** fest:
   - EncryptionTemplate
   - GeneralPurposeTemplate
   - SignatureTemplate
4. Erteilen Sie dem SCEPSvc-Benutzer die volle Berechtigung für MSCEP.
5. Erweitern Sie im IIS-Manager die Zertifizierungsstelle, und klicken Sie anschließend auf **Anwendungspools**.
6. Klicken Sie im rechten Bereich auf **Neu starten**, um den SCEP-Anwendungspool neu zu starten.

7 Erweitern Sie die Zertifizierungsstelle im IIS-Manager, und erweitern Sie anschließend **Websites** > **Standard-Website**.

8 Klicken Sie im rechten Bereich auf **Neu starten**.

Deaktivieren von Kennwort abfragen im Microsoft CA-Server

1 Starten Sie auf Ihrem Computer den Registry-Editor.

2 Navigieren Sie zu **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP**.

3 Sellten Sie EnforcePassword auf **0** ein.

4 Erweitern Sie die Zertifizierungsstelle im IIS-Manager, klicken Sie auf **Anwendungspools**, und wählen Sie **SCEP** aus.

5 Klicken Sie im rechten Bereich auf **Erweiterte Einstellungen**.

6 Setzen Sie Benutzerprofil laden auf **Wahr**, und klicken Sie anschließend auf **OK**.

7 Klicken Sie im rechten Bereich auf **Neu starten**, um den SCEP-Anwendungspool neu zu starten.

8 Erweitern Sie die Zertifizierungsstelle im IIS-Manager, und erweitern Sie anschließend **Websites** > **Standard-Website**.

9 Klicken Sie im rechten Bereich auf **Neu starten**.

Beim Öffnen der NDES über den Webbrowser können Sie jetzt nur den CA-Fingerabdruck anzeigen lassen.

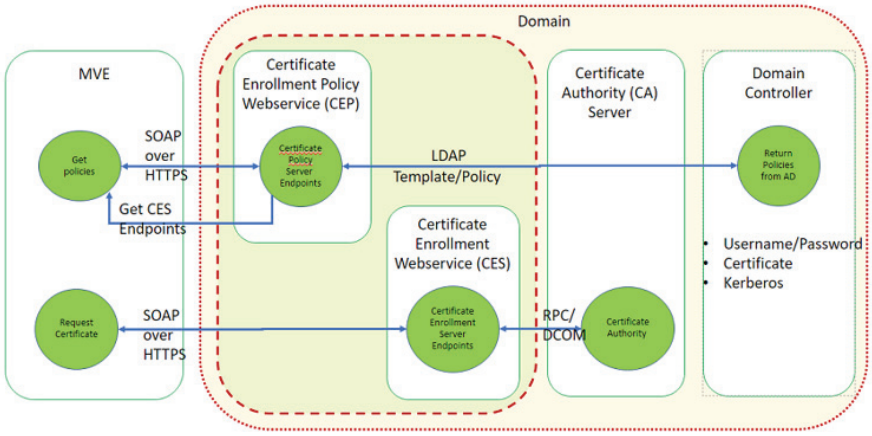
Verwalten von Zertifikaten mit Microsoft Certificate Authority über MSCEWS

Dieser Abschnitt enthält Informationen zur Konfiguration von Certificate Enrollment Policy Web Service (CEP) und Certificate Enrollment Web Service (CES). Da Microsoft empfiehlt, CEP und CES auf zwei verschiedenen Computern zu installieren, wird in diesem Dokument dasselbe beschrieben. Wir bezeichnen diese Webdienste als CEP-Server bzw. CES-Server.

Hinweis: Der Benutzer muss über eine vorkonfigurierte Enterprise Certificate Authority (CA) und einen Domänencontroller verfügen.

Systemvoraussetzungen

Das Betriebssystem Windows Server 2012 R2 wird für alle Einstellungen in diesem Abschnitt verwendet. Die folgenden Installationsanforderungen und -funktionen gelten für CEP und CES, sofern nicht anders angegeben.



Erstellen Sie die folgenden Kontotypen im Domänen-Controller:

- Service-Administrator: Benannt als **CEPAdmin** und **CESAdmin**
  - Dieser Benutzer muss Teil der **lokalen Admin-Gruppe** auf den entsprechenden CEP- und CES-Servern sein.
  - Dieser Benutzer muss Mitglied der **Unternehmensadmin**-Gruppe sein.
- Dienstkonto: Benannt als **CEPSvc** und **CESSvc**
  - Dieser Benutzer muss Teil der **lokalen IIS_IUSRS**-Gruppe sein.
  - Erfordert die Berechtigung zum **Anfordern von Zertifikaten** auf der Zertifizierungsstelle für den entsprechenden **CEPSvc** und **CESSvc**.

Anforderungen an die Netzwerkkonnektivität

- Die Anforderungen an die Netzwerkkonnektivität sind ein wichtiger Bestandteil des Deployment, insbesondere in Szenarien, in denen CEP und CES in einem Perimeter-Netzwerk gehostet werden.
- Die gesamte Clientverbindung zu beiden Diensten findet innerhalb einer HTTPS-Sitzung statt, sodass nur HTTPS-Datenverkehr zwischen dem Client und den Webdiensten zulässig ist.

- CEP kommuniziert mit Active Directory Domain Services (AD DS) über standardmäßige Lightweight Directory Access Protocol (LDAP)- und sichere LDAP (LDAPS)-Ports (TCP 389 bzw. 636).
- CES kommuniziert mit CA über DCOM (Distributed Component Object Model).

  Hinweise:

  - Standardmäßig verwendet DCOM willkürliche flüchtige Ports.
  - CA kann so konfiguriert werden, dass ein bestimmter Portbereich reserviert wird, um die Firewall-Konfiguration zu vereinfachen.

Erstellen von SSL-Zertifikaten für CEP- und CES-Server

CES und CEP müssen Secure Sockets Layer (SSL) für die Kommunikation mit Clients verwenden (über HTTPS). Jeder Dienst muss über ein gültiges Zertifikat verfügen, das über eine EKU-Richtlinie (Enhanced Key Usage) zur Serverauthentifizierung im lokalen Computerzertifikatsspeicher verfügt.

1. Installieren Sie den IIS-Dienst auf dem Server.
2. Melden Sie sich beim CEP-Server an, und fügen Sie dann das Root-CA-Zertifikat im Speicher der Trusted-Root-Zertifizierungsstelle hinzu.
3. Starten Sie die IIS-Verwaltungskonsole, und wählen Sie dann **Server-Startseite** aus.
4. Öffnen Sie in der Hauptansicht die Datei **Serverzertifikate** aus.
5. Klicken Sie auf **Aktionen** > **Zertifikatsanforderung erstellen**.
6. Geben Sie im Fenster Eigenschaften qualifizierter Verbindungsname die erforderlichen Informationen ein und klicken Sie dann auf **Weiter**.
7. Wählen Sie im Dialogfeld Eigenschaften Kryptografie-Serviceanbieter die Bitlänge aus, und klicken Sie dann auf **Weiter**.
8. Speichern Sie die Datei.
9. Lassen Sie die Datei von der Zertifizierungsstelle signieren, die Sie für CEP und CES verwenden möchten.

   Hinweis: Stellen Sie sicher, dass die EKU der Serverauthentifizierung im signierten Zertifikat aktiviert ist.
10. Kopieren Sie die signierte Datei zurück auf den CEP-Server.
11. Wählen Sie in der IIS-Verwaltungskonsole die Option **Server-Startseite** aus.
12. Öffnen Sie im Abschnitt Hauptansicht die Option **Serverzertifikate**.
13. Klicken Sie auf **Aktionen** > **Zertifikatsanforderung abschließen**.
14. Wählen Sie im Fenster Antwort der Zertifizierungsstelle angeben die signierte Datei aus.
15. Geben Sie einen Namen ein, und wählen Sie dann im Menü Zertifikatsspeicher die Option **Persönlich**aus.
16. Schließen Sie die Zertifikatsinstallation ab.
17. Wählen Sie in der IIS-Verwaltungskonsole die Standard-Website aus.
18. Klicken Sie auf **Aktionen** > **Bindungen**.
19. Klicken Sie im Dialogfeld Websitebindungen auf **Hinzufügen**.
20. Stellen Sie im Dialogfeld Websitebindung hinzufügen den Typ auf **https** ein, und suchen Sie dann im SSL-Zertifikat nach dem neu erstellten Zertifikat.

21 Wählen Sie in der IIS-Verwaltungskonsole die Option **Standard-Website** aus, und öffnen Sie dann die SSL-Einstellungen.

22 Aktivieren Sie SSL erforderlich, und stellen Sie Clientzertifikate auf **Ignorieren** ein.

23 Starten Sie IIS neu.

Hinweis: Gehen Sie beim CES-Server genauso vor.

Erstellen von Zertifikatsvorlagen

Der Benutzer muss eine Zertifikatsvorlage für die Zertifikatsregistrierung erstellen. Gehen Sie wie folgt vor, um aus einer vorhandenen Zertifikatsvorlage zu kopieren:

1 Melden Sie sich bei der Enterprise CA mit den Anmeldeinformationen für den CA-Administrator an.

2 Erweitern Sie die Zertifizierungsstelle, klicken Sie mit der rechten Maustaste auf **Zertifikatsvorlagen**, und klicken Sie anschließend auf **Verwalten**.

3 Klicken Sie in der Konsole der Zertifikatsvorlage mit der rechten Maustaste auf **Webserver-Zertifikatsvorlage**, und klicken Sie dann auf **Vorlage duplizieren**.

4 Geben Sie auf der Registerkarte Allgemein der Vorlage den Namen **MVEWebServer**.

5 Geben Sie auf der Registerkarte Sicherheit dem CA-Administrator **Lese**-, **Schreib**- und **Registrierungsberechtigungen**.

6 Erteilen Sie den authentifizierten Benutzern **Lese**- und **Registrierungsberechtigungen**.

7 Wählen Sie auf der Registerkarte Betreff-Name die Option **In der Anfrage angeben** aus.

8 Legen Sie auf der Registerkarte Allgemein den Gültigkeitszeitraum des Zertifikats fest.

9 Wenn Sie diese Zertifikatsvorlage für die Ausgabe eines **802.1X-Zertifikats** für Drucker verwenden möchten, gehen Sie wie folgt vor:

   a Wählen Sie auf der Registerkarte **Erweiterungen** die Option **Anwendungsrichtlinien** aus der Liste der Erweiterungen aus, die in dieser Vorlage enthalten sind.

   b Klicken Sie auf **Bearbeiten** > **Hinzufügen**.

   c Wählen Sie im Dialogfeld Anwendungsrichtlinie hinzufügen die Option **Clientauthentifizierung** aus.

   d Klicken Sie auf **OK**.

10 Klicken Sie im Dialogfeld Eigenschaften der Zertifikatsvorlage auf **OK**.

11 Klicken Sie im CA-Fenster mit der rechten Maustaste auf **Zertifikatsvorlagen**, und klicken Sie dann auf **Neue** > **Zertifikatsvorlage**.

12 Wählen Sie **MVEWebServer** aus und klicken Sie auf **OK**.

Überblick über die Authentifizierungsmethoden

CEP und CES unterstützen die folgenden Authentifizierungsmethoden:

- Integrierte Windows-Authentifizierung, auch bekannt als **Kerberos-Authentifizierung**
- Clientzertifikat-Authentifizierung, auch bekannt als **X.509-Zertifikatsauthentifizierung**
- **Authentifizierung mit Benutzername und Kennwort**

Integrierte Windows-Authentifizierung

Die integrierte Windows-Authentifizierung verwendet Kerberos, um einen ununterbrochenen Authentifizierungsfluss für Geräte bereitzustellen, die mit dem internen Netzwerk verbunden sind. Diese Methode wird für interne Deployments bevorzugt, da sie die vorhandene Kerberos-Infrastruktur in AD DS verwendet. Außerdem sind minimale Änderungen an den Clientcomputern für Zertifikate erforderlich.

Hinweis: Verwenden Sie diese Authentifizierungsmethode, wenn Clients *nur* auf den Webdienst zugreifen müssen, während sie direkt mit Ihrem internen Netzwerk verbunden sind.

Clientzertifikat-Authentifizierung

Diese Methode wird gegenüber der Authentifizierung mit Benutzername und Kennwort bevorzugt, da sie sicherer ist. Es ist keine direkte Verbindung zum Unternehmensnetzwerk erforderlich.

Hinweise:

- Verwenden Sie diese Authentifizierungsmethode, wenn Sie Clients digitale X.509-Zertifikate zur Authentifizierung bereitstellen möchten.
- Mit dieser Methode werden die im Internet verfügbaren Webdienste aktiviert.

Authentifizierung mithilfe von Benutzername und Kennwort

Die Methode mit Benutzername und Kennwort ist die einfachste Form der Authentifizierung. Diese Methode wird in der Regel für Clients verwendet, die nicht direkt mit dem internen Netzwerk verbunden sind. Die Authentifizierungsoption ist weniger sicher als die Clientzertifikat-Authentifizierung, erfordert jedoch keine Bereitstellung eines Zertifikats.

Hinweis: Verwenden Sie diese Authentifizierungsmethode, wenn Sie über das interne Netzwerk oder über das Internet auf den Webdienst zugreifen können.

Delegationsanforderungen

Durch eine Delegation kann ein Dienst die Identität eines Benutzer- oder Computerkontos für den Zugriff auf Ressourcen im gesamten Netzwerk annehmen.

Eine Delegation ist für den CES-Server erforderlich, wenn alle folgenden Szenarien zutreffen:

- CA und CES befinden sich nicht auf demselben Computer.
- CES kann anfängliche Anmeldeanforderungen verarbeiten, anstatt nur Verlängerungsanfragen für Zertifikate zu verarbeiten.
- Der Authentifizierungstyp ist auf **integrierte Windows-Authentifizierung** oder **Clientzertifikat-Authentifizierung**eingestellt.

In den folgenden Szenarien ist für den CES-Server keine Delegation erforderlich:

- CA und CES befinden sich auf demselben Computer.
- Benutzername und Kennwort sind die Authentifizierungsmethode.

Hinweise:

- Microsoft empfiehlt, CEP und CES als Domänenbenutzerkonten auszuführen.
- Benutzer müssen einen geeigneten Service Principal Name (SPN) erstellen, bevor sie die Delegation auf dem Domainbenutzerkonto konfigurieren.

Ermöglichen der Delegation

1. Um eine SPN für ein Domänenbenutzerkonto zu erstellen, verwenden Sie den Befehl **setspn** wie folgt:

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

   Hinweise:

   - Der Kontoname lautet CESSvc.
   - CES wird auf einem Computer mit einem vollqualifizierten Domänennamen (FQDN) von **ces.msca.com** in der Domäne msca.com ausgeführt.

2. Öffnen Sie das CESSvc-Domänen-Benutzerkonto im Domänencontroller.
3. Wählen Sie auf der Registerkarte Delegation die Option **Diesem Benutzer nur für die Delegation an bestimmte Dienste vertrauen** aus.
4. Wählen Sie die geeignete Delegation basierend auf der Authentifizierungsmethode aus.

   Hinweise:

   - Wenn Sie die integrierte Windows-Authentifizierung auswählen, konfigurieren Sie die Delegation so, dass **nur Kerberos** verwendet wird.
   - Wenn der Dienst die Clientzertifikat-Authentifizierung verwendet, konfigurieren Sie die Delegation so, dass ein beliebiges Authentifizierungsprotokoll verwendet wird.
   - Wenn Sie mehrere Authentifizierungsmethoden konfigurieren möchten, konfigurieren Sie die Delegation für die Verwendung eines beliebigen Authentifizierungsprotokolls.

5. Klicken Sie auf **Hinzufügen**.
6. Wählen Sie im Dialogfeld Dienste hinzufügen **Benutzer** oder **Computer** aus.
7. Geben Sie den Hostnamen des CA-Servers ein, und klicken Sie dann auf **Namen prüfen**.
8. Wählen Sie im Dialogfeld Dienste hinzufügen einen der folgenden Dienste aus, die delegiert werden sollen:
   - Hostservice (HOST) für diesen CA-Server
   - Remote Procedure Call System Service (RPCSS) für diesen CA-Server
9. Schließen Sie das Dialogfeld „Domänenbenutzereigenschaften“.

Für CEP-Domänenbenutzer, die die Windows-integrierte Authentifizierung verwenden, gehen Sie wie folgt vor:

1. Um eine SPN für ein Domänenbenutzerkonto zu erstellen, verwenden Sie den Befehl **setspn** wie folgt:

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

   Hinweis: Der Kontoname lautet CESSvc.

2. Öffnen Sie das CEPSvc-Domänenbenutzerkonto im Domänencontroller.
3. Wählen Sie auf der Registerkarte Delegation die Option **Diesem Benutzer für die Delegation nicht vertrauen** aus.

Konfigurieren der integrierten Windows Authentifizierung

Verwenden Sie Windows PowerShell, um CEP und CES zu installieren.

CEP konfigurieren

Das cmdlet **Install-AdcsRegistrmentPolicyWebService** konfiguriert den Certificate Enrollment Policy Web Service (CEP). Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1. Melden Sie sich mit dem CEPAdmin-Benutzernamen an, und starten Sie dann PowerShell im Administratormodus.
2. Führen Sie den Befehl **`Import-Module ServerManager`** aus.
3. Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Pol`** aus.
4. Führen Sie den Befehl **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Kerberos -SSLCertThumbprint "sslCertThumbPrint"`** aus.

   Hinweis: Ersetzen Sie *<sslCertThumbPrint>* durch den Thumbprint des für den CEP-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.
5. Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.
6. Starten Sie die IIS-Verwaltungskonsole.
7. Erweitern Sie im Bereich Verbindungen den Webserver, der CEP hostet.
8. Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung **ADPolicyProvider_CEP_Kerberos**.
9. Doppelklicken Sie in der virtuellen Anwendung **Home** auf Anwendungseinstellungen, und doppelklicken Sie dann **auf FriendlyName**.
10. Geben Sie unter Wert einen Namen ein, und schließen Sie dann das Dialogfeld.
11. Doppelklicken Sie auf **URI**, und kopieren Sie dann **Wert**.

    Hinweise:

    - Wenn Sie eine andere Authentifizierungsmethode auf demselben CEP-Server konfigurieren möchten, müssen Sie die ID ändern.
    - Diese URL wird in MVE oder einer beliebigen Clientanwendung verwendet.
12. Klicken Sie im linken Bereich auf **Anwendungspools**.
13. Wählen Sie **WSEnrollmentPolicyServer** aus, und klicken Sie dann im rechten Bereich auf **Aktionen** > **Erweiterte Einstellungen**.
14. Wählen Sie unter Prozessmodell das Identitätsfeld aus.
15. Wählen Sie im Dialogfeld Anwendungspool-Identität das benutzerdefinierte Konto aus, und geben Sie dann **`CEPSvc`** als Domänenbenutzernamen ein.
16. Schließen Sie alle Dialogfelder, und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.
17. Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.

CES konfigurieren

Das **Install-AdcsEnrollmentWebService** cmdlet konfiguriert den Certificate Enrollment Web Service (CES). Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1. Melden Sie sich mit dem **`CESAdmin`**-Benutzernamen beim CES-Server an, und starten Sie dann PowerShell im Administratormodus.
2. Führen Sie den Befehl **`Import-Module ServerManager`** aus.
3. Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Svc`** aus.
4. Führen Sie den Befehl **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Kerberos`** aus.

   Hinweise:

   - Ersetzen Sie *<sslCertThumbPrint>* durch den Thumbprint des für den CES-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.
   - Ersetzen Sie **`CA1.contoso.com`** durch den CA-Computernamen.
   - Ersetzen Sie **`contoso-CA1-CA`** durch den gemeinsamen CA-Namen.
5. Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.
6. Starten Sie die IIS-Verwaltungskonsole.
7. Erweitern Sie im Bereich Verbindungen den Webserver, der CES hostet.
8. Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung: **contoso-CA1-CA _CES_Kerberos**.
9. Klicken Sie im linken Bereich auf **Anwendungspools**.
10. Wählen Sie **WSEnrollmentServer** aus, und klicken Sie dann im rechten Bereich auf **Aktionen** > **Erweiterte Einstellungen**.
11. Wählen Sie unter Prozessmodell das Identitätsfeld aus.
12. Wählen Sie im Dialogfeld **`Anwendungspool-Identität`** das benutzerdefinierte Konto aus, und geben Sie dann **`CESSvc`** als Domänenbenutzernamen ein.
13. Schließen Sie alle Dialogfelder und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.
14. Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.
15. Aktivieren Sie für CESSvc-Domänenbenutzer die Delegierung. Weitere Informationen finden Sie unter "Ermöglichen der Delegation" auf Seite 94.

Konfigurieren der Clientzertifikat-Authentifizierung

CEP konfigurieren

Das cmdlet **Install-AdcsRegistrmentPolicyWebService**konfiguriert CEP. Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1. Melden Sie sich mit dem CEPAdmin-Benutzernamen an, und starten Sie dann PowerShell im Administratormodus.
2. Führen Sie den Befehl **`Import-Module ServerManager`** aus.
3. Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Pol`** aus.
4. Führen Sie den Befehl **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType Certificate -SSLCertThumbprint "sslCertThumbPrint"`** aus.

   Hinweis: Ersetzen Sie <*sslCertThumbPrint*> durch den Thumbprint des für den CEP-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.
5. Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.
6. Starten Sie die IIS-Verwaltungskonsole.
7. Erweitern Sie im Bereich Verbindungen den Webserver, der CEP hostet.
8. Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung **ADPolicyProvider_CEP_Certificate**.
9. Doppelklicken Sie in der virtuellen Anwendung **Home** auf Anwendungseinstellungen, und doppelklicken Sie dann **auf FriendlyName**.
10. Geben Sie unter Wert einen Namen ein, und schließen Sie das Dialogfeld.
11. Doppelklicken Sie auf **URI**, und kopieren Sie dann **Wert**.

    Hinweise:

    - Wenn Sie eine andere Authentifizierungsmethode auf demselben CEP-Server konfigurieren möchten, müssen Sie die ID ändern.
    - Diese URL wird in MVE oder einer beliebigen Clientanwendung verwendet.
12. Klicken Sie im linken Bereich auf **Anwendungspools**.
13. Wählen Sie **WSEnrollmentPolicyServer** aus, und klicken Sie dann im rechten Bereich auf **Aktionen** > **Erweiterte Einstellungen**.
14. Wählen Sie unter Prozessmodell das Identitätsfeld aus.
15. Wählen Sie im Dialogfeld Anwendungspool-Identität das benutzerdefinierte Konto aus, und geben Sie dann **`CEPSvc`** als Domänenbenutzernamen ein.
16. Schließen Sie alle Dialogfelder, und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.
17. Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.

CES konfigurieren

Das **Install-AdcsEnrollmentWebService** cmdlet konfiguriert den Certificate Enrollment Web Service (CES). Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1. Melden Sie sich mit dem **`CESAdmin`**-Benutzernamen beim CES-Server an, und starten Sie dann PowerShell im Administratormodus.
2. Führen Sie den Befehl **`Import-Module ServerManager`** aus.
3. Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Svc`** aus.
4. Führen Sie den Befehl **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType Certificate`** aus.

   Hinweise:

   - Ersetzen Sie *<sslCertThumbPrint>* durch den Thumbprint des für den CES-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.
   - Ersetzen Sie **`CA1.contoso.com`** durch den CA-Computernamen.
   - Ersetzen Sie **`contoso-CA1-CA`** durch den gemeinsamen CA-Namen.
   - Wenn Sie bereits eine Authentifizierungsmethode auf dem Host konfiguriert haben, entfernen Sie **`ApplicationPoolIdentity`** aus dem Befehl.
5. Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.
6. Starten Sie die IIS-Verwaltungskonsole.
7. Erweitern Sie im Bereich Verbindungen den Webserver, der CEP hostet.
8. Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung: **contoso-CA1-CA _CES_Certificate**.
9. Klicken Sie im linken Bereich auf **Anwendungspools**.
10. Wählen Sie **WSEnrollmentServer** aus und klicken Sie dann im rechten Bereich auf **Aktionen** > **Erweiterte Einstellungen**.
11. Wählen Sie unter Prozessmodell das Identitätsfeld aus.
12. Wählen Sie im Dialogfeld Anwendungspool-Identität das benutzerdefinierte Konto aus, und geben Sie dann **CESSvc** als Domänenbenutzernamen ein.
13. Schließen Sie alle Dialogfelder und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.
14. Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.
15. Aktivieren Sie für CESSvc-Domänenbenutzer die Delegierung. Weitere Informationen finden Sie unter "Ermöglichen der Delegation" auf Seite 94.

Erstellen eines Clientzertifikats

1. Öffnen Sie von einem beliebigen Domänenbenutzerkonto aus **certlm.msc**.
2. Klicken Sie auf **Zertifikate** > **Persönlich** > **Zertifikate** > **Alle Aufgaben** > **Neues Zertifikat anfordern**.
3. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Active Directory-Registrierung** > **Clientzugriff**.

Hinweis: Gehen Sie wie folgt vor, wenn Sie die Optionen zur **Active Directory-Registrierung** nicht verwenden möchten:

a Klicken Sie auf **Von mir konfiguriert** > **Neue hinzufügen**.

b Geben Sie den Enrollment Policy Server-URI als CEP-Serveradresse für Username_Password oder die Kerberos-Authentifizierung ein.

c Wählen Sie als Authentifizierungstyp **Integrierte Windows-Authentifizierung**aus.

d Klicken Sie auf **Server validieren**.

e Klicken Sie nach der erfolgreichen Validierung auf **Hinzufügen**.

f Klicken Sie auf **Weiter**.

g Wählen Sie eine beliebige Vorlage aus.

5 Klicken Sie auf **Details** > **Eigenschaften**.

6 Klicken Sie auf **Integrieren**.

7 Geben Sie auf der Registerkarte Betreff einen vollständigen Domänennamen (FQDN) an.

8 Wählen Sie auf der Registerkarte Privater Schlüssel die Option **Privaten Schlüssel exportierbar machen**.

9 Klicken Sie auf **Anwenden** > **Integrieren**.

Führen Sie nach der Registrierung des Clientzertifikats die folgenden Schritte aus, um das Clientzertifikat im PFX-Format zu exportieren.

1 Klicken Sie auf **Zertifikat** > **Alle Aufgaben** > **Exportieren**.

2 Klicken Sie auf **Weiter** > **Ja, privaten Schlüssel exportieren**.

3 Klicken Sie auf **Weiter**.

4 Geben Sie das vom Client bereitgestellte Kennwort ein.

5 Klicken Sie auf **Weiter**.

6 Geben Sie den Dateinamen im Dialogfeld Zertifikatexport an.

7 Klicken Sie auf **Weiter** > **Fertig stellen**.

Konfigurieren der Authentifizierung mit Benutzername und Kennwort

CEP konfigurieren

Das cmdlet **Install-AdcsRegistrmentPolicyWebService** konfiguriert den Certificate Enrollment Policy Web Service (CEP). Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1 Melden Sie sich mit dem CEPAdmin-Benutzernamen an, und starten Sie dann PowerShell im Administratormodus.

2 Führen Sie den Befehl **`Import-Module ServerManager`** aus.

3 Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Pol`** aus.

4. Führen Sie den Befehl **`Install-AdcsEnrollmentPolicyWebService -AuthenticationType UserName -SSLCertThumbprint "sslCertThumbPrint"`** aus.

   Hinweis: Ersetzen Sie *<sslCertThumbPrint>* durch den Thumbprint des für den CEP-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.

5. Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.
6. Starten Sie die IIS-Verwaltungskonsole.
7. Erweitern Sie im Bereich Verbindungen den Webserver, der CEP hostet.
8. Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung: **ADPolicyProvider_CEP_UsernamePassword**.
9. Doppelklicken Sie in der virtuellen Anwendung **Home** auf Anwendungseinstellungen, und doppelklicken Sie dann **auf FriendlyName**.
10. Geben Sie unter **Wert** einen Namen ein, und schließen Sie das Dialogfeld.
11. Doppelklicken Sie auf **URI**, und kopieren Sie dann **Wert**.

    Hinweise:

    - Wenn Sie eine andere Authentifizierungsmethode auf demselben CEP-Server konfigurieren möchten, müssen Sie die ID ändern.
    - Diese URL wird in MVE oder einer beliebigen Clientanwendung verwendet.
12. Klicken Sie im linken Bereich auf **Anwendungspools**.
13. Wählen Sie **WSEnrollmentPolicyServer** aus, und klicken Sie dann im rechten Bereich auf **Aktionen** > **Erweiterte Einstellungen**.
14. Wählen Sie unter Prozessmodell das Identitätsfeld aus.
15. Wählen Sie im Dialogfeld Anwendungspool-Identität das benutzerdefinierte Konto aus, und geben Sie dann **`CEPSvc`** ein.
16. Schließen Sie alle Dialogfelder, und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.
17. Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.

CES konfigurieren

Das **Install-AdcsEnrollmentWebService** cmdlet konfiguriert den Certificate Enrollment Web Service (CES). Es wird auch verwendet, um andere Instanzen des Dienstes innerhalb einer vorhandenen Installation zu erstellen.

1. Melden Sie sich mit dem **`CESAdmin`**-Benutzernamen beim CES-Server an, und starten Sie dann PowerShell im Administratormodus.
2. Führen Sie den Befehl **`Import-Module ServerManager`** aus.
3. Führen Sie den Befehl **`Add-WindowsFeature Adcs-Enroll-Web-Svc`** aus.
4. Führen Sie den Befehl **`Install-AdcsEnrollmentWebService -ApplicationPoolIdentity -CAConfig "CA1.contoso.com\contoso-CA1-CA" -SSLCertThumbprint "sslCertThumbPrint" -AuthenticationType UserName`** aus.

Hinweise:

- Ersetzen Sie *<sslCertThumbprint>* durch den Thumbprint des für den CES-Server erstellten SSL-Zertifikats, nachdem Sie die Leerzeichen zwischen den Thumbprint-Werten gelöscht haben.
- Ersetzen Sie **`CA1.contoso.com`** durch den CA-Computernamen.
- Ersetzen Sie **`contoso-CA1-CA`** durch den gemeinsamen CA-Namen.
- Wenn Sie bereits eine Authentifizierungsmethode auf dem Host konfiguriert haben, entfernen Sie **`ApplicationPoolIdentity`** aus dem Befehl.

5 Schließen Sie die Installation ab, indem Sie entweder **Y** oder **A** auswählen.

6 Starten Sie die IIS-Verwaltungskonsole.

7 Erweitern Sie im Bereich Verbindungen den Webserver, der CES hostet.

8 Erweitern Sie **Sites**, erweitern Sie **Standard-Website**, und klicken Sie dann auf den Namen der entsprechenden virtuellen Installationsanwendung: **contoso-CA1-CA_CES_UsernamePassword**.

9 Klicken Sie im linken Bereich auf **Anwendungspools**.

10 Wählen Sie **WSEnrollmentServer** aus und klicken Sie dann im rechten Bereich unter Aktionen auf **Aktionen** > **Erweiterte Einstellungen**.

11 Wählen Sie unter Prozessmodell das Identitätsfeld aus.

12 Wählen Sie im Dialogfeld Anwendungspool-Identität das benutzerdefinierte Konto aus, und geben Sie dann **`CESSvc`** als Domänenbenutzernamen ein.

13 Schließen Sie alle Dialogfelder und recyceln Sie dann IIS im rechten Bereich der IIS-Verwaltungskonsole.

14 Geben Sie in PowerShell **`iisreset`** ein, um IIS neu zu starten.

Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über SCEP

In diesem Abschnitt wird beschrieben, wie Sie OpenXPKI CA Version 2.5.x mit dem Simple Certificate Enrollment Protocol (SCEP) konfigurieren.

Hinweise:

- Stellen Sie sicher, dass Sie das Betriebssystem Debian 8 Jessie verwenden.
- Weitere Informationen zu OpenXPKI erhalten Sie unter **www.openxpki.org**.

Konfigurieren von OpenXPKI CA

Installieren von OpenXPKI CA

1 Verbinden Sie den Computer mit PuTTY oder einem anderen Client.

2 Führen Sie auf dem Client den Befehl **`sudo su -`** aus, um zum Root-Benutzer zu gelangen.

3 Geben Sie das Root-Kennwort ein.

4 Ändern Sie in **nano /etc/apt/sources.list** die Quelle zum Installieren der Updates.

5 Aktualisieren Sie die Datei. Beispiel:

```
#

# 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 Speichern Sie die Datei.

7 Führen Sie die folgenden Befehle aus:

- **apt-get Update**
- **apt-get Upgrade**

8 Aktualisieren Sie die CA-Zertifikatlisten auf dem Server mit **apt-get install ca-certificates**.

9 Installieren Sie **en_US.utf8 locale** mit **dpkg-reconfigure locales**.

10 Wählen Sie das Gebietsschema **en_US.UTF-8 UTF-8** aus, und machen Sie es anschließend zum standardmäßigen Gebietsschema für das System.

Hinweis: Verwenden Sie die Tabulatortaste und die Leertaste zum Auswählen und Navigieren im Menü.

11 Prüfen Sie die Gebietsschemas, die Sie mit **locale –a** generiert haben.

Beispielausgabe

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

12 Kopieren Sie den Fingerabdruck des OpenXPKI-Pakets mit **nano /home/Release.key**. Kopieren Sie den Schlüssel beispielsweise in **/home**.

13 Geben Sie **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** als Wert ein.

14 Führen Sie den folgenden Befehl aus:

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

15 Fügen Sie das Paket mit dem Befehl **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -** hinzu.

16 Fügen Sie das Repository mit **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list** und anschließend **aptitude update** zu Ihrer Quellenliste (jessie) hinzu.

17 Installieren Sie MySQL und Perl MySQL-Binding mit **aptitude install mysql-server libdbd-mysql-perl**.

18 Installieren Sie apache2.2-common mit **aptitude install apache2.2-common**.

19 Installieren Sie in **nano /etc/apt/sources.list** das fastcgi-Modul, um die Benutzeroberfläche zu beschleunigen.

Hinweis: Wir empfehlen die Verwendung von **mod_fcgid**.

20 Fügen Sie die Zeile **deb http://http.us.debian.org/debian/jessie main** in der Datei hinzu, und speichern Sie sie.

21 Führen Sie die folgenden Befehle aus:

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

22 Aktivieren Sie das fastcgi-Modul mit **a2enmod fcgid**.

23 Installieren Sie das OpenXPKI-Kernpaket mit **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Starten Sie den Apache® Server mit **service apache2 restart** neu.

25 Prüfen Sie mit **openxpkiadm version**, ob die Installation erfolgreich war.

Hinweis: Wenn die Installation erfolgreich war, zeigt das System die Version der installierten OpenXPKI an. Beispiel: **Version (core): 2.5.5**.

26 Erstellen Sie die leere Datenbank, und weisen Sie anschließend den Datenbankbenutzer mit **mysql -u root -p** zu.

Hinweise:

- Dieser Befehl muss in den Client eingegeben werden. Andernfalls können Sie das Kennwort nicht eingeben.
- Geben Sie das Passwort für MySQL ein. In diesem Beispiel ist **root** der MySQL-Benutzer.
- **openxpki** ist der Benutzer, auf dem OpenXPKI installiert ist.

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

Wenn der MySQL-Service nicht läuft, führen Sie **/etc/init.d/mysql start** aus, um den Service zu starten.

27 Geben Sie **quit** ein, um MySQL zu beenden.

28 Speichern Sie die verwendeten Zugangsdaten in **/etc/openxpki/config.d/system/database.yaml**.

Beispielhafter Datei-Inhalt

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

Hinweis: Ändern Sie **user** und **passwd** so, dass sie mit dem MySQL-Benutzernamen und -Kennwort übereinstimmen.

29 Speichern Sie die Datei.

30 Führen Sie für ein leeres Datenbankschema **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki** aus der bereitgestellten Schemadatei aus.

31 Geben Sie das Kennwort für die Datenbank ein.

Konfigurieren von OpenXPKI CA mit Standardskript

Hinweis: Das Standardskript konfiguriert nur den Standardbereich **ca-one**. CDP und CRLs sind nicht konfiguriert.

1 Entpacken Sie das Beispielskript für die Installation des Zertifikats mit **gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz**.

2 Führen Sie das Skript mit **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh** aus.

3 Bestätigen Sie das Setup mit **openxpkiadm alias --realm ca-one**.

Beispielausgabe

```
=== 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 Prüfen Sie mit **openxpkictl start**, ob die Installation erfolgreich war.

Beispielausgabe

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

5 Gehen Sie folgendermaßen vor, um auf den OpenXPKI-Server zuzugreifen:
   a Geben Sie in einem Webbrowser **`http://ipaddress/openxpki/`** ein.
   b Melden Sie sich als **Bediener** an. Das Standardkennwort lautet **`openxpki`**.

   Hinweis: Die Bedieneranmeldung hat zwei vorkonfigurierte Bedienerkonten, **raop** und **raop2**.
6 Erstellen Sie eine Zertifikatsanforderung, und testen Sie sie.

Manuelles Konfigurieren von OpenXPKI CA

Übersicht

Hinweis: Stellen Sie zu Beginn sicher, dass Sie über die grundlegenden Kenntnisse für das Erstellen von OpenSSL-Zertifikaten verfügen.

Erstellen Sie zum manuellen Konfigurieren der OpenXPKI CA Folgendes:

1 Root-CA-Zertifikat Weitere Informationen finden Sie unter "Erstellen eines Root-CA-Zertifikats" auf Seite 107.
2 CA-Signaturgeberzertifikat, signiert von der Root-CA. Weitere Informationen finden Sie unter "Erstellen eines Signaturgeberzertifikats" auf Seite 107.
3 Datentresorzertifikat, selbstsigniert. Weitere Informationen finden Sie unter "Erstellen eines Tresorzertifikats" auf Seite 107.
4 SCEP-Zertifikat, vom Signaturgeberzertifikat signiert.

Hinweise:

- Verwenden Sie bei der Auswahl des Signatur-Hash entweder SHA256 oder SHA512.
- Die Änderung der Größe des öffentlichen Schlüssels ist optional.

In diesem Fall verwenden wir das Verzeichnis **/etc/certs/openxpki_ca-one/** zur Zertifikatgenerierung. Sie können jedoch jedes beliebige Verzeichnis verwenden.

Erstellen einer OpenSSL-Konfigurationsdatei

1 Führen Sie den folgenden Befehl aus:

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

   Hinweis: Wenn Ihr Server unter Verwendung des FQDN (Fully Qualified Domain Name) erreichbar ist, verwenden Sie den DNS des Servers anstelle seiner IP-Adresse.

Beispieldatei

```
# 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 Ändern Sie die IP-Adresse und den CA-Zertifikatnamen mit den Setup-Informationen.

3 Speichern Sie die Datei.

Erstellen einer Kennwortdatei für Zertifikatschlüssel

1 Führen Sie den folgenden Befehl aus:

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

2 Geben Sie Ihr Kennwort ein.

3 Speichern Sie die Datei.

Erstellen eines Root-CA-Zertifikats

Hinweis: Sie können ein selbstsigniertes Root-CA-Zertifikat erstellen oder eine Zertifikatsanforderung generieren und diese anschließend von der Root-CA signieren lassen.

Führen Sie die folgenden Befehle aus:

Hinweis: Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

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**

Erstellen eines Signaturgeberzertifikats

Hinweis: Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

1 Führen Sie den folgenden Befehl aus:

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

2 Ändern Sie den Betreff in der Anforderung mit Ihren CA-Informationen mit **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 Rufen Sie das von der Root-CA signierte Zertifikat mit **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** ab.

Erstellen eines Tresorzertifikats

Hinweise:

- Das Tresorzertifikat ist selbstsigniert.

- Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

1 Führen Sie den folgenden Befehl aus:

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

2 Ändern Sie den Betreff in Ihren CA-Informationen mit **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 Führen Sie den folgenden Befehl aus:

```
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
```

Erstellen eines SCEP-Zertifikats

Hinweis: Das SCEP-Zertifikat wird vom Signaturgeberzertifikat signiert.

Führen Sie die folgenden Befehle aus:

Hinweis: Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

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
```

Kopieren der Schlüsseldatei und Erstellen eines Symlinks

1 Kopieren Sie die Schlüsseldateien nach **/etc/openxpki/ca/ca-one/**.

Hinweis: Die Schlüsseldateien müssen von OpenXPKI gelesen werden können.

```
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 Erstellen Sie den Symlink.

Hinweis: Symlinks sind Aliase, die von der Standardkonfiguration verwendet werden.

```
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
```

Importieren von Zertifikaten

Importieren Sie das Root-Zertifikat, das Signaturgeberzertifikat, das Tresorzertifikat und das SCEP-Zertifikat mit den entsprechenden Token in die Datenbank.

Führen Sie die folgenden Befehle aus:

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. Prüfen Sie mit **openxpkiadm alias --realm ca-one**, ob der Import erfolgreich war.

Beispielausgabe

```
=== 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
```

Starten von OpenXPKI

1 Führen Sie den Befehl **`openxpkictl start`** aus.

Beispielausgabe

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

2 Gehen Sie folgendermaßen vor, um auf den OpenXPKI-Server zuzugreifen:

a Geben Sie in einem Webbrowser **`http://ipaddress/openxpki/`** ein.

Hinweis: Anstelle von **`ipaddress`** können Sie auch den FQDN des Servers verwenden.

b Melden Sie sich als **Bediener** an. Das Standardkennwort lautet **`openxpki`**.

Hinweis: Die Bedieneranmeldung hat zwei vorkonfigurierte Bedienerkonten, **raop** und **raop2**.

3 Erstellen Sie eine Zertifikatsanforderung, und testen Sie sie.

Generieren von CRL-Informationen

Hinweis: Wenn Ihr Server über FQDN erreichbar ist, verwenden Sie den DNS des Servers anstelle seiner IP-Adresse.

1 Stoppen Sie den OpenXPKI-Service mit **`Openxpkictl stop`**.

2 Aktualisieren Sie in **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml** den Abschnitt **`connectors: cdp`** wie folgt:

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

a Aktualisieren Sie in **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml** Folgendes:

- **`crl_distribution_points:`** section

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

- **`authority_info_access:`** section

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

Ändern Sie die IP-Adresse und den CA-Zertifikatnamen entsprechend Ihrem CA-Server.

b Gehen Sie in **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml** wie folgt vor:

- Aktualisieren Sie ggf. **`nextupdate`** und **`renewal`**.
- Fügen Sie **`ca_issuers`** zum folgenden Abschnitt hinzu:

```
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/
```

Ändern Sie die IP-Adresse und den CA-Zertifikatnamen entsprechend Ihrem CA-Server.

3 Starten Sie den OpenXPKI-Service mit **`Openxpkictl start`**.

Konfigurieren der CRL-Zugänglichkeit

1 Beenden Sie den Apache-Dienst mit **`service apache2 stop`**.

2 Erstellen Sie ein Verzeichnis **CertEnroll** für crl im Verzeichnis **/var/www/openxpki/**.

3 Legen Sie **openxpki** als Eigentümer dieses Verzeichnisses fest, und konfigurieren Sie anschließend die Berechtigungen für das Lesen und Ausführen von Apache sowie für andere Dienste als schreibgeschützt.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Fügen Sie eine Referenz zur Apache-Datei alias.conf mit **`nano /etc/apache2/mods-enabled/alias.conf`** hinzu.

5 Fügen Sie nach dem Abschnitt **`<Directory "/usr/share/apache2/icons">`** Folgendes hinzu:

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

6 Fügen Sie eine Referenz in der Datei apache2.conf mit **nano /etc/apache2/apache2.conf** hinzu.

7 Fügen Sie im Abschnitt **`Apache2 HTTPD server`** Folgendes hinzu:

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

8 Starten Sie den Apache-Dienst mit **`service apache2 start`**.

Aktivieren des SCEP-Dienstes

1 Stoppen Sie den OpenXPKI-Service mit **`openxpkictl stop`**.

2 Installieren Sie das openca-tools-Paket mit **`aptitude install openca-tools`**.

3 Starten Sie den OpenXPKI-Service mit **`openxpkictl start`**.

Testen Sie den Service mit einem beliebigen Client, z. B. CertNanny mit SSCEP.

Hinweis: SSCEP ist ein Befehlszeilenclient für SCEP. Sie können SSCEP über **https://github.com/certnanny/sscop** herunterladen.

Aktivieren des Zertifikats "Unterzeichner im Auftrag" (Registrierungsagent)

Für automatische Zertifikatsanforderungen verwenden wir die "Unterzeichner im Auftrag"-Zertifikatfunktion von OpenXPKI.

1. Stoppen Sie den OpenXPKI-Dienst mit **`openxpkictl stop`**.
2. Fügen Sie in **nano /etc/openxpki/config.d/realm/ca-one/SCEP/generic.yaml** im Abschnitt **`autorisierten_signer:`** eine Regel für den Betreff-Name des Signaturgeberzertifikats hin.

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

Hinweise:

- In dieser Regel ist jeder Zertifikat-CN, der mit **`Markvision_`** beginnt, das "Unterzeichner im Auftrag"-Zertifikat.
- Der Betreff-Name wird in MVE für die Generierung des Signaturgebers im "Unterzeichner im Auftrag"-Zertifikat festgelegt.
- Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.
- Wenn der CN in MVE geändert wird, fügen Sie den aktualisierten CN in OpenXPKI hinzu.
- Sie können nur ein Zertifikat als "Unterzeichner im Auftrag" festlegen und anschließend den vollständigen CN angeben.

3. Speichern Sie die Datei.
4. Starten Sie den OpenXPKI-Service mit **`openxpkictl start`**.

Aktivieren der automatischen Genehmigung von Zertifikatsanforderungen in OpenXPKI CA

1. Stoppen Sie den OpenXPKI-Service mit **`openxpkictl stop`**.
2. Aktualisieren Sie in **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml** Folgendes: **`eligible:`** section:

Alter Inhalt

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

Neuer Inhalt

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

Hinweise:

- Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.
- Um Zertifikate manuell zu genehmigen, kennzeichnen Sie **`value: 1`** als Kommentar, und entfernen Sie das Kommentarzeichen in den anderen Zeilen, die zuvor als Kommentare gekennzeichnet waren.

3. Speichern Sie die Datei.
4. Starten Sie den OpenXPKI-Service mit **`openxpkictl start`**.

Erstellen eines zweiten Bereichs

In OpenXPKI können Sie mehrere PKI-Strukturen im selben System konfigurieren. In den folgenden Themen wird gezeigt, wie ein weiterer Bereich für MVE mit dem Namen **ca-two** erstellt wird.

Kopieren und Festlegen des Verzeichnisses

1. Kopieren Sie die Beispielverzeichnisstruktur **/etc/openxpki/config.d/realm/ca-one** in ein neues Verzeichnis (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) in dem Bereichsverzeichnis.
2. Aktualisieren Sie in **/etc/openxpki/config.d/system/realms.yaml** den folgenden Bereich:

Alter Inhalt

```
# 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/
```

Neuer Inhalt

```
# 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. Speichern Sie die Datei.

Erstellen von Zertifikaten

Die folgenden Anweisungen zeigen, wie das Signaturgeberzertifikat, das Tresorzertifikat und das SCEP-Zertifikat generiert werden. Die Root-CA signiert das Signaturgeberzertifikat, und das Signaturgeberzertifikat signiert das SCEP-Zertifikat. Das Tresorzertifikat ist selbstsigniert.

1. Generieren Sie Zertifikate, und signieren Sie sie anschließend. Weitere Informationen finden Sie unter "Manuelles Konfigurieren von OpenXPKI CA" auf Seite 105.

   Hinweis: Ändern Sie den gemeinsamen Zertifikatnamen, damit der Benutzer leicht zwischen verschiedenen Zertifikaten für verschiedene Bereiche unterscheiden kann. Sie können **DC=CA-ONE** in **DC=CA-TWO** ändern. Die Zertifikatdateien werden im Verzeichnis **/etc/certs/openxpki_ca-two/** erstellt.

2. Kopieren Sie die Schlüsseldateien nach **/etc/openxpki/ca/ca-two/**.

   Hinweis: Die Schlüsseldateien müssen von OpenXPKI gelesen werden können.

   ```
   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. Erstellen Sie den Symlink. Erstellen Sie außerdem einen Symlink für das Root-CA-Zertifikat.

   Hinweis: Symlinks sind Aliase, die von der Standardkonfiguration verwendet werden.

   ```
   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. Importieren Sie das Signaturgeberzertifikat, das Tresorzertifikat und das SCEP-Zertifikat in die Datenbank mit den entsprechenden Token für **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. Prüfen Sie mit **openxpkiadm alias --realm ca-two**, ob der Import erfolgreich war.

Beispielausgabe

```
=== 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
```

In diesem Fall sind die Root-CA-Informationen für **ca-one** und **ca-two** identisch.

6 Wenn Sie das Kennwort des Zertifikatschlüssels während der Zertifikatserstellung geändert haben, aktualisieren Sie **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.

7 Generieren Sie die CRLs für diesen Bereich. Weitere Informationen finden Sie unter "Generieren von CRL-Informationen" auf Seite 110.

8 Veröffentlichen Sie die CRLs für diesen Bereich. Weitere Informationen finden Sie unter "Konfigurieren der CRL-Zugänglichkeit" auf Seite 111.

9 Starten Sie den OpenXPKI-Dienst mit **openxpkictl restart** neu.

Beispielausgabe

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

10 Gehen Sie folgendermaßen vor, um auf den OpenXPKI-Server zuzugreifen:

a Geben Sie in einem Webbrowser **http://ipaddress/openxpki/** ein.

b Melden Sie sich als **Bediener** an. Das Standardkennwort lautet **openxpki**.

Hinweis: Die Bedieneranmeldung hat zwei vorkonfigurierte Bedienerkonten, **raop** und **raop2**.

Konfigurieren des SCEP-Endpunkts für mehrere Bereiche

Der SCEP-Endpunkt der Standardbereichs ist **http://<ipaddress>/scep/scep**. Wenn Sie mehrere Bereiche haben, konfigurieren Sie einen eindeutigen SCEP-Endpunkt (andere Konfigurationsdatei) für jeden Bereich. In den folgenden Anweisungen verwenden wir zwei PKI-Bereiche: **ca-one** und **ca-two**.

1 Kopieren Sie die Standardkonfigurationsdatei in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

Hinweis: Benennen Sie die Datei als **ca-one.conf**.

2 Ändern Sie in **nano /etc/openxpki/scep/ca-one.conf** den Bereichswert in **realm=ca-one**.

3 Erstellen Sie eine weitere Konfigurationsdatei in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

Hinweis: Benennen Sie die Datei als **ca-two.conf**.

4 Ändern Sie in **nano /etc/openxpki/scep/ca-two.conf** den Bereichswert in **realm=ca-two**.

5 Starten Sie den OpenXPKI-Dienst mit **openxpkictl restart** neu.

Die SCEP-Endpunkte sind die folgenden:

- **`ca-one`** – **http://ipaddress/scep/ca-one**
- **`ca-two`** – **http://ipaddress/scep/ca-two**

Wenn Sie zwischen Anmeldeinformationen und Standardzertifikatvorlagen für verschiedene PKI-Bereiche unterscheiden möchten, benötigen Sie möglicherweise eine erweiterte Konfiguration.

Gleichzeitiges aktivieren mehrerer aktiver Zertifikate mit demselben Betreff

Standardmäßig kann in OpenXPKI nur ein Zertifikat mit demselben Betreff-Namen gleichzeitig aktiv sein. Wenn Sie jedoch mehrere benannte Zertifikate durchsetzen, müssen mehrere aktive Zertifikate mit demselben Betreff-Namen gleichzeitig vorhanden sein.

1. Ändern Sie in **/etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml** im Abschnitt **`policy`** den Wert für **`max_active_certs`** von **`1`** in **`0`**.

   Hinweise:

   - REALM NAME ist der Name des Bereichs. Zum Beispiel: **ca-one**.
   - Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.
2. Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Festlegen der Standard-Anschlussnummer für OpenXPKI CA

Standardmäßig hört Apache auf Anschlussnummer 80. Legen Sie die Standard-Anschlussnummer für OpenXPKI CA fest, um Konflikte zu vermeiden.

1. Fügen Sie in **/etc/apache2/ports.conf** einen Anschluss hinzu, oder ändern Sie ihn. Zum Beispiel **`Listen 8080`**.
2. Fügen Sie in **/etc/apache2/sites-enabled/000-default.conf** den Abschnitt **`VirtualHost`** hinzu, oder ändern Sie ihn, um einen neuen Anschluss zuzuordnen. Zum Beispiel: **`<VirtualHost *:8080>`**.
3. Starten Sie den Apache-Server mit **`systemctl restart apache2`** neu.

Um den Status zu prüfen, führen Sie **`netstat -tlpn| grep apache`** aus. Die OpenXPKI SCEP-URL lautet jetzt **http://ipaddress:8080/scep/ca-one**, und die Web-URL lautet **http://ip address:8080/openxpki**.

Ablehnen von Zertifikatsanforderungen ohne Kennwortabfrage in OpenXPKI CA

Standardmäßig akzeptiert OpenXPKI Anforderungen, ohne das Kennwort abzufragen. Die Zertifikatsanforderung wird nicht abgelehnt, und die CA und der CA-Administrator bestimmen, ob die Anforderung genehmigt oder abgelehnt werden soll. Um potenzielle Sicherheitsprobleme zu vermeiden, deaktivieren Sie diese Funktion, damit Zertifikatsanforderungen, die ungültige Kennwörter enthalten, sofort abgelehnt werden. In MVE ist Kennwort abfragen nur erforderlich, wenn das Registrierungsagent-Zertifikat generiert wird.

1. Ändern Sie in **etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml** im Abschnitt **`policy`** den Wert für **`allow_man_authen`** von **`1`** in **`0`**.

Hinweise:

- REALM NAME ist der Name des Bereichs. Zum Beispiel: **ca-one**.
- Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.

2 Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Hinzufügen der Clientauthentifizierungs-EKU zu Zertifikaten

1 Ändern Sie in **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml** im Bereich **`extended_key_usage:`** den Wert für **`client_auth:`** in **1**.

Hinweise:

- REALM NAME ist der Name des Bereichs. Zum Beispiel: **ca-one**.
- Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.

2 Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Abrufen des vollständigen Zertifikatsbetreffs bei Anforderung über SCEP

Standardmäßig liest OpenXPKI nur den CN des Betreffs des anfragenden Zertifikats. Die restlichen Informationen, wie Land, Ort und DC, sind hartcodiert. Wenn ein Zertifikat beispielsweise **`C=US`**, **`ST=KY`**, **`L=Lexington`**, **`O=Lexmark`**, **`OU=ISS`**, **`CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`** ist, dann wird der Betreff nach dem Signieren des Zertifikats durch SCEP in **`DC=Test Deployment`**, **`DC= OpenXPKI`**, **`CN=ET0021B7C34AEC.dhcp.dev.lexmark.com`** geändert.

Hinweis: REALM NAME ist der Name des Bereichs. Zum Beispiel: **ca-one**.

1 Ändern Sie in **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml** im Bereich **`enroll`** den Wert für **`dn`** wie folgt:

```
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 Speichern Sie die Datei.

3 Erstellen Sie eine Datei mit dem Namen **l.yaml** im Verzeichnis **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

4 Fügen Sie Folgendes hinzu:

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

5 Speichern Sie die Datei.

6 Erstellen Sie eine Datei mit dem Namen **st.yaml** im Verzeichnis **/etc/openxpki/config.d/realm/REALM NAME/profile/template**.

7 Fügen Sie Folgendes hinzu:

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

8 Speichern Sie die Datei.

Hinweis: OpenXPKI muss Eigentümer beider Dateien und lesbar, schreibbar und ausführbar sein.

9 Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Entziehen von Zertifikaten und Veröffentlichen von CRL

1 Greifen Sie auf den OpenXPKI-Server zu.

   a Geben Sie in einem Webbrowser **`http://ipaddress/openxpki/`** ein.

   b Melden Sie sich als **Bediener** an. Das Standardkennwort lautet **`openxpki`**.

   Hinweis: Die Bedieneranmeldung hat zwei vorkonfigurierte Bedienerkonten, **raop** und **raop2**.

2 Klicken Sie auf **Workflow-Suche** > **Jetzt suchen**.

3 Klicken Sie auf ein Zertifikat, das Sie widerrufen möchten, und klicken Sie anschließend auf den Zertifikatlink.

4 Klicken Sie im Bereich Aktion auf **Widerrufsanforderung**.

5 Geben Sie die entsprechenden Werte ein, und klicken Sie anschließend auf **Fortfahren** > **Anfrage abschicken**.

6 Genehmigen Sie die Anfrage auf der nächsten Seite. Der Zertifikatswiderruf wartet auf die nächste CRL-Veröffentlichung.

7 Klicken Sie im Abschnitt PKI-Operation auf **Zertifikatwiderrufsliste (CRL) ausstellen**.

8 Klicken Sie auf **Erstellung der Widerruflisten Zertifikatsvorlage** > **Fortfahren**.

9 Klicken Sie im Abschnitt PKI-Operation auf **CA/CRL veröffentlichen**.

10 Klicken Sie auf **Workflow-Suche** > **Jetzt suchen**.

11 Klicken Sie auf das widerrufene Zertifikat mit dem Typ **certificate_revocation_request_v2**.

12 Klicken Sie auf **Aktivierung erzwingen**.

In der neuen CRL finden Sie die Seriennummer und den Widerrufsgrund des widerrufenen Zertifikats.

Verwalten von Zertifikaten mit OpenXPKI Certificate Authority über EST

Dieser Abschnitt hilft dem Benutzer bei der Konfiguration von OpenXPKI CA Version 3.x.x mit dem EST-Protokoll.

Hinweise:

- Stellen Sie sicher, dass Sie das Betriebssystem Debian 10 Buster verwenden.
- Weitere Informationen zu OpenXPKI erhalten Sie unter **www.openxpki.org**.

Konfigurieren von OpenXPKI CA

Installieren von OpenXPKI CA

1. Verbinden Sie den Computer mit PuTTY oder einem anderen Client.
2. Führen Sie auf dem Client den Befehl **`sudo su -`** aus, um zum Root-Benutzer zu gelangen.
3. Geben Sie das Root-Kennwort ein.
4. Ändern Sie in **nano /etc/apt/sources.list** die Quelle zum Installieren der Updates.
5. Aktualisieren Sie die Datei. Beispiel:

```
#

# 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. Speichern Sie die Datei.
7. Führen Sie die folgenden Befehle aus:
   - **`apt-get Update`**
   - **`apt-get Upgrade`**
8. Aktualisieren Sie die CA-Zertifikatlisten auf dem Server mit **`apt-get install ca-certificates`**.
9. Installieren Sie **en_US.utf8 locale** mit **`dpkg-reconfigure locales`**.
10. Wählen Sie das Gebietsschema **en_US.UTF-8 UTF-8** aus, und machen Sie es anschließend zum standardmäßigen Gebietsschema für das System.

    Hinweis: Verwenden Sie die Tabulatortaste und die Leertaste zum Auswählen und Navigieren im Menü.

11 Prüfen Sie die Gebietsschemas, die Sie mit **`locale -a`** generiert haben.

Beispielausgabe

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

12 Kopieren Sie den Fingerabdruck des OpenXPKI-Pakets mit **`nano /home/Release.key`**. Kopieren Sie den Schlüssel beispielsweise in **/home**.

13 Geben Sie **`55D89776 006F632B E0196E3E D2495509 BAFDDC74 22FEAAD2 F055074E 0FE3A724`** als Wert ein.

14 Führen Sie den folgenden Befehl aus:

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

15 Fügen Sie das Paket mit dem Befehl **`wget https://packages.openxpki.org/v3/debian/Release.key -O - | apt-key add -`** hinzu.

16 Fügen Sie das Repository mit **`echo "deb http://packages.openxpki.org/v3/debian/ buster release" > /etc/apt/sources.list.d/openxpki.list`** und anschließend **`apt update`** zu Ihrer Quellenliste (buster) hinzu.

17 Installieren Sie MySQL und Perl MySQL-Binding mit **`apt install mariadb-server libdbd-mariadb-perl`**.

18 Installieren Sie apache2.2-common mit **`apt install apache2`**.

19 Installieren Sie in **nano /etc/apt/sources.list** das fastcgi-Modul, um die Benutzeroberfläche zu beschleunigen.

Hinweis: Wir empfehlen die Verwendung von **`mod_fcgid`**.

20 Fügen Sie die Zeile **`deb http://http.us.debian.org/debian/buster main`** in der Datei hinzu und speichern Sie sie.

21 Führen Sie die folgenden Befehle aus:

```
apt-get Update
apt install libapache2-mod-fcgid
```

22 Aktivieren Sie das fastcgi-Modul mit **`a2enmod fcgid`**.

23 Installieren Sie das OpenXPKI-Kernpaket mit **`apt install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n`**.

24 Starten Sie den Apache Server mit **`service apache2 restart`** neu.

25 Prüfen Sie mit **`openxpkiadm version`**, ob die Installation erfolgreich war.

Hinweis: Wenn die Installation erfolgreich war, zeigt das System die Version der installierten OpenXPKI an. Beispiel: **Version (core): 3.18.2**.

26 Erstellen Sie die leere Datenbank, und weisen Sie anschließend den Datenbankbenutzer mit **`mariadb -u root -p`** zu.

Hinweise:

- Dieser Befehl muss in den Client eingegeben werden. Andernfalls können Sie das Kennwort nicht eingeben.
- Geben Sie das Passwort für MySQL ein. In diesem Beispiel ist **root** der MySQL-Benutzer.
- **openxpki** ist der Benutzer, auf dem OpenXPKI installiert ist.

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

Wenn der MySQL-Service nicht läuft, führen Sie **/etc/init.d/mysql start** aus, um den Service zu starten.

27 Geben Sie **quit** ein, um MySQL zu beenden.

28 Speichern Sie die verwendeten Zugangsdaten in **/etc/openxpki/config.d/system/database.yaml**.

Beispielhafter Datei-Inhalt

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

Hinweis: Ändern Sie **user** und **passwd** so, dass sie mit dem MariaDB-Benutzernamen und -Kennwort übereinstimmen.

29 Speichern Sie die Datei.

30 Führen Sie für ein leeres Datenbankschema **zcat /usr/share/doc/libopenxpki-perl/examples/schema-mariadb.sql.gz | \ mysql -u root --password --database openxpki** aus der bereitgestellten Schemadatei aus.

31 Geben Sie das Kennwort für die Datenbank ein.

Konfigurieren von OpenXPKI CA mit Standardskript

Hinweis: Das Standardskript konfiguriert nur den Standardbereich **ca-one**. CDP und CRLs sind nicht konfiguriert.

1 Führen Sie das Skript mit **bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh** aus.

2 Bestätigen Sie die Installation mit **openxpkiadm alias --realm democa**.

Beispielausgabe

```
=== 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 Prüfen Sie mit **`openxpkictl start`**, ob die Installation erfolgreich war.

Beispielausgabe

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

4 Gehen Sie folgendermaßen vor, um auf den OpenXPKI-Server zuzugreifen:

a Geben Sie in einem Webbrowser **`http://ipaddress/openxpki/`** ein.

b Fügen Sie den Benutzernamen und die entsprechenden Kennwörter in einer **`userdb.yaml`**-Datei hinzu. Gehen Sie wie folgt vor, um den Benutzernamen und das Kennwort hinzuzufügen:

- Checken Sie aus zu **/home/pkiadm** und dann **nano userdb.yaml**.
- Fügen Sie Folgendes ein:

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

Hinweis: In diesem Fall bezieht sich estRA auf den Benutzernamen. Geben Sie **`openxpkiadm hashpwd`** ein, um das Kennwort zu generieren. Wenn eine Meldung angezeigt wird, in der nach dem Kennwort und einem verschlüsselten ssha256-Kennwort gefragt wird, kopieren Sie es und fügen Sie es in den Digest eines beliebigen Benutzers ein.

Hinweis: Die verfügbaren Rollen in der Bedieneranmeldung sind „RA-Bediener“, „CA-Bediener“ und „Benutzer“.

5 Geben Sie den Benutzernamen und das Kennwort ein.

6 Erstellen Sie eine Zertifikatsanforderung, und testen Sie sie.

Manuelles Konfigurieren von OpenXPKI CA

Übersicht

Hinweis: Stellen Sie zu Beginn sicher, dass Sie über die grundlegenden Kenntnisse für das Erstellen von OpenSSL-Zertifikaten verfügen.

Erstellen Sie zum manuellen Konfigurieren der OpenXPKI CA Folgendes:

1. Root-CA-Zertifikat Weitere Informationen finden Sie unter "Erstellen eines Root-CA-Zertifikats" auf Seite 107.
2. CA-Signaturgeberzertifikat, signiert von der Root-CA. Weitere Informationen finden Sie unter "Erstellen eines Signaturgeberzertifikats" auf Seite 107.
3. Datentresorzertifikat, selbstsigniert. Weitere Informationen finden Sie unter "Erstellen eines Tresorzertifikats" auf Seite 107.
4. Web-Zertifikat, vom Signaturgeberzertifikat signiert. Weitere Informationen finden Sie unter "Einrichten des Webservers" auf Seite 126.

Hinweise:

- Verwenden Sie bei der Auswahl des Signatur-Hash entweder SHA256 oder SHA512.
- Die Änderung der Größe des öffentlichen Schlüssels ist optional.

Ab Version 3.10 können Sie die Schlüssel direkt mit dem Befehl openxpkiadm alias verwalten:

- Führen Sie **mkdir -p /etc/openxpki/local/keys** aus, um das Verzeichnis zu erstellen. Der Standardspeicherort des Verzeichnisses ist **/etc/openxpki/local/keys**.
- Führen Sie **openxpkictl start** aus, um den Server zu starten.

In diesem Fall verwenden wir das Verzeichnis **/etc/certs/openxpki_democa/** zur Zertifikatgenerierung. Sie können jedoch jedes beliebige Verzeichnis verwenden.

Erstellen einer OpenSSL-Konfigurationsdatei

Die OpenSSL-Konfigurationsdatei enthält X.509-Erweiterungen zum Generieren und Signieren von Zertifikatsanforderungen.

1. Führen Sie den folgenden Befehl aus:

   nano /etc/certs/openxpki_democa/openssl.conf

   Hinweis: Wenn Ihr Server unter Verwendung des FQDN (Fully Qualified Domain Name) erreichbar ist, verwenden Sie den DNS des Servers anstelle seiner IP-Adresse.

Beispieldatei

```
# 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 Ersetzen Sie die IP-Adresse und den CA-Zertifikatnamen mit den Setup-Informationen.

3 Speichern Sie die Datei.

Erstellen einer Kennwortdatei für Zertifikatschlüssel

1 Führen Sie den folgenden Befehl aus:

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

2 Geben Sie Ihr Kennwort ein.

3 Speichern Sie die Datei.

Erstellen eines Root-CA-Zertifikats

Sie können ein selbstsigniertes Root-CA-Zertifikat erstellen oder eine Zertifikatsanforderung generieren und diese anschließend von der Root-CA signieren lassen.

Hinweis: Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

1. Führen Sie den folgenden Befehl aus:

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

2. Ersetzen Sie den Betreff in der Anforderung durch Ihre CA-Informationen mit **openssl req -new -key /etc/certs/openxpki_democa/ca-root-1.key -out /etc/certs/openxpki_democa/ca-root-1.csr**.

3. Rufen Sie das von der Root-CA signierte Zertifikat mit **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** auf.

4. Gehen Sie zu **/etc/certs/openxpki_democa/**, wo **ca-root-1.crt** gespeichert ist.

5. Führen Sie den folgenden Befehl aus:

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

Erstellen eines Signaturgeberzertifikats

Hinweis: Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

1. Führen Sie den folgenden Befehl aus:

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

2. Ersetzen Sie den Betreff in der Anforderung mit Ihren CA-Informationen mit **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. Rufen Sie das von der Root-CA signierte Zertifikat mit **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** ab.

4. Führen Sie den folgenden Befehl aus:

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

Erstellen eines Tresorzertifikats

Hinweise:

- Das Tresorzertifikat ist selbstsigniert.
- Ersetzen Sie die Schlüssellänge, den Signaturalgorithmus und den Zertifikatnamen durch die entsprechenden Werte.

1. Führen Sie den folgenden Befehl aus:

   ```
   openssl req -new -x509 -keyout vault.key -out vault.crt -days 1100 -
   config /etc/certs/openxpki_democa/openssl.conf
   ```

2. Ändern Sie den Betreff in der Anforderung mit Ihren CA-Informationen mit **`openxpkiadm certificate import --file vault.crt`**.

3. Führen Sie den folgenden Befehl aus:

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

   Hinweis: Geben Sie die erforderlichen Werte an, behalten Sie **`/CN=DataVault`** als Betreff bei.

Erstellen eines Webzertifikats

1. Führen Sie den folgenden Befehl aus:

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

2. Ersetzen Sie den Betreff in der Anforderung mit Ihren CA-Informationen mit **`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. Führen Sie den folgenden Befehl aus:

   ```
   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
   ```

Einrichten des Webservers

1. Führen Sie die folgenden Befehle aus:

   ```
   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 Starten Sie den Apache-Dienst mit **apache2 restart** neu.

3 Führen Sie den folgenden Befehl aus, um den erfolgreichen Import der Dateien zu prüfen:

```
openxpkiadm alias --realm democa
```

Beispielausgabe

```
=== 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
```

Verfügbar machen des Kennworts des Zertifikatschlüssels für OpenXPKI

1 Ändern Sie den Wert in der Datei **nano /etc/openxpki/config.d/system/crypto.yaml**.

2 Kommentare für Cache aufheben: **Daemon unter secret: Standard**:

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

Starten von OpenXPKI

1 Führen Sie den Befehl **openxpkictl start** aus.

Beispielausgabe

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

2 Greifen Sie auf den OpenXPKI-Server zu:

a Geben Sie in einem Webbrowser **http://ipaddress/openxpki/** ein.

b Fügen Sie die Benutzernamen und entsprechenden Kennwörter in einer **userdb.yaml**-Datei hinzu:

- Checken Sie aus zu **/home/pkiadm** und dann zu **nano userdb.yaml**.
- Fügen Sie Folgendes ein:

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

Hinweis: Hier verweist estRA auf den Benutzernamen.

- Geben Sie **openxpkiadm hashpwd** ein, um das Kennwort zu generieren. Eine Meldung mit dem Kennwort und einem verschlüsselten ssha256-Kennwort wird angezeigt.
- Kopieren Sie das Kennwort und fügen Sie es dann in den Digest eines beliebigen Benutzers ein.

Hinweis: Die Bedieneranmeldung verfügt über zwei vorkonfigurierte Rollen: RA-Bediener, CA-Bediener und Benutzer.

3 Geben Sie den Benutzernamen und das Kennwort ein.

4 Erstellen Sie eine Zertifikatsanforderung, und testen Sie sie.

Generieren von CRL-Informationen

Hinweis: Wenn Ihr Server über FQDN erreichbar ist, verwenden Sie den DNS des Servers anstelle seiner IP-Adresse.

1 Stoppen Sie den OpenXPKI-Service mit **openxpkictl stop**.

2 Aktualisieren Sie in **nano /etc/openxpki/config.d/realm/democa/publishing.yaml** den Abschnitt **connectors: cdp** wie folgt:

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

a Aktualisieren Sie in **nano /etc/openxpki/config.d/realm/democa/profile/default.yaml** Folgendes:

- **crl_distribution_points:** section

```
critical: 0
uri:
    - https://FQDN of the est/openxkpi/CenrtEnroll/[% ISSUER.CN.0 %].crl
    - ldap://localhost/[% ISSUER.DN %]
```

- **authority_info_access:** section

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

Ändern Sie die IP-Adresse und den CA-Zertifikatnamen entsprechend Ihrem CA-Server.

Hinweis: Der Pfad Authority_Info_Access (AIA) wird im Download -Ordner gespeichert. Sie können den Speicherort jedoch nach Ihren Wünschen festlegen.

b Gehen Sie in **nano /etc/openxpki/config.d/realm/democa/crl/default.yaml** wie folgt vor:

- Aktualisieren Sie ggf. **nextupdate** und **renewal**.
- Fügen Sie **ca_issuers** zum folgenden Abschnitt hinzu:

```
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/
```

Ändern Sie die IP-Adresse und den CA-Zertifikatnamen entsprechend Ihrem CA-Server.

3 Starten Sie den OpenXPKI-Service mit **openxpkictl start**.

Veröffentlichen von CRL-Informationen

Nach dem Erstellen der CRLs müssen Sie diese veröffentlichen, damit alle darauf zugreifen können.

1 Beenden Sie den Apache-Dienst mit **service apache2 stop**.

2 Erstellen Sie ein Verzeichnis **CertEnroll** für CRL im Verzeichnis **/var/www/openxpki/**.

3 Legen Sie **openxpki** als Eigentümer dieses Verzeichnisses fest, und konfigurieren Sie anschließend die Berechtigungen für das Lesen und Ausführen von Apache sowie für andere Dienste als schreibgeschützt.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Fügen Sie eine Referenz zur Apache-Datei alias.conf mit **nano /etc/apache2/mods-enabled/alias.conf** hinzu.

5 Fügen Sie nach dem Abschnitt **<Directory "/usr/share/apache2/icons">** Folgendes hinzu:

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

6 Fügen Sie eine Referenz in der Datei apache2.conf mit **nano /etc/apache2/apache2.conf** hinzu.

7 Fügen Sie im Abschnitt **Apache2 HTTPD server** Folgendes hinzu:

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

8 Starten Sie den Apache-Dienst mit **service apache2 start**.

Aktivieren der automatischen Genehmigung von Zertifikatsanforderungen in OpenXPKI CA

1. Stoppen Sie den OpenXPKI-Service mit **`openxpkictl stop`**.
2. Aktualisieren Sie in **/etc/openxpki/config.d/realm/democa/est/default.yaml** die **`Berechtigung:`** section:

Alter Inhalt

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

Neuer Inhalt

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

Hinweise:

- Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.
- Um Zertifikate manuell zu genehmigen, kennzeichnen Sie **`value: 1`** als Kommentar, und entfernen Sie das Kommentarzeichen in den anderen Zeilen, die zuvor als Kommentare gekennzeichnet waren.

3. Speichern Sie die Datei.
4. Starten Sie den OpenXPKI-Service mit **`openxpkictl start`**.

Ändern von Details, um ca-cert-Download zu aktivieren

1. Führen Sie den folgenden Befehl aus:

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

2. Ersetzen Sie **`my $mime = "application/pkcs7-mime; smime-type=certs-only";`** mit **`my $mime = "application/pkcs7-mime";`**.
3. Starten Sie den OpenXPKI-Service mit **`openxpkictl`**.

Erstellen eines zweiten Bereichs

In OpenXPKI können Sie mehrere PKI-Strukturen im selben System konfigurieren. In den folgenden Themen wird gezeigt, wie ein weiterer Bereich für MVE mit dem Namen **democa-two** erstellt wird.

Kopieren und Festlegen des Verzeichnisses

1. Erstellen Sie ein Verzeichnis, nämlich **democa2**, für den zweiten Bereich in **/etc/openxpki/config.d/realm**.
2. Kopieren Sie die Beispielverzeichnisstruktur **/etc/openxpki/config.d/realm/ca-one** in ein neues Verzeichnis (**cp -r /etc/openxpki/config.d/realm.tpl/*/etc/openxpki/config.d/realm/democa2**) in dem Bereichsverzeichnis.
3. Aktualisieren Sie in **/etc/openxpki/config.d/system/realms.yaml** den folgenden Bereich:

Alter Inhalt

```
# 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/
```

Neuer Inhalt

```
# 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. Speichern Sie die Datei.

Konfigurieren des EST-Endpunkts für mehrere Bereiche

Sie können den EST-Endpunkt mit einem Tupel konfigurieren, das aus dem Berechtigungsteil der URI und der optionalen Beschriftung besteht (z. B. www.example.com:80 und arbitraryLabel1). In den folgenden Anweisungen verwenden wir zwei PKI-Bereiche: **`democa`** und **`democa2`**.

1. Kopieren Sie die Standardkonfigurationsdatei in **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa.conf**.

   Hinweis: Benennen Sie die Datei **`democa.conf`**.

2. Ändern Sie in **nano /etc/openxpki/est/democa.conf** den Bereichswert zu **`realm=democa`**.

   Hinweis: Je nach Ihren Anforderungen müssen Sie möglicherweise die entsprechenden Zeilen für die Abschnitte **simpleenroll**, **simplereenroll**, **csrattrs** und **cacerts** aufheben. Lassen Sie die Umgebungsabschnitte kommentiert. Führen Sie den gleichen Vorgang für **default.conf** aus.

3 Erstellen Sie eine weitere Konfigurationsdatei in **cp /etc/openxpki/est/default.conf /etc/openxpki/est/democa2.conf**.

Hinweis: Benennen Sie die Datei **`democa2.conf`**.

4 Ändern Sie in **nano /etc/openxpki/est/democa2.conf** den Bereichswert zu **`realm=democa2`**

Hinweis: Je nach Ihren Anforderungen müssen Sie möglicherweise die entsprechenden Zeilen für die Abschnitte **simpleenroll**, **simplereenroll**, **csrattrs** und **cacerts** aufheben. Lassen Sie die Umgebungsabschnitte kommentiert.

5 Kopieren Sie die Datei **default.yaml** in die folgenden Speicherorte:

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

Hinweis: Benennen Sie die Datei **`democa.yaml`**.

6 Kopieren Sie die Datei **default.yaml** in die folgenden Speicherorte:

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

Hinweis: Benennen Sie die Datei **`democa2.yaml`**.

7 Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Wählen Sie die folgenden URLs aus, um den EST-Server zu öffnen, der einem Bereich über einen Webbrowser entspricht:

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

Wenn Sie zwischen Anmeldeinformationen und Standardzertifikatvorlagen für verschiedene PKI-Bereiche unterscheiden möchten, benötigen Sie möglicherweise eine erweiterte Konfiguration.

Erstellen eines Signaturgeberzertifikats

Die folgenden Anweisungen zeigen, wie ein Signaturgeberzertifikat im zweiten Bereich generiert wird. Sie können dieselben Stamm- und Tresorzertifikate wie im ersten Bereich verwenden.

1 Erstellen Sie eine OpenSSL-Konfigurationsdatei in **nano /etc/certs/openxpki_democa2/openssl.conf**.

Hinweis: Ändern Sie den gemeinsamen Zertifikatnamen, damit der Benutzer leicht zwischen verschiedenen Zertifikaten für verschiedene Bereiche unterscheiden kann. Die Zertifikatdateien werden im Verzeichnis **/etc/certs/openxpki_democa2/** erstellt.

2 Wechseln Sie zum Verzeichnis des Tresorzertifikats im ersten Bereich und importieren Sie das Zertifikat aus dem ersten Bereich.

3 Führen Sie den folgenden Code aus:

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

Erstellen einer Kennwortdatei für Zertifikatschlüssel

1 Führen Sie den folgenden Befehl aus:

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

2 Geben Sie Ihr Kennwort ein.

3. Erstellen Sie ein Signaturgeberzertifikat. Weitere Informationen finden Sie unter "Erstellen eines Signaturgeberzertifikats" auf Seite 107.
4. Prüfen Sie mit **openxpkiadm alias --realm democa2**, ob der Import erfolgreich war.

   Hinweis: Wenn Sie das Schlüsselkennwort des Zertifikats während der Zertifikatserstellung geändert haben, aktualisieren Sie **nano /etc/openxpki/config.d/realm/democa2/crypto.yaml**.
5. Generieren Sie die CRLs für den zweiten Bereich. Weitere Informationen finden Sie unter "Generieren von CRL-Informationen" auf Seite 110.

   Hinweis: Stellen Sie sicher, dass Sie den richtigen CA-Zertifikatsnamen entsprechend des Bereichs verwenden.
6. Veröffentlichen Sie die CRLs für diesen Bereich. Weitere Informationen finden Sie unter "Veröffentlichen von CRL-Informationen" auf Seite 129.
7. Starten Sie den OpenXPKI-Dienst mit **openxpkictl restart** neu.

Beispielausgabe

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

Gleichzeitiges Aktivieren mehrerer aktiver Zertifikate mit demselben Betreff

Standardmäßig kann in OpenXPKI nur ein Zertifikat mit demselben Betreff-Namen gleichzeitig aktiv sein. Wenn Sie jedoch mehrere benannte Zertifikate durchsetzen, müssen mehrere aktive Zertifikate mit demselben Betreff-Namen gleichzeitig vorhanden sein.

1. Ändern Sie in **/etc/openxpki/config.d/realm/REALM NAME/est/< REALM NAME >.yaml** im Abschnitt **`Richtlinie`** den Wert für **`max_active_certs`** von **1** zu **0**.

   Hinweise:

   - REALM NAME ist der Name des Bereichs. Zum Beispiel: **ca-one**.
   - Überprüfen Sie den Abstand und den Einzug in der Skriptdatei.
2. Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

Festlegen der Standard-Anschlussnummer für OpenXPKI CA

Standardmäßig hört Apache für https auf Anschlussnummer 443. Legen Sie die Standard-Anschlussnummer für OpenXPKI CA fest, um Konflikte zu vermeiden.

1. Ändern Sie in **/etc/apache2/Ports.conf** den 443-Anschluss zu einem anderen Anschluss. Beispiel:

Alter Inhalt

```
Listen 80

<IfModule ssl_module>
   Listen 443
</IfModule>

<IfModule mod_gnutls.c>
```

```
  Listen 443
</IfModule>
```

Neuer Inhalt

```
Listen 80

<IfModule ssl_module>
   Listen 9443
</IfModule>

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

2. Fügen Sie in **/etc/apache2/sites-available/openxpki.conf** den Abschnitt **`VirtualHost`** hinzu, oder ändern Sie ihn, um einen neuen Anschluss zuzuordnen. Zum Beispiel: **`<VirtualHost *:443>`** zu **`<VirtualHost *:9443>`**.
3. Fügen Sie in **/etc/apache2/sites-available/default-ssl.conf** **`VirtualHost`** hinzu, oder ändern Sie ihn, um einen neuen Anschluss zuzuordnen. Zum Beispiel:**`<VirtualHost *:443>`** zu **`<VirtualHost *: 9443>`**.
4. Starten Sie den Apache-Server mit **`systemctl restart apache2`** neu.

   Hinweis: Wenn Sie nach der **SSL-/TLS** -Passphrase gefragt werden, geben Sie das Kennwort ein, während Sie das TLS-Webserverzertifikat im EST-Server hinzufügen.
5. Geben Sie in **tinddopenxpkiweb01.dhcp.dev.lexmark.com:9443 (RSA):**die Passphrase für die **SSL-/TLS** -Schlüssel ein.

Um den Status zu prüfen, führen Sie **`netstat -tlpn| grep apache`** aus. Die OpenXPKI SCEP-URL lautet jetzt **https://ipaddress** und die Web-URL ist **FQDN:9443/openxpki**.

Aktivieren der Standardauthentifizierung

1. Führen Sie den folgenden Befehl aus:

   `apt -y install apache2-utils`
2. Erstellen Sie ein Benutzerkonto, das Zugriff auf den Server hat. Geben Sie folgende Informationen ein:

   ```
   htpasswd -c /etc/apache2/.htpasswd <username>
                  New password:
                  Re-type new password:
                  Adding password for user <username>
   ```
3. Gehen Sie zum Verzeichnis **`cd /etc/apache2/sites-enabled/`**.
4. Fügen Sie in **nano openxpki.conf** die folgenden Zeilen in **`<VirtualHost *: 443 block>`** ein:

   ```
   #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 Add **`ErrorDocument 401 %{unescape:%00}`** vor **SSLEngine** im selben virtuellen Hostblock.

Beispiel

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

6 Starten Sie den Apache-Dienst **apache2 service** mit **service apache2 restart** neu.

Hinweis: Die Standardauthentifizierung funktioniert mit dem oben genannten Benutzernamen und Kennwort.

Aktivieren der Clientzertifikat-Authentifizierung

1 Rufen Sie das folgende Verzeichnis auf: **`cd /etc/apache2/sites-enabled/`**.

2 Für den erforderlichen Host in **nano openxpki.conf** muss **SSLVerifyClient require** hinzugefügt werden.

Wenn Sie beispielsweise Port 443 verwenden, ändern Sie den Abschnitt **VirtualHost** wie folgt:

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

3 Entfernen Sie den Befehl **SSLVerifyClient optional_no_ca**.

4 Speichern Sie die Datei und geben Sie dann **`quit`** ein, um MySQL zu beenden.

5 Rufen Sie das folgende Verzeichnis auf: **`cd /etc/openxpki/config.d/realm/democa/est`**.

6 Öffnen Sie **default.yaml** und **democa.yaml**.

Hinweis: Wenn die Bezeichnung anders ist, ändern Sie die YAML-Datei.

7 Führen Sie den folgenden Befehl aus:

```
vi default.yaml
```

8 Fügen Sie im Abschnitt **authorized_signer** Folgendes hinzu:

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

Wenn der Betreff-Name des Clientzertifikats **test123** lautet, fügen Sie Folgendes im Abschnitt **`authorized_signer`** hinzu:

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

9 Speichern Sie die Datei und geben Sie **`quit`** ein, um MySQL zu verlassen.

10 Starten Sie den OpenXPKI-Dienst mit **`openxpkictl restart`** neu.

11 Starten Sie den Apache-Dienst mit **`service apache2 restart`** neu.

Wodurch wird der SAN-Unterschied verursacht, der verhindert, dass das System die CRL abruft?

Der SAN-Unterschied kann auftreten, wenn Sie die CRL-Informationen aktivieren. Dieser Fehler weist darauf hin, dass die IP oder der Hostname nicht mit dem Wert des SAN im Webzertifikat übereinstimmt. Um diesen Fehler zu vermeiden, verwenden Sie den FQDN im Pfad der CRL anstelle der IP. Sie können auch das Webzertifikat konfigurieren und den FQDN Ihres Systems im Feld SAN verwenden.

Warum sind die Token ca-signer-1 und vault-1 offline?

Wenn die Seite Systemstatus anzeigt, dass die Token ca-signer-1 und vault-1 offline sind, führen Sie folgende Schritte aus:

1. Ändern Sie den Schlüsselwert in **/etc/openxpki/config.d/realm/realm name/crypto.yaml**.
2. Starten Sie den OpenXPKI-Dienst neu.

Verwalten von Druckerwarnungen

Übersicht

Alarme werden ausgelöst, wenn beim Drucker ein Benutzereingriff erforderlich ist. Mithilfe von Aktionen können Sie benutzerdefinierte E-Mail-Nachrichten versenden oder Skripten ausführen, wenn eine Warnung auftritt. Ereignisse legen fest, welche Aktionen ausgeführt werden, wenn bestimmte Alarme aktiv sind. Zur Registrierung für Warnungen von einem Drucker müssen Sie Aktionen erstellen und diese anschließend einem Ereignis zuweisen. Weisen Sie das Ereignis den Druckern zu, die überwacht werden sollen.

Hinweis: Diese Funktion trifft nicht auf gesicherte Drucker zu.

Erstellen einer Aktion

Bei einer Aktion handelt es sich entweder um eine E-Mail-Benachrichtigung oder um ein Ereignisanzeigeprotokoll. Einem Ereignis zugewiesene Aktionen werden ausgelöst, wenn eine Druckerwarnung auftritt.

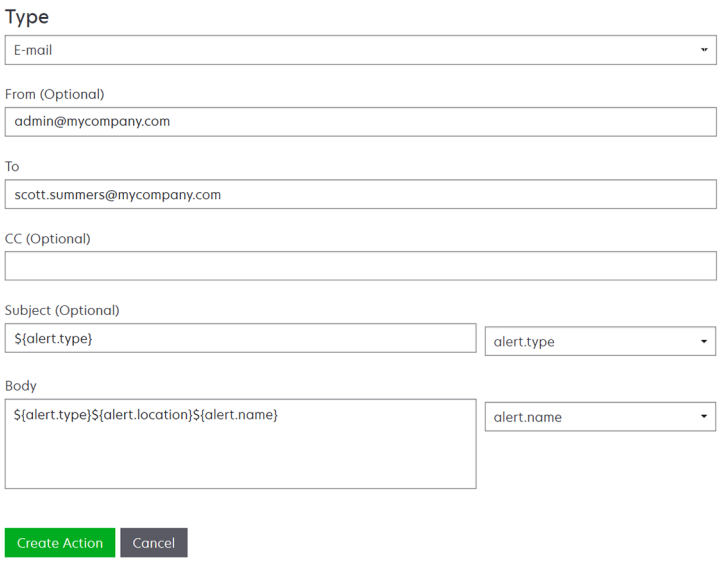
1. Klicken Sie im Menü Drucker auf **Ereignisse & Aktionen** > **Aktionen** > **Erstellen**.
2. Geben Sie einen eindeutigen Namen für die Aktion und ihre Beschreibung ein.
3. Wählen Sie einen Aktionstyp aus.

E-Mail

Hinweis: Stellen Sie zunächst sicher, dass die E-Mail-Einstellungen konfiguriert sind. Weitere Informationen finden Sie unter "Konfigurieren der E-Mail-Einstellungen" auf Seite 149.

a. Wählen Sie im Menü Typ die Option **E-Mail** aus.

b. Geben Sie die entsprechenden Werte in die Felder ein. Sie können die verfügbaren Platzhalter teilweise oder vollständig als Betreffzeile oder als Teil einer E-Mail-Nachricht verwenden. Weitere Informationen finden Sie unter "Informationen zu Aktionsplatzhaltern" auf Seite 138.

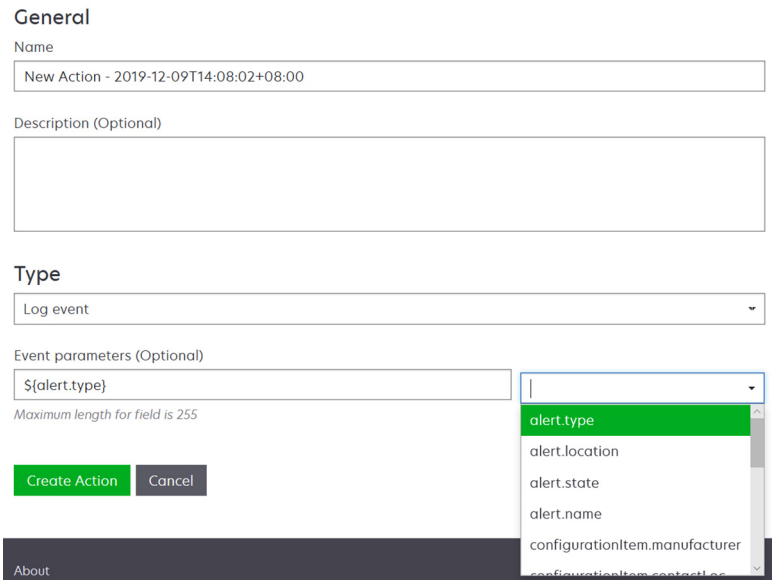


c Klicken Sie auf **Aktion erstellen**.

Ereignisprotokoll

a Wählen Sie im Menü Typ die Option **Ereignisprotokoll** aus.

b Geben Sie die Ereignisparameter ein. Sie können auch die verfügbaren Platzhalter im Drop-Down-Menü verwenden. Weitere Informationen finden Sie unter "Informationen zu Aktionsplatzhaltern" auf Seite 138.



c Klicken Sie auf **Aktion erstellen**.

Informationen zu Aktionsplatzhaltern

Sie können die verfügbaren Platzhalter in der Betreffzeile oder der E-Mail-Nachricht verwenden. Platzhalter sind variable Elemente, die bei Verwendung durch die tatsächlichen Werte ersetzt werden.

- **${eventHandler.timestamp}**: Datum und Uhrzeit der Verarbeitung des Ereignisses durch MVE. Beispiel: **`14. März 2017 13:42:24`**.
- **${eventHandler.name}**: Der Name des Ereignisses.
- **${configurationItem.name}**: Der Systemname des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.address}**: Die MAC-Adresse des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.ipAddress}**: Die IP-Adresse des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.ipHostname}**: Der Hostname des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.model}**: Der Modellname des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.serialNumber}**: Die Seriennummer des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.propertyTag}**: Die Kennzeichnung des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.contactName}**: Der Kontaktname des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.contactLocation}**: Der Kontaktstandort des Druckers, der die Warnung ausgelöst hat.
- **${configurationItem.manufacturer}**: Der Hersteller des Druckers, der die Warnung ausgelöst hat.
- **${alert.name}**: Der Name der ausgelösten Warnung.
- **${alert.state}**: Der Status der Warnung. Er kann "Aktiv" oder "Gelöscht" lauten.

- **${alert.location}**: Die Stelle im Drucker, an der die ausgelöste Warnung aufgetreten ist.
- **"${alert.type}**: Der Schweregrad der ausgelösten Warnung, z. B. **`Warnung`** oder **`Eingriff erforderlich`**.

Verwalten von Aktionen

1. Klicken Sie im Menü "Drucker" auf **Ereignisse & Aktionen** > **Aktionen**.
2. Gehen Sie wie folgt vor:

Aktion bearbeiten

a. Wählen Sie eine Aktion aus, und klicken Sie dann auf **Bearbeiten**.
b. Konfigurieren Sie die Einstellungen.
c. Klicken Sie auf **Änderungen speichern**.

Aktionen löschen

a. Wählen Sie eine oder mehrere Aktionen aus.
b. Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Aktion testen

a. Wählen Sie eine Aktion aus, und klicken Sie auf **Testen**.
b. Zur Überprüfung der Testergebnisse zeigen Sie die Aufgabenprotokolle an.

Hinweise:

- Weitere Informationen finden Sie unter "Anzeigen von Protokollen" auf Seite 145.
- Wenn Sie eine E-Mail-Aktion testen, sollten Sie prüfen, ob die E-Mail an den Empfänger gesendet wurde.

Erstellen von Ereignissen

Sie können Warnungen in Ihrer Druckerflotte überwachen. Erstellen Sie ein Ereignis, und richten Sie dann eine Aktion ein, die ausgeführt wird, wenn die angegebenen Warnungen auftreten. Ereignisse werden bei gesicherten Druckern nicht unterstützt.

1. Klicken Sie im Menü "Drucker" auf **Ereignisse & Aktionen** > **Ereignisse** > **Erstellen**.
2. Geben Sie einen eindeutigen Namen für das Ereignis und seine Beschreibung ein.
3. Wählen Sie im Abschnitt "Warnungen" eine oder mehrere Warnungen aus. Weitere Informationen finden Sie unter "Informationen zu Druckerwarnungen" auf Seite 140.
4. Wählen Sie im Abschnitt "Aktionen" eine oder mehrere Aktionen aus, die ausgeführt werden, wenn die ausgewählten Warnungen aktiv sind.

   Hinweis: Weitere Informationen finden Sie unter "Erstellen einer Aktion" auf Seite 137.
5. Aktivieren Sie das System, sodass ausgewählte Aktionen ausgeführt werden, wenn auf dem Drucker Warnungen gelöscht werden.

6 Legen Sie vor dem Ausführen von ausgewählten Aktionen eine Frist fest.

Hinweis: Wenn die Warnung vor Fristablauf gelöscht wird, wird die Aktion nicht ausgeführt.

7 Klicken Sie auf **Ereignis erstellen**.

Informationen zu Druckerwarnungen

Alarme werden ausgelöst, wenn beim Drucker ein Benutzereingriff erforderlich ist. Die folgenden Warnungen können einem Ereignis in MVE zugewiesen werden:

- **Papierstau in der automatischen Dokumentenzuführung (ADZ)**: Papier staut sich in der ADZ und muss physisch entfernt werden.
  - Papier staut sich am ADZ-Ausgang des Scanners
  - Papier staut sich in ADZ des Scanners
  - Stau am ADZ-Umkehrsensor des Scanners
  - Papier in Scanner-ADZ entfernt
  - Kein Papier in Scanner-ADZ
  - Stau in ADZ-Vorregistrierung des Scanners
  - Stau in ADZ-Registrierung des Scanners
  - Scannerwarnung – Alle Originale erneut einlegen, um den Auftrag erneut zu starten
- **Klappe oder Abdeckung offen**: Eine Klappe am Drucker ist offen und muss geschlossen werden.
  - Klappe/Abdeckung prüfen: Ablage
  - Klappe offen
  - Abdeckungswarnung
  - Abdeckung geschlossen
  - Abdeckung geöffnet
  - Abdeckung offen oder DruckTonerkassette fehlt
  - Duplexabdeckung ist offen
  - ADZ-Abdeckung des Scanners geöffnet
  - Scanner-Stauklappe offen
- **Falsche(s) Medienformat oder -sorte**: Ein Auftrag wird gedruckt und ein bestimmtes Papier muss in das Fach eingelegt werden.
  - Falsches Briefumschlagformat
  - Falsche manuelle Zuführung
  - Falsche Medien
  - Falsches Medienformat
  - Medien einlegen
- **Speicher voll oder -fehler**: Der Drucker weist nur noch wenig Speicherplatz auf und muss Änderungen anwenden.
  - Seite ist zu komplex
  - Die Dateien werden gelöscht
  - Sortierspeicher reicht nicht aus
  - Unzureichender Defragmentierungsspeicher
  - Nicht genug Faxspeicher

  - Nicht genügend Arbeitsspeicher
  - Nicht genug Speicher - angehaltene Aufträge können verloren gehen
  - Nicht genügend Speicher für "Ressourcen speichern"
  - Speicher voll
  - Wenig PS-Speicher
  - Zu viele Seiten im Scanner – Scanauftrag abgebrochen
  - Verringerung der Auflösung
- **Fehlfunktion einer Option**: Eine Option des Druckers befindet sich in einem Fehlerstatus. Folgende Optionen stehen zur Verfügung: Einzugsoptionen, Ausgabeoptionen, Schriftartenkarten, Benutzer-Flash-Karten, Laufwerke und Finisher.
  - Ausrichtung/Verbindung überprüfen
  - Duplex-Verbindung überprüfen
  - Installation von Finisher/Mailbox prüfen
  - Stromversorgung prüfen
  - Beschädigte Option
  - Beschädigte Option
  - Gerät entnehmen
  - Duplexwarnung
  - Duplexfach fehlt
  - Externer Netzwerkadapter fehlt
  - Finisher-Warnung
  - Finisher-Klappe oder Sicherheitssperre offen
  - Finisher-Papierwand offen
  - Falsches Duplexgerät
  - Falsche Papierzuführung
  - Falsche Ablage
  - Falsches unbekanntes Gerät
  - Falsche Optionsinstallation
  - Eingabewarnung
  - Konfigurationsfehler bei Eingabe
  - Option: Warnung
  - Ablage voll
  - Ablage fast voll
  - Ausgabekonfigurationsfehler
  - Option voll
  - Option fehlt
  - Papiereinzugsmechanismus fehlt
  - Option "Aufträge drucken"
  - Gerät wieder einsetzen
  - Ablage wieder einsetzen
  - Zu viele Zufuhrfächer installiert

  - Zu viele Optionen installiert
  - Zu viele Ablagen installiert
  - Fach fehlt
  - Fach fehlt während des Einschaltvorgangs
  - Facherkennungsfehler
  - Papierzuführung nicht kalibriert
  - Option nicht formatiert
  - Nicht unterstützte Option
  - Papierzuführung wieder einsetzen
- **Papierstau**: Papier staut sich im Drucker und muss physisch entfernt werden.
  - Interner Papierstau
  - Warnung: Papierstau
  - Papierstau
- **Scanner-Fehler**: Am Scanner ist ein Problem aufgetreten.
  - Scannerrückseite – Kabel nicht eingesteckt
  - Scannerrücklauf gesperrt
  - Flachbett/Leitstreifen des Scanners reinigen
  - Scanner deaktiviert
  - Flachbettabdeckung des Scanners offen
  - Scannervorderseite – Kabel nicht eingesteckt
  - Ungültige Scanner-Registrierung
- **Verbrauchsmaterialfehler**: Bei einem Verbrauchsmaterial des Druckers ist ein Problem aufgetreten.
  - Falsches Verbrauchsmaterial
  - Falsche Tonerkassette
  - Beschädigtes Verbrauchsmaterial
  - Fixierstation oder Auftragsrolle fehlt
  - Linke Tonerkassette ist fehlerhaft oder fehlt
  - Rechte Tonerkassette ist fehlerhaft oder fehlt
  - Falsches Verbrauchsmaterial
  - Vorbereitung fehlgeschlagen
  - Verbrauchsmaterialwarnung
  - Verbrauchsmaterialstau
  - Verbrauchsmaterial fehlt
  - Auswurfgriff der DruckTonerkassette gezogen
  - DruckTonerkassette nicht richtig eingesetzt
  - Verbrauchsmaterial nicht kalibriert
  - Nicht lizenziertes Verbrauchsmaterial
  - Nicht unterstütztes Verbrauchsmaterial
- **Verbrauchsmaterial oder Füllstand leer**: Ein Verbrauchsmaterial des Druckers muss ausgetauscht werden.
  - Papierzuführung leer
  - Verbraucht

  - Drucker zur Wartung bereit
  - Planmäßige Wartung
  - Verbrauchsmaterial leer
  - Verbrauchsmaterial voll
  - Verbrauchsmaterial voll oder fehlt

  Hinweis: Der Drucker sendet die Warnung als Fehlermeldung und eine Warnung. Wenn eine dieser Warnungen ausgelöst wird, ist die zugehörige Aktion zweimal aufgetreten.
- **Verbrauchsmaterial oder Füllstand niedrig**: Ein Verbrauchsmaterial des Druckers geht zur Neige.
  - Frühwarnung
  - 1. wenig
  - Wenig Papier
  - Erneuern
  - Fast leer
  - Fast verbraucht
  - Verbrauchsmaterial niedrig
  - Verbrauchsmaterial fast voll
- **Nicht kategorisierte Warnung oder Bedingung**
  - Farbkalibrierungsfehler
  - Datenübertragungsfehler
  - Druckwerk CRC-Fehler
  - Externe Warnung
  - Faxverbindung unterbrochen
  - Lüfter blockiert
  - Hex aktiv
  - Duplexseite einlegen und 'Fortfahren' drücken
  - Interne Warnung
  - Interner Netzwerkadapter muss gewartet werden
  - Warnung für logische Einheit
  - Offline
  - Offline für Warnungsaufforderung
  - Vorgang fehlgeschlagen
  - Benutzereingriff - Warnung
  - Seitenfehler
  - Anschlusswarnung
  - Anschlusskommunikationsfehler
  - Anschluss deaktiviert
  - Strom sparen
  - Ausschalten
  - PS-Auftragszeitsperre
  - PS-Zeitsperre für manuelle Zufuhr
  - Konfiguration erforderlich

- SIMM-Prüfsummenfehler
- Verbrauchsmaterial kalibrieren
- Toner-Patch-Erkennung fehlgeschlagen
- Unbekannte Warnsituation
- Unbekannte Konfiguration
- Unbekannte Warnsituation für Scanner
- Benutzer gesperrt
- Allgemeine Warnung

Verwalten von Ereignissen

1. Klicken Sie im Menü "Drucker" auf **Ereignisse & Aktionen** > **Ereignisse**.
2. Führen Sie einen der folgenden Schritte aus:

Ereignis bearbeiten

a. Wählen Sie ein Ereignis aus, und klicken Sie dann auf **Bearbeiten**.
b. Konfigurieren Sie die Einstellungen.
c. Klicken Sie auf **Änderungen speichern**.

Ereignisse löschen

a. Wählen Sie ein oder mehrere Ereignisse aus.
b. Klicken Sie auf **Löschen**, und bestätigen Sie dann das Löschen.

Anzeigen von Aufgabestatus und Verlauf

Übersicht

Bei Aufgaben handelt es sich um alle in MVE ausgeführten Druckerverwaltungsaktivitäten. Dazu zählen z. B. Druckersuche, Prüfung und Durchsetzung von Konfigurationen. Auf der Seite Status wird der Status aller derzeit ausgeführten Aufgaben und der in den letzten 72 Stunden ausgeführten Aufgaben angezeigt. Informationen der aktuell ausgeführten Aufgaben werden in das Protokoll eingetragen. Aufgaben, die älter sind als 72 Stunden, können nur als einzelne Protokolleinträge auf der Seite Protokoll angezeigt werden; Sie können mithilfe der Aufgaben-IDs nach ihnen suchen.

Anzeigen des Aufgabenstatus

Klicken Sie im Menü "Aufgaben" auf **Status**.

Hinweis: Der Aufgabenstatus wird in Echtzeit aktualisiert.

Aufgaben werden angehalten

1. Klicken Sie im Menü "Aufgaben" auf **Status**.
2. Wählen Sie im derzeit ausgeführten Abschnitt "Aufgaben" eine oder mehrere Aufgaben aus.
3. Klicken Sie auf **Stopp**.

Anzeigen von Protokollen

1. Klicken Sie im Menü "Aufgaben" auf **Protokolle**.
2. Wählen Sie Aufgabenkategorien, Aufgabenarten oder einen Zeitraum aus.

   Hinweise:

   - Über das Suchfeld können Sie nach mehreren Aufgaben-IDs suchen. Trennen Sie mehrere Aufgaben-IDs durch Komma, oder geben Sie mit einem Bindestrich einen Bereich an. Beispielsweise `11, 23, 30-35`.
   - Klicken Sie auf **Nach CSV exportieren**, um die Suchergebnisse zu exportieren.

Protokolle löschen

1. Klicken Sie im Menü "Aufgaben" auf **Protokoll**.
2. Klicken Sie auf **Protokoll löschen** und wählen Sie dann ein Datum aus.
3. Klicken Sie auf **Protokoll löschen**.

Exportieren von Protokollen

1. Klicken Sie im Menü Aufgaben auf **Protokoll**.
2. Wählen Sie Aufgabenkategorien, Aufgabenarten oder einen Zeitraum aus.
3. Klicken Sie auf **Nach CSV exportieren**.

Festlegen von Zeitplänen für Aufgaben

Erstellen eines Zeitplans

1. Klicken Sie im Menü Aufgaben auf **Zeitplan** > **Erstellen**.
2. Geben Sie im Abschnitt Allgemein einen eindeutigen Namen für die geplanten Aufgaben und eine Beschreibung ein.
3. Führen Sie im Abschnitt Aufgabe einen der folgenden Schritte aus:

Prüfung planen

a. Wählen Sie **Prüfung** aus.
b. Wählen Sie einen gespeicherten Suchvorgang aus.

Übereinstimmungsprüfung planen

a. Wählen Sie **Übereinstimmung** aus.
b. Wählen Sie einen gespeicherten Suchvorgang aus.

Druckerstatusprüfung planen

a. Wählen Sie **Aktueller Status** aus.
b. Wählen Sie einen gespeicherten Suchvorgang aus.
c. Wählen Sie eine Aktion aus.

Konfigurationsbereitstellung planen

a. Wählen Sie **Datei bereitstellen** aus.
b. Wählen Sie einen gespeicherten Suchvorgang aus.
c. Navigieren Sie zur Datei, und wählen Sie anschließend den Dateityp aus.
d. Wählen Sie bei Bedarf eine Bereitstellungsmethode bzw. das Protokoll aus.

Suche planen

a. Wählen Sie **Suche** aus.
b. Wählen Sie ein Suchprofil aus.

Konfigurationsdurchsetzung planen

a. Wählen Sie **Durchsetzung** aus.
b. Wählen Sie einen gespeicherten Suchvorgang aus.

Zertifikatüberprüfung planen

Wählen Sie **Zertifikat validieren** aus.

Hinweis: Während der Validierung kommuniziert MVE mit dem CA-Server, um die Zertifikatskette und die Zertifikatsperrliste (Certificate Revocation List, CRL) herunterzuladen. Das Zertifikat des Anmeldeagenten wird ebenfalls generiert. Mit diesem Zertifikat kann der CA-Server MVE vertrauen.

Export einer Ansicht planen

a Wählen Sie **Export anzeigen** aus.

b Wählen Sie einen gespeicherten Suchvorgang aus.

c Wählen Sie eine Anzeigevorlage aus.

d Geben Sie die Liste von E-Mail-Adressen ein, an die die exportierten Dateien gesendet werden.

4 Stellen Sie im Abschnitt Zeitplan das Datum, die Uhrzeit und die Häufigkeit der Aufgabe ein.

5 Klicken Sie auf **Geplante Aufgabe erstellen**.

Verwalten von geplanten Aufgaben

1 Klicken Sie im Menü Aufgaben auf **Zeitplan**.

2 Führen Sie einen der folgenden Schritte aus:

Eine geplante Aufgabe bearbeiten

a Wählen Sie eine Aufgabe aus, und klicken Sie dann auf **Bearbeiten**.

b Konfigurieren Sie die Einstellungen.

c Klicken Sie auf **Geplante Aufgabe bearbeiten**.

Hinweis: Die Informationen über die letzte Ausführung werden entfernt, wenn eine geplante Aufgabe bearbeitet wird.

Löschen Sie eine geplante Aufgabe

a Wählen Sie eine Aufgabe aus, und klicken Sie auf **Löschen**.

b Klicken Sie auf **Geplante Aufgabe löschen**.

Ausführen weiterer Verwaltungsaufgaben

Konfigurieren allgemeiner Einstellungen

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **Allgemein**, und wählen Sie dann eine Hostnamen-Quelle aus.
   - **Drucker**: Das System ruft den Hostnamen beim Drucker ab.
   - **Reverse DNS Lookup**: Das System ruft den Hostnamen mithilfe der IP-Adresse aus der DNS-Tabelle ab.
3. Stellen Sie die Häufigkeit der erneuten Warnregistrierung ein.

   Hinweis: Drucker können durch Änderungen den Warnregistrierungsstatus verlieren, so zum Beispiel bei Neustart oder Aktualisierungen der Firmware. MVE versucht den Status automatisch bei Ende des aktuellen Intervalls, das in der Häufigkeit der erneuten Warnregistrierung eingestellt ist, wiederherzustellen.
4. Klicken Sie auf **Änderungen speichern**.

Konfigurieren der E-Mail-Einstellungen

Aktivieren Sie die SMTP-Konfiguration, damit MVE Datenexportdateien und Ereignisbenachrichtigungen per E-Mail senden kann.

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **E-Mail**, und wählen Sie dann **E-Mail SMTP-Konfiguration aktivieren**.
3. Geben Sie den SMTP-Mailserver und -Anschluss ein.
4. Wählen Sie die richtige Verschlüsselung aus.

   Hinweise:

   - Wählen Sie für die SSL-Verschlüsselung den Anschluss 465 aus.
   - Wählen Sie für die TLS/STARTTLS-Verschlüsselung den Anschluss 587 aus.
5. Geben Sie die E-Mail-Adresse des Absenders ein.
6. Wenn der Benutzer sich vor dem E-Mail-Versand anmelden muss, wählen Sie die Option **Anmeldung erforderlich**, und geben Sie die Benutzeranmeldeinformationen ein.
7. Klicken Sie auf **Änderungen speichern**.

Hinzufügen eines Haftungsausschlusses bei Anmeldung

Sie können einen Haftungsausschluss bei Anmeldung konfigurieren, der angezeigt wird, wenn Benutzer sich bei einer neuen Sitzung anmelden. Benutzer müssen den Haftungsausschluss akzeptieren, bevor Sie auf MVE zugreifen können.

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **Haftungsausschluss**, und wählen Sie dann **Haftungsausschluss vor der Anmeldung aktivieren**.
3. Geben Sie den Text des Haftungsausschlusses ein.
4. Klicken Sie auf **Änderungen speichern**.

Signieren des MVE-Zertifikats

Secure Socket Layer (SSL) oder Transport Layer Security (TLS) ist ein gängiges Sicherheitsprotokoll, das die Kommunikation zwischen einem Server und Client mittels Datenverschlüsselung und Zertifikatauthentifizierung schützt. In MVE wird TLS zum Schutz der sensiblen Informationen zwischen MVE-Server und Webbrowser verwendet. Die geschützten Informationen können folgende sein: Druckerkennwörter, Sicherheitsrichtlinien, MVE-Benutzeranmeldeinformationen oder Drucker-Authentifizierungsinformationen, z. B. LDAP oder Kerberos.

TLS ermöglicht die Verschlüsselung dieser Daten durch den MVE-Server und den Webbrowser vor dem Sendevorgang und die Entschlüsselung nach dem Empfang. Außerdem setzt SSL voraus, dass sich der Server mit einem Zertifikat beim Web-Browser authentifiziert, um seine Identität nachzuweisen. Dieses Zertifikat ist entweder selbst oder von einer vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters signiert. Standardmäßig ist MVE für die Verwendung eines selbst signierten Zertifikats konfiguriert.

1. Laden Sie die Signieraufforderung für das Zertifikat herunter.
   a. Klicken Sie in der oberen rechten Ecke der Seite auf .
   b. Klicken Sie auf **TLS** > **herunterladen**.
   c. Wählen Sie **Signierungsanforderung für Zertifikat** aus.

   Hinweis: Die Signierungsanforderung für das Zertifikat enthält Subject Alternative Names (SANs – Listen von alternativen Namen für den Inhaber des Zertifikats).
2. Verwenden Sie eine vertrauenswürdige Zertifizierungsstelle zum Signieren des Zertifikats.
3. Installieren Sie das durch eine vertrauenswürdige Zertifizierungsstelle signierte Zertifikat.
   a. Klicken Sie in der oberen rechten Ecke der Seite auf .
   b. Klicken Sie auf **TLS** > **Signiertes Zertifikat installieren**.
   c. Laden Sie das durch eine vertrauenswürdige Zertifizierungsstelle signierte Zertifikat hoch, und klicken Sie anschließend auf **Zertifikat installieren**.
   d. Klicken Sie auf **MVE-Dienst neu starten**.

      Hinweis: Durch einen Neustart des MVE-Dienstes wird das System neu gestartet, und der Server ist u. U. für einige Minuten nicht verfügbar. Stellen Sie vor dem Neustart des Dienstes sicher, dass aktuell keine Aufgaben ausgeführt werden.

Entfernen von Benutzerinformationen und Verweisen

MVE erfüllt die Datenschutzrichtlinien der DSGVO (Datenschutz-Grundverordnung). MVE kann so konfiguriert werden, dass das Recht auf Vergessenwerden gilt und private Benutzerinformationen aus dem System entfernt werden.

Entfernen von Benutzern

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **Benutzer**, und wählen Sie dann einen oder mehrere Benutzer aus.
3. Klicken Sie auf **Löschen** > **Benutzer löschen**.

Entfernen von Benutzerinformationen in LDAP

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **LDAP**.
3. Entfernen Sie alle benutzerbezogenen Informationen in den Suchfiltern und den Bindungseinstellungen.

Entfernen von Benutzerinformationen im E-Mail-Server

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **E-Mail**.
3. Entfernen Sie alle benutzerbezogenen Informationen, z. B. Benutzeranmeldeinformationen, die für die Authentifizierung mit dem E-Mail-Server verwendet werden.

Entfernen von Benutzerinformationen in den Aufgabenprotokollen

Weitere Informationen finden Sie unter "Protokolle löschen" auf Seite 145.

Entfernen von Benutzerinformationen in einer Konfiguration

1. Klicken Sie im Menü Konfigurationen auf **Alle Konfigurationen**.
2. Klicken Sie auf den Konfigurationsnamen.
3. Entfernen Sie auf der Registerkarte Standard alle benutzerbezogenen Werte aus den Druckereinstellungen, z. B. Kontaktname und Kontaktstandort.

Entfernen von Benutzerinformationen in einer erweiterten Sicherheitskomponente

1. Klicken Sie im Menü Konfigurationen auf **Alle erweiterten Sicherheitskomponenten**.
2. Klicken Sie auf den Komponentennamen.
3. Entfernen Sie im Abschnitt Erweiterte Sicherheitseinstellungen alle benutzerbezogenen Werte.

Entfernen von Benutzerinformationen in gespeicherten Suchen

1. Klicken Sie im Menü Drucker auf **Gespeicherte Suchvorgänge**.
2. Klicken Sie auf einen gespeicherten Suchvorgang.

3 Entfernen Sie alle Suchkriterien, die benutzerbezogene Werte verwenden, z. B. Kontaktname und Kontaktstandort.

Entfernen von Benutzerinformationen in Schlüsselwörtern

1 Klicken Sie im Menü Drucker auf **Druckerliste**.

2 Heben Sie die Zuweisung von benutzerbezogenen Schlüsselwörtern zu den Druckern auf.

3 Klicken Sie im Menü Drucker auf **Schlüsselwörter**.

4 Entfernen Sie alle Schlüsselwörter, die benutzerbezogene Informationen verwenden.

Entfernen von Benutzerinformationen in Ereignissen und Aktionen

1 Klicken Sie im Menü Drucker auf **Ereignisse & Aktionen**.

2 Entfernen Sie alle Aktionen, die E-Mail-Verweise auf Benutzer enthalten.

Häufig gestellte Fragen

Markvision Enterprise – FAQ

Warum kann ich beim Erstellen einer Konfiguration aus der Liste "Unterstützte Modelle" nicht mehrere Drucker auswählen?

Konfigurationseinstellungen und Befehle sind für die Druckermodelle unterschiedlich.

Können andere Benutzer auf meine gespeicherten Suchvorgänge zugreifen?

Ja. Alle Benutzer können auf gespeicherte Suchvorgänge zugreifen.

Wo befinden sich die Protokolldateien?

Sie finden die Installationsprotokolldateien im versteckten Verzeichnis des Benutzers, der MVE installiert. Beispiel: **`C:\Benutzer\Administrator\AppData\Local\Temp\mveLexmark-install.log`**.

Sie finden die ***.log**-Anwendungsprotokolldateien im Ordner ***`installation_dir`*`\Lexmark\Markvision Enterprise\tomcat\logs`**, wobei es sich bei ***`installation_dir`*** um den Installationsordner von MVE handelt.

Was ist der Unterschied zwischen Hostname und Reverse DNS Lookup?

Ein Hostname ist ein eindeutiger Name, der einem Netzwerkdrucker zugewiesen wurde. Jeder Hostname entspricht einer IP-Adresse. Reverse DNS Lookup wird verwendet, um den angegebenen Hostnamen und Domänennamen einer bestimmten IP-Adresse zu ermitteln.

Wo finde ich Reverse DNS Lookup in MVE?

Reverse DNS Lookup befindet sich unter "Allgemeine Einstellungen". Weitere Informationen finden Sie unter "Konfigurieren allgemeiner Einstellungen" auf Seite 149.

Wie kann ich manuell Regeln für die Windows-Firewall hinzufügen?

Führen Sie die Eingabeaufforderung als Administrator aus, und geben Sie Folgendes ein:

```
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"
```

Dabei handelt es sich bei ***`installation_dir`*** um den Installationsordner von MVE.

Wie richte ich MVE ein, um einen anderen Anschluss als Port 443 zu verwenden?

1. Beenden Sie den Markvision Enterprise-Dienst.
   a. Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **services.msc** ein.
   b. Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Stopp**.
2. Öffnen Sie die Datei ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

   Dabei handelt es sich bei ***installation_dir*** um den Installationsordner von MVE.
3. Ändern Sie den **Anschluss-Port**-Wert auf einen anderen nicht verwendeten Anschluss.

```
<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. Ändern Sie den **redirectPort**-Wert auf dieselbe Anschlussnummer, die beim Anschluss-Port verwendet wird.

```
<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. Starten Sie den Markvision Enterprise-Dienst erneut.
   a. Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **services.msc** ein.
   b. Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Neu starten**.
6. Zugriff auf MVE mithilfe des neuen Anschlusses.

   Öffnen Sie beispielsweise einen Web-Browser, und geben Sie in das Feld "URL" Folgendes ein: **https://*MVE_SERVER*:*port*/mve**.

   Dabei ist ***MVE_SERVER*** der Hostname bzw. die IP-Adresse der auf dem Server gehosteten MVE-Software, und ***Port*** ist die Anschluss-Port-Nummer.

Wie kann ich die Ziffern und TLS-Versionen anpassen, die MVE verwendet?

1. Beenden Sie den Markvision Enterprise-Dienst.
   a. Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **services.msc** ein.
   b. Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Stopp**.

2 Öffnen Sie die Datei ***installation_dir*\Lexmark\Markvision Enterprise\tomcat\conf\server.xml**.

Dabei handelt es sich bei ***installation_dir*** um den Installationsordner von MVE.

3 Konfigurieren Sie die Ziffern und TLS-Versionen.

Weitere Informationen zur Konfiguration finden Sie in den **Anweisungen für die Apache Tomcat SSL-/TLS-Konfiguration**.

Weitere Informationen zu den Protokollen und Ziffernwerten finden Sie in der **Dokumentation für Apache Tomcat SSL-Support-Informationen**.

4 Starten Sie den Markvision Enterprise-Dienst erneut.

a Öffnen Sie das Dialogfeld Ausführen, und geben Sie anschließend **services.msc** ein.

b Klicken Sie mit der rechten Maustaste auf **Markvision Enterprise**, und klicken Sie anschließend auf **Neu starten**.

Wie verwalte ich CRL-Dateien bei der Verwendung von Microsoft CA Enterprise?

1 Rufen Sie die CRL-Datei vom CA-Server ab.

Hinweise:

- Für Microsoft CA Enterprise wird die CRL nicht automatisch über SCEP heruntergeladen.
- Weitere Informationen erhalten Sie im *Konfigurationshandbuch für Microsoft Certificate Authority*.

2 Speichern Sie die CRL-Datei im Ordner ***installation_dir*\Lexmark\Markvision Enterprise\apps\library\crl**, wobei ***installation_dir*** der Installationsordner von MVE ist.

3 Konfigurieren Sie die Zertifizierungsstelle in MVE.

Hinweis: Dieser Prozess wird nur für das SCEP-Protokoll verwendet.

Fehlerbehebung

Benutzer hat das Passwort vergessen

Setzen Sie das Passwort des Benutzers zurück.

Sie müssen über Administratorrechte verfügen, um das Passwort zurückzusetzen.

1. Klicken Sie in der oberen rechten Ecke der Seite auf .
2. Klicken Sie auf **Benutzer**, und wählen Sie dann einen Benutzer aus.
3. Klicken Sie auf **Bearbeiten**, und ändern Sie dann das Passwort.
4. Klicken Sie auf **Änderungen speichern**.

Wenn Sie Ihr Passwort vergessen haben, gehen Sie wie folgt vor:

- Wenden Sie sich an einen anderen Administrator, um Ihr Passwort zurückzusetzen.
- Setzen Sie sich mit dem Lexmark Kundendienst in Verbindung.

Administrator hat das Kennwort vergessen.

Erstellen Sie ein weiteres Administratorkonto, und löschen Sie dann das vorherige Konto.

Sie können das Markvision Enterprise-Kennwortdienstprogramm verwenden, um ein weiteres Administratorkonto zu erstellen.

1. Navigieren Sie zu dem Ordner, in dem Markvision Enterprise installiert ist.

   Beispiel: **`C:\Program Files\`**
2. Starten Sie die Datei **mvepwdutility-windows.exe** im Verzeichnis Lexmark\Markvision Enterprise\.
3. Wählen Sie eine Sprache aus und klicken Sie dann auf **OK** > **Weiter**.
4. Wählen Sie **Benutzerkonto hinzufügen** > **Weiter** aus.
5. Geben Sie die Benutzeranmeldeinformationen ein.
6. Klicken Sie auf **Weiter**.
7. Greifen Sie auf MVE zu, und löschen Sie dann den vorherigen Administrator.

   Hinweis: Weitere Informationen finden Sie unter "Verwalten von Benutzern" auf Seite 30.

Seite wird nicht geladen

Dieses Problem kann auftreten, wenn Sie den Webbrowser geschlossen haben, ohne sich abzumelden.

Probieren Sie eine oder mehrere der folgenden Vorgehensweisen:

Löschen Sie den Cache, und löschen Sie die Cookies in Ihrem Webbrowser

Greifen Sie auf die MVE-Anmeldeseite zu, und melden Sie sich dann mit Ihren Anmeldeinformationen an.

Öffnen Sie einen Web-Browser, und geben Sie dann Folgendes ein: **`https://MVE_SERVER/mve/login`**, wobei ***`MVE_SERVER`*** der Hostname oder die IP-Adresse der auf dem Server gehosteten MVE-Software ist.

Netzwerkdrucker kann nicht gefunden werden

Probieren Sie eine oder mehrere der folgenden Methoden:

Stellen Sie sicher, dass der Drucker eingeschaltet ist.

Stellen Sie sicher, dass das Netzkabel sicher an den Drucker und eine ordnungsgemäß geerdete Netzsteckdose angeschlossen ist.

Verbindung des Druckers mit dem Netzwerk

Starten Sie den Drucker neu.

Stellen Sie sicher, dass TCP/IP auf dem Drucker aktiviert ist.

Stellen Sie sicher, dass die von MVE verwendeten Anschlüsse geöffnet sind und dass SNMP und mDNS aktiviert sind.

Weitere Informationen finden Sie unter "Erläuterungen zu Anschlüssen und Protokollen" auf Seite 162.

Wenden Sie sich an Ihren Ansprechpartner bei Lexmark.

Falsche Druckerinformationen

Durchführen von Audits

Weitere Informationen finden Sie unter "Überprüfen von Druckern" auf Seite 61.

MVE erkennt einen Drucker nicht als gesicherten Drucker.

Stellen Sie sicher, dass der Drucker gesichert ist.

Weitere Informationen zum Sichern von Druckern finden Sie im Dokument *Markvision Enterprise und Druckersicherheit*.

Stellen Sie sicher, dass mDNS eingeschaltet und nicht blockiert ist.

Löschen Sie den Drucker, und führen Sie die Druckererkennung erneut aus.

Weitere Informationen finden Sie unter "Erkennen von Druckern" auf Seite 34.

Das Erzwingen von Konfigurationen mit mehreren Anwendungen schlägt beim ersten Versuch fehl, ist jedoch bei den nachfolgenden Versuchen erfolgreich.

Erhöhen der Zeitsperren

1. Navigieren Sie zu dem Ordner, in dem Markvision Enterprise installiert ist.

   Beispiel: **`C:\Program Files\`**

2. Navigieren Sie zum Ordner Lexmark\MarkVision Enterprise\apps\dm-mve\WEB-INF\classes.
3. Öffnen Sie mit einem Texteditor die Datei *platform.properties*.
4. Bearbeiten Sie den Wert **`cdcl.ws.readTimeout`**.

   Hinweis: Der Wert wird in Millisekunden angegeben. 90.000 Millisekunden entsprechen zum Beispiel 90 Sekunden.

5. Öffnen Sie mit einem Texteditor die Datei *devCom.properties*.
6. Bearbeiten Sie die Werte **`lst.responseTimeoutsRetries`**.

   Hinweis: Der Wert wird in Millisekunden angegeben. 10.000 Millisekunden entsprechen zum Beispiel 10 Sekunden.

   Beispiel: **`lst.responseTimeoutsRetries=10000 15000 20000`**. Der erste Verbindungsversuch erfolgt nach 10 Sekunden, der zweite Verbindungsversuch nach 15 Sekunden und der dritte Verbindungsversuch nach 20 Sekunden.

7. Wenn Sie LDAP GSSAPI verwenden, erstellen Sie gegebenenfalls eine Datei *parameters.properties*.

   Fügen Sie die folgende Einstellung hinzu: **`lst.negotiation.timeout=400`**

   Hinweis: Der Wert wird in Sekunden angegeben.

8. Speichern Sie die Änderungen.

Die Durchsetzung von Konfigurationen mit Druckerzertifikat schlägt fehl

Manchmal wird während der Durchsetzung kein neues Zertifikat ausgestellt.

Erhöhen Sie die Anzahl der Anmeldungswiederholungen

Fügen Sie den folgenden Schlüssel in die **Datei platform.properties** ein:

```
enrol.maxEnrolmentRetry=10
```

Der Wert für die Wiederholung muss größer als fünf sein.

OpenXPKI Zertifizierungsstelle

Zertifikatausstellung mit dem OpenXPKI CA-Server fehlgeschlagen

Stellen Sie sicher, dass der Schlüssel "Unterzeichner im Auftrag" in MVE mit dem Schlüssel des autorisierten Unterzeichners im CA-Server übereinstimmt.

Beispiel:

Wenn der folgende der **ca.onBehhalf.cn**-Schlüssel in der Datei **platform.properties** in MVE ist,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

muss der folgende der **authorized_signer**-Schlüssel in der Datei **generic.yaml** im CA-Server sein.

```
rule1:
            # Full DN
                    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

Weitere Informationen zum Konfigurieren des OpenXPKI CA-Servers finden Sie im *Konfigurationshandbuch für OpenXPKI Certificate Authority*.

Ein interner Fehler tritt auf.

Installieren Sie das Gebietsschema en_US.utf8.

1. Führen Sie den Befehl **`dpkg-reconfigure locales`** aus.
2. Installieren Sie das Gebietsschema **en_US.utf8** (locale -a | grep en_US).

Die Anmeldeaufforderung wird nicht angezeigt.

Beim Zugriff auf **http://yourhost/openxpki/** erhalten Sie nur das Open Source TrustCenter-Banner ohne Anmeldeaufforderung.

Aktivieren Sie `fcgid`.

Führen Sie die folgenden Befehle aus:

1. `a2enmod fcgid`
2. `service apache2 restart`

Ein Fehler "Verschachtelter Connector ohne Klasse" tritt auf.

Ein Fehler **`AUSNAHME: Verschachtelter Connector ohne Klasse (scep.scep-server-1.connector.initial)`** tritt bei /usr/share/perl5/Connector/Multi.pm Zeile 201 auf.

Aktualisieren Sie `scep.scep-server-1`.

Ersetzen Sie in **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml** **`scep.scep-server-1`** durch **`scep.generic`**.

Hinweis: Ersetzen Sie **`REAL`** durch den Namen des Bereichs. Wenn Sie beispielsweise den Standardbereich verwenden, verwenden Sie **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Zertifikate können nicht manuell genehmigt werden.

Die Schaltfläche Manuell genehmigen wird beim manuellen Genehmigen von Zertifikaten nicht angezeigt.

Aktualisieren Sie `scep.scep-server-1`.

Ersetzen Sie in **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml** **`scep.scep-server-1`** durch **`scep.generic`**.

Hinweis: Ersetzen Sie **`REAL`** durch den Namen des Bereichs. Wenn Sie beispielsweise den Standardbereich verwenden, verwenden Sie **`ca-one`**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Beim Genehmigen von Registrierungsanforderungen tritt ein Perl-Fehler auf.

Aktualisieren Sie `scep.scep-server-1`.

Ersetzen Sie in **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml** **`scep.scep-server-1`** durch **`scep.generic`**.

Hinweis: Ersetzen Sie **REAL** durch den Namen des Bereichs. Wenn Sie beispielsweise den Standardbereich verwenden, verwenden Sie **ca-one**.

```
eligible:
     initial:
            value@: connector:scep.generic.connector.initial
```

Die Token ca-signer-1 und vault-1 sind offline

Die Seite Systemstatus zeigt an, dass die Token **ca-signer-1** und **vault-1** offline sind.

Probieren Sie eine oder mehrere der folgenden Methoden:

Kennwort des Zertifikatschlüssels ändern

Ändern Sie das Kennwort des Zertifikatschlüssels in **/etc/openxpki/config.d/realm/ca-one/crypto.yaml**.

Die korrekten Symlinks erstellen und die Schlüsseldatei kopieren

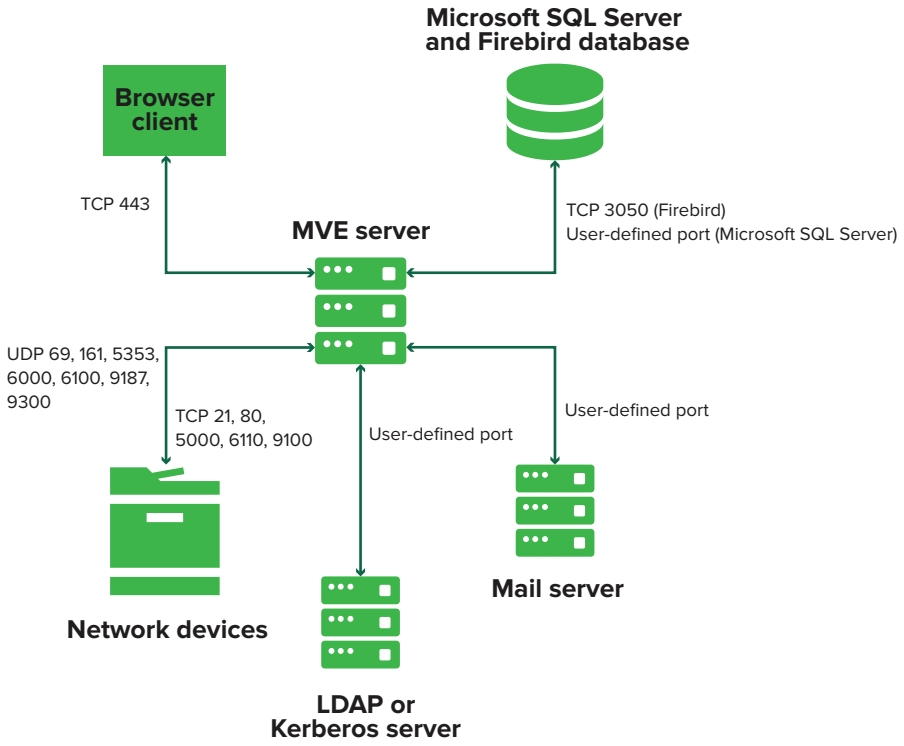
Weitere Informationen finden Sie unter "Kopieren der Schlüsseldatei und Erstellen eines Symlinks" auf Seite 108.

Stellen Sie sicher, dass die Schlüsseldatei von OpenXPKI gelesen werden kann.

Anhang

Erläuterungen zu Anschlüssen und Protokollen

Wie in der folgenden Übersicht dargestellt, setzt MVE verschiedene Anschlüsse und Protokolle für verschiedene Netzwerkkommunikationstypen ein:



Hinweise:

- Die Anschlüsse sind bidirektional und müssen für MVE geöffnet oder aktiv sein, um ordnungsgemäß zu funktionieren. Stellen Sie sicher, dass alle Druckeranschlüsse aktiviert sind.
- Für einige Kommunikationen ist ein flüchtiger Anschluss erforderlich, das bedeutet ein zugewiesener Bereich verfügbarer Anschlüsse am Server. Wenn ein Client eine temporäre Kommunikationssitzung anfragt, weist der Server dem Client einen dynamischen Anschluss zu. Der Anschluss ist nur kurzzeitig gültig und kann wieder verwendet werden, wenn die vorherige Sitzung abläuft.

Kommunikation zwischen Server und Drucker

In der folgenden Tabelle sehen Sie die während der Kommunikation zwischen MVE-Server und Netzwerkdruckern verwendeten Anschlüsse und Protokolle.

Protokoll	MVE-Server	Drucker	Einsatzgebiet
Network Printing Alliance Protocol (Protokoll im NPAP-Format)	UDP 9187	UDP 9300	Kommunikation mit Lexmark Netzwerkdruckern.
XML-Netzwerktransport (XMLNT)	UDP 9187	UDP 6000	Kommunikation mit einigen Lexmark Netzwerkdruckern.
Lexmark Secure Transport (LST)	UDP 6100 Flüchtiger TCP-Anschluss (Transmission Control Protocol) (Quittungsbetrieb)	UDP 6100 TCP 6110 (Quittungsbetrieb)	Sichere Kommunikation mit einigen Lexmark Netzwerkdruckern.
Multicast Domain Name System (mDNS)	Flüchtiger UDP-Anschluss (User Datagram Protocol)	UDP 5353	Suche nach Lexmark Netzwerkdruckern und Festlegen von Druckersicherheitsfunktionen. **Hinweis:** Dieser Anschluss ist erforderlich, damit MVE mit gesicherten Druckern kommunizieren kann.
Simple Network Management Protocol (SNMP)	Flüchtiger UDP-Anschluss	UDP 161	Suche nach und Kommunikation mit Netzwerkdruckern von Lexmark und von Drittanbietern.
File Transfer Protocol (FTP)	Flüchtiger TCP-Anschluss	TCP 21 TCP 20	Dateien bereitstellen.
Hypertext Transfer Protocol (HTTP)	Flüchtiger TCP-Anschluss	TCP 80	Dateien bereitstellen oder Konfigurationen durchsetzen.
		TCP 443	Dateien bereitstellen oder Konfigurationen durchsetzen.
Hypertext Transfer Protocol over SSL (HTTPS)	Flüchtiger TCP-Anschluss	TCP 161 TCP 443	Dateien bereitstellen oder Konfigurationen durchsetzen.
RAW	Flüchtiger TCP-Anschluss	TCP 9100	Dateien bereitstellen oder Konfigurationen durchsetzen.

Kommunikation zwischen Drucker und Server

Dies sind Anschluss und Protokoll, die während der Kommunikation zwischen Netzwerkdruckern und dem MVE-Server verwendet werden.

Protokoll	Drucker	MVE-Server	Einsatzgebiet
NPAP	UDP 9300	UDP 9187	Generieren und empfangen von Warnungen

Kommunikation zwischen Server und Datenbank

In der folgenden Tabelle sehen Sie die während der Kommunikation zwischen MVE-Server und Datenbanken verwendeten Anschlüsse.

MVE-Server	Datenbank	Einsatzgebiet
Flüchtiger TCP-Anschluss	Benutzerdefinierter Anschluss. Der Standardanschluss ist TCP 1433.	Kommunikation mit einer SQL Server-Datenbank.
Flüchtiger TCP-Anschluss	TCP 3050	Kommunikation mit einer Firebird-Datenbank.

Kommunikation zwischen Client und Server

Dies sind Anschluss und Protokoll, die während der Kommunikation zwischen Browserclient und MVE-Server verwendet werden.

Protokoll	Browserclient	MVE-Server
Hypertext Transfer Protocol over SSL (HTTPs)	TCP-Anschluss	TCP 443

Kommunikation zwischen Server und Mail-Server

In der folgenden Tabelle sehen Sie die während der Kommunikation zwischen MVE-Server und Mail-Server verwendeten Anschlüsse und Protokolle.

Protokoll	MVE-Server	SMTP-Server	Einsatzgebiet
Simple Mail Transfer Protocol (SMTP)	Flüchtiger TCP-Anschluss	Benutzerdefinierter Anschluss. Der Standardanschluss ist TCP 25.	Stellt die E-Mail-Funktionen für den Empfang von Druckerwarnungen bereit.

Kommunikation zwischen Server und LDAP-Server

Dies sind Anschlüsse und Protokoll, die während der Kommunikation zwischen MVE-Server und einem LDAP-Server verwendet werden, einschließlich Benutzergruppen und Authentifizierungsfunktionen.

Protokoll	MVE-Server	LDAP-Server	Einsatzgebiet
Lightweight Directory Access Protocol (LDAP)	Flüchtiger TCP-Anschluss	Benutzerdefinierter Anschluss. Der Standardanschluss ist TCP 389.	Authentifizierung von MVE-Benutzern, die einen LDAP-Server verwenden.
Lightweight Directory Access Protocol über TLS (LDAPS)	Flüchtiger TCP-Anschluss	Benutzerdefinierter Anschluss. Der Standardanschluss ist TCP 636.	Authentifizierung von MVE-Benutzern, die einen LDAP-Server über TLS verwenden.
Kerberos	Flüchtiger UDP-Anschluss	Benutzerdefinierter Anschluss. Der Standardanschluss ist UDP 88.	Authentifizierung von MVE-Benutzern mit Kerberos.

Aktivieren der automatischen Genehmigung von Zertifikatsanforderungen in Microsoft CA

Standardmäßig befinden sich alle CA-Server im Ausstehend-Modus, und Sie müssen jede signierte Zertifikatsanforderung manuell genehmigen. Da diese Methode für Bulk-Anforderungen unpraktisch ist, aktivieren Sie die automatische Genehmigung signierter Zertifikate.

1. Klicken Sie im Server-Manager auf **Extras > Zertifizierungsstelle**.
2. Klicken Sie im linken Bereich mit der rechten Maustaste auf die Zertifizierungsstelle, und klicken Sie anschließend auf **Eigenschaften > Richtlinienmodul**.
3. Klicken Sie auf der Registerkarte Anforderungsbehandlung auf **Einstellungen in der Zertifikatsvorlage befolgen, falls zutreffend**, und klicken Sie anschließend auf **OK**.

   Hinweis: Wenn **Zertifikatsanforderungsstatus auf ausstehend festlegen** aktiviert ist, müssen Sie das Zertifikat manuell genehmigen.
4. Starten Sie den CA-Dienst neu.

Widerrufen von Zertifikaten

Hinweis: Stellen Sie zu Beginn sicher, dass der CA-Server für CRLs konfiguriert ist und dass sie verfügbar sind.

1. Öffnen Sie auf dem CA-Server die **Zertifizierungsstelle**.
2. Erweitern Sie im linken Bereich die Zertifizierungsstelle, und klicken Sie anschließend auf **Ausgestellte Zertifikate**.
3. Klicken Sie mit der rechten Maustaste auf ein Zertifikat, das Sie widerrufen möchten, und klicken Sie anschließend auf **Alle Aufgaben > Zertifikat widerrufen**.
4. Wählen Sie einen Grundcode und das Datum und die Uhrzeit für den Widerruf aus, und klicken Sie anschließend auf **Ja**.
5. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Widerrufene Zertifikate**, und klicken Sie anschließend auf **Alle Aufgaben > Veröffentlichen**.

   Hinweis: Stellen Sie sicher, dass das widerrufene Zertifikat unter Widerrufene Zertifikate aufgeführt ist.

Sie können die Seriennummer des widerrufenen Zertifikats in der CRL sehen.

Hinweise

Hinweis zur Ausgabe

September 2022

Der folgende Abschnitt gilt nicht für Länder, in denen diese Bestimmungen mit dem dort geltenden Recht unvereinbar sind: LEXMARK INTERNATIONAL, INC., STELLT DIESE VERÖFFENTLICHUNG OHNE MANGELGEWÄHR ZUR VERFÜGUNG UND ÜBERNIMMT KEINERLEI GARANTIE, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, DER GESETZLICHEN GARANTIE FÜR MARKTGÄNGIGKEIT EINES PRODUKTS ODER SEINER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. In einigen Staaten ist der Ausschluss von ausdrücklichen oder stillschweigenden Garantien bei bestimmten Rechtsgeschäften nicht zulässig. Deshalb besitzt diese Aussage für Sie möglicherweise keine Gültigkeit.

Diese Publikation kann technische Ungenauigkeiten oder typografische Fehler enthalten. Die hierin enthaltenen Informationen werden regelmäßig geändert; diese Änderungen werden in höheren Versionen aufgenommen. Verbesserungen oder Änderungen an den beschriebenen Produkten oder Programmen können jederzeit vorgenommen werden.

Die in dieser Softwaredokumentation enthaltenen Verweise auf Produkte, Programme und Dienstleistungen besagen nicht, dass der Hersteller beabsichtigt, diese in allen Ländern zugänglich zu machen, in denen diese Softwaredokumentation angeboten wird. Kein Verweis auf ein Produkt, Programm oder einen Dienst besagt oder impliziert, dass nur dieses Produkt, Programm oder dieser Dienst verwendet werden darf. Sämtliche Produkte, Programme oder Dienste mit denselben Funktionen, die nicht gegen vorhandenen Beschränkungen bezüglich geistigen Eigentums verstoßen, können stattdessen verwendet werden. Bei Verwendung anderer Produkte, Programme und Dienstleistungen als den ausdrücklich vom Hersteller empfohlenen ist der Benutzer für die Beurteilung und Prüfung der Funktionsfähigkeit selbst zuständig.

Technischen Support von Lexmark erhalten Sie unter **http://support.lexmark.com**.

Informationen zur Lexmark Datenschutzrichtlinie für die Verwendung dieses Produkts finden Sie unter **www.lexmark.com/privacy**.

Unter **www.lexmark.com** erhalten Sie Informationen zu Zubehör und Downloads.

Marken

Lexmark, das Lexmark-Logo und Markvision sind Marken oder eingetragene Marken von Lexmark International, Inc. in den USA und/oder anderen Ländern.

Windows, Microsoft, Microsoft Edge, PowerShell, SQL Server und Windows Server sind Marken der Microsoft-Unternehmensgruppe.

Firebird ist eine eingetragene Marke der Firebird Foundation.

Google Chrome ist eine Marke von Google LLC.

Apple and Safari are registered trademarks of Apple Inc.

Java ist eine eingetragene Marke von Oracle und/oder seinen Tochtergesellschaften.

Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

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

Lizenzhinweise

Alle Lizenzhinweise zu diesem Produkt finden Sie im Programmordner.

Glossar

Aktion	Eine E-Mail-Benachrichtigung oder eine Befehlszeilenanwendung. Einem Ereignis zugewiesene Aktionen werden ausgelöst, wenn eine Druckerwarnung auftritt.
Ereignis	Legt fest, welche Aktionen ausgeführt werden, wenn bestimmte Alarme aktiv sind.
Gesicherter Drucker	Ein Drucker, der so konfiguriert ist, dass er über einen verschlüsselten Kanal kommuniziert und für den Zugriff auf seine Funktionen oder Anwendungen eine Authentifizierung verlangt.
Konfiguration	Eine Zusammenfassung von Einstellungen, die einem Drucker oder einer Gruppe von Druckermodellen zugewiesen und durchgesetzt werden können. Innerhalb einer Konfiguration können Sie Printer Settings ändern und Anwendungen, Lizenzen, Firmware und CA-Zertifikate für die Drucker bereitstellen.
Schlüsselwort	Ein benutzerdefinierter, den Druckern zugewiesener Text, anhand dessen im System nach diesen Druckern gesucht werden kann. Wenn Sie eine Suche mit einem Schlüsselwort filtern, werden nur Drucker angezeigt, die mit dem Schlüsselwort markiert wurden.
Suchprofil	Ein Profil mit einer Reihe von Parametern, die zum Suchen von Druckern in einem Netzwerk verwendet werden. Es kann auch vordefinierte Konfigurationen enthalten, die Druckern automatisch während der Suche zugewiesen und durchgesetzt werden können.
Token	Eine Kennung, die Datenwerte des Druckers für variable Einstellungen in einer Konfiguration enthält.
Überprüfung	Die Sammlung von Druckerdaten wie Druckerstatus, Verbrauchsmaterialien und Funktionen.
Variableneinstellungen	Eine Reihe von Printer Settings, die dynamische Werte enthalten und in eine Konfiguration integriert werden können

Index

Zeichen

A

Ä

B

C

D

E

F

G

H

I

K

L

M

N

O

W

Z