Lexmark

Markvision Enterprise

Version 4.0

Administrator's Guide

Contents

Managing printer alerts... 95

Viewing task status and history..103

Scheduling tasks..105

Performing other administrative tasks..................................107

Frequently asked questions..110

Change history

November 2020

- Updated information on the following:
  - Supported printer models
  - Supported databases
- Added information on the following:
  - Managing and deploying configurations
  - Backing up and restoring the database
  - Managing certificates using OpenXPKI and Microsoft Certificate Authority
- Added support for the following:
  - Managing and deploying configurations to a group of printer models
  - Creating custom database names

February 2020

- Updated information on the following:
  - Supported printer models
  - Supported servers
  - Supported databases
  - Valid Markvision^{TM} Enterprise (MVE) upgrade path
- Added information on the following:
  - Instructions for best practices
  - Instructions on managing automated certificates
  - Default advanced security components and their settings
  - Other ways in securing printers
  - Sample scenarios

June 2019

- Updated information on the following:
  - Footnotes added to printer models that require certificates
  - Assigning dbo rights when setting up the database
  - Valid upgrade path when upgrading to version 3.4
  - Files that are needed when backing up and restoring the database
  - LDAP server authentication settings
  - Certificate validity status, dates, and time zone parameters are added to the search rule settings
  - Configuring the permissions and function access controls in the printer security settings
  - Selecting a firmware file from the resource library when updating the printer firmware
  - Selecting the start date, start and pause time, and days of the week when updating the printer firmware
  - Managing configurations

- Added information on the following:
  - Understanding printer security states
  - Configuring advanced security components
  - Creating an advanced security component from a printer
  - Generating a printable version of the configuration settings
  - Uploading a printer fleet certificate authority
  - Removing user information and references
  - Understanding permissions and function access controls
  - Troubleshooting steps when enforcement of configurations with multiple applications fails
  - Troubleshooting steps when an Admin user has forgotten the password

August 2018

- Updated information on the following:
  - Supported printer models
  - Setting up the database
  - Upgrading to MVE 3.3
  - Frequently asked questions
  - Creating an action
  - Creating a schedule
- Added information on the following:
  - Setting up a run-as domain user account
  - Exporting logs
  - Troubleshooting steps when MVE does not recognize secured printers

July 2018

- Updated information on upgrading to MVE 3.2.

April 2018

- Updated information on the following:
  - Supported printer models
  - Setting up the database
  - Backing up and restoring database files
  - The URL for accessing MVE
  - Understanding variable settings
- Added information on the following:
  - Configuring printer certificates
  - Stopping tasks
  - Updating printer firmware

September 2017

- Updated information on the following:
  - System requirements
  - Communication between MVE and Lexmark^{TM} Forms Printer 2580, 2581, 2590, and 2591 models
  - Manual dropping of Microsoft SQL Server databases
  - Backing up and restoring database files
  - Required security settings for function access controls when deploying firmware and solution files to printers
  - Support for licenses when deploying applications
  - Printer alerts and their associated actions
  - Printer state automatic recovery
  - Events and keywords assignment

June 2017

- Initial document release for MVE 3.0.

Overview

Understanding Markvision Enterprise

Markvision Enterprise (MVE) is a web-based printer management utility software designed for IT professionals.

With MVE, you can manage a large fleet of printers in an enterprise environment efficiently by doing the following:

- Find, organize, and track a fleet of printers. You can audit a printer to collect printer data such as status, settings, and supplies.
- Create configurations and assign them to printers.
- Deploy firmware, printer certificates, certificate authority (CA), and applications to the printers.
- Monitor printer events and alerts.

This document provides information on how to configure, use, and troubleshoot the application.

This document is intended for administrators.

Getting started

Best practices

This topic outlines the recommended steps to use MVE in managing your fleet effectively.

1 Install MVE in your environment.

    a Create a server using the latest Windows Server environment.

       Related content:

          Web server requirements

    b Create a domain user account that does not have administrator access.

       Related content:

          Setting up a run-as user

    c Create a Microsoft SQL Server database, set up encryption, and then give the new user account access to the databases.

       Related content:

          • **Database requirements**

          • **Setting up the database**

    d Install MVE using the domain user account and the SQL server with Windows Authentication.

       Related content:

          Installing MVE

2 Set up MVE, and then discover and organize your fleet.

    a Sign the server certificate.

       Related content:

          • **Signing the MVE certificate**

          • **Setting up MVE to manage certificates automatically**

    b Set up the LDAP settings.

       Related content:

          • **Enabling LDAP server authentication**

          • **Installing LDAP certificates**

    c Connect to an e-mail server.

       Related content:

          Configuring e-mail settings

    d Discover your fleet.

       Related content:

          Discovering printers

    e Schedule audits and status updates.

       Related content:

          • **Auditing printers**

          • **Updating printer status**

    f Set up basic settings, such as contact names, locations, asset tags, and time zones.

    g Organize your fleet. Use keywords, such as locations, to categorize the printers.

       Related content:

- **Assigning keywords to printers**
- **Creating a saved search**

3 Secure your fleet.

    a Secure printer access using the default advanced security components.

       Related content:

- **Securing printers using the default configurations**
- **Understanding permissions and function access controls**
- **Other ways to secure your printers**

    b Create a secured configuration that includes certificates.

       Related content:

- **Creating a configuration**
- **Importing files to the resource library**

    c Enforce the configuration on your current fleet.

       Related content:

- **Assigning configurations to printers**
- **Enforcing configurations**

    d Schedule enforcements and conformance checks.

       Related content:
          Creating a schedule

    e Add configurations to discovery profiles to secure new printers.

       Related content:
          Creating a discovery profile

    f Sign printer certificates.

       Related content:
          Signing the MVE certificate

4 Keep your firmware up to date.

    Related content:
       Updating the printer firmware

5 Install and configure applications.

    Related content:

- **Creating a configuration**
- **Importing files to the resource library**

6 Monitor your fleet.

    Related content:
       Creating a saved search

System requirements

MVE is installed as a web server and can be accessed from a web browser on any computer on the network. MVE also uses a database to store information about the printer fleet. The following lists are the requirements for the web server, database, and user system:

Web server requirements

Processor	At least 2GHz dual-core processor that uses Hyper-Threading Technology (HTT)
RAM	At least 4GB
Hard disk drive	At least 60GB

Note: MVE, Lexmark Document Distributor (LDD), and Device Deployment Utility (DDU) cannot be run on the same server.

Supported servers

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

Note: MVE supports only the 64-bit version of the operating systems.

Database requirements

Supported databases

- Firebird® database (built-in)
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

Note: The recommended minimum database size is 60GB to allocate 20MB for FRAMEWORK, and 4.5MB for MONITOR and QUARTZ. For more information, see .

User system requirements

Supported web browsers

- Microsoft Edge
- Internet Explorer 11 or later
- Mozilla Firefox (latest version)
- Google Chrome™ (latest version)
- Apple Safari (latest version)

Screen resolution

At least 1280 x 768 pixels

Supported languages

- Brazilian Portuguese
- English
- French
- German
- Italian
- Simplified Chinese
- Spanish

Supported printer models

- Dell 3330dn[1], 3333dn[1], 3335dn[1]
- Dell 5230dn[1], 5350dn[1], 5530dn[1], 5535dn[1]
- Dell B2360dn, B3460dn, B3465dn
- Dell B5460dn, B5465dnf, S5830dn
- Dell S2830dn
- Dell S5840cdn
- Lexmark 4600, 6500
- Lexmark B2236
- Lexmark B2338[2], B2442[2], B2546[2], B2650[2], B2865[1]
- Lexmark B3440, B3442
- Lexmark C2132
- Lexmark C2240[2], C2325[2], C2425[2], C2535[2]
- Lexmark C3224
- Lexmark C3326
- Lexmark C3426
- Lexmark C4150[2], C6160[2], C9235[2]
- Lexmark C520[1], C522[1], C524[1], C530[1], C532[1], C534[1], C540[3], C543[3], C544[3], C546[3]
- Lexmark C734[1], C736[1], C746, C748
- Lexmark C770[1], C772[1], C780[1], C782[1], C792
- Lexmark C920[1], C925[1], C935[1], C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS331
- Lexmark CS421[2], CS521[2], CS622[2]
- Lexmark CS431
- Lexmark CS720[2], CS725[2]
- Lexmark CS727[2], CS728[2], CX727[2]

- Lexmark CS820[2], CS827[2]
- Lexmark CS921[2], CS923[2], CS927[2]
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX331
- Lexmark CX421[2], CX522[2], CX622[2], CX625[2]
- Lexmark CX431
- Lexmark CX725
- Lexmark CX820[2], CX825[2], CX827[2], CX860[2]
- Lexmark CX920[2], CX921[2], CX922[2], CX923[2], CX924[2], CX927[2]
- Lexmark E250[1], E260[3], E352[1], E360[3], E450[1], E460[1], E462[1]
- Lexmark Forms Printer 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 M5155, M5163, M5170
- Lexmark M5255[2], M5265[2], M5270[2]
- Lexmark MB2236
- Lexmark MB2338[2], MB2442[2], MB2546[2], MB2650[2], MB2770[2]
- Lexmark MB3442
- Lexmark MC2325[2], MC2425[2], MC2535[2], MC2640[2]
- Lexmark MC3224
- Lexmark MC3326
- Lexmark MC3426
- 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, MS431
- 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, MX431
- 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 T640[1], T642[1], T644[1], T650[1], T652[1], T654[1], T656[1]

- Lexmark W840[1], W850[1]
- Lexmark X264[3], X363[3], X364[3], X463[1], X464[1], X466[1]
- Lexmark X543[3], X544[3], X546[3], X548
- Lexmark X642[1], X644[1], X646[1], X651[1], X652[1], X654[1], X656[1], X658[1]
- Lexmark X734[1], X736[1], X738[1], X746, X748, X792
- Lexmark X850[1], X852[1], X854[1], X860[1], X862[1], X864[1]
- Lexmark X925, X940[1], X945[1], X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235[2], XC2240[2], XC4240[2]
- Lexmark XC4140[2], XC4150[2], XC6152[2], XC8155[2], XC8160[2]
- Lexmark XC9225[2], XC9235[2], XC9245[2], XC9255[2], XC9265[2]
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242[2], XM1246[2], XM3250[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
- Pantum CM7105DN
- Pantum CM7000
- Pantum CP2300DN
- Pantum CP2500
- Pantum CP2500DN Plus
- Pantum M7600
- Pantum M7650DN
- Pantum P4000
- Pantum P4200DN
- Pantum P5000
- Pantum P5500DN
- Source Technologies ST9530[1]
- Source Technologies ST9620[1], ST9630[1]
- Source Technologies ST9712, ST9715, ST9717, ST9720, ST9722, ST9730
- Source Technologies ST9815[2], ST9818[2], ST9820[2], ST9821[2], ST9822[2], ST9830[2]
- Toshiba e-Studio 305CP
- Toshiba e-Studio 388CP[2]
- Toshiba e-Studio 305CS, 306CS
- Toshiba e-Studio 338CS[2], 388CS[2], 389CS[2], 479CS[2]
- Toshiba e-Studio 385P, 470P
- Toshiba e-Studio 385S, 425S
- Toshiba e-Studio 408P[2], 478P[2]
- Toshiba e-Studio 408S[2], 448S[2], 478S[2]

- Toshiba e-Studio 409P[2], 409S[2]
- Toshiba e-Studio 520P, 525P
- Toshiba e-Studio 528P[2]

[1] A printer certificate update is required. In this release, the Java platform security and performance update removes support for some certificate-signing algorithms, such as MD5 and SHA1. This change prevents MVE from working with some printers. For more information, see the **help information documentation**.

[2] SNMPv3 support must be enabled on the printer.

[3] If an advanced security password is set on the printer, then MVE cannot support the printer.

[4] MVE cannot communicate with Lexmark Forms Printer 2580, 2581, 2590, and 2591 models that are in the Not Ready state. The communication works only when MVE has previously communicated with the printer in the Ready state. The printer can be in the Not Ready state when there are errors or warnings, such as empty supplies. To change the state, resolve the error or warning, and then press **Ready**.

Setting up the database

You can use either Firebird or Microsoft SQL Server as the back-end database. The following table can help you decide on what database to use.

	Firebird	Microsoft SQL Server
Server installation	Must be installed on the same server as MVE.	Can be run from any server.
Communication	Locked down to only localhost.	Communicates over a static port or a dynamic named instance. SSL/TLS communication with a secured Microsoft SQL server is supported.
Performance	Shows performance issues with large fleets.	Shows the best performance for large fleets.
Database size	Default database sizes are 6MB for FRAMEWORK, and 1MB for MONITOR and QUARTZ. The FRAMEWORK table grows at 1KB for each printer record that is added.	Default database sizes are 20MB for FRAMEWORK, and 4.5MB for MONITOR and QUARTZ. The FRAMEWORK table grows at 1KB for each printer record that is added.
Configuration	Configured automatically during installation.	Requires preinstallation setup.

If you are using Firebird, then the MVE installer installs and configures Firebird with no other configuration required.

If you are using Microsoft SQL Server, then before installing MVE, do the following:

- Allow the application to run automatically.
- Set the network libraries to use TCP/IP sockets.
- Create the following databases:

  Note: The following are default database names. You can also provide custom database names.

- FRAMEWORK
- MONITOR
- QUARTZ

- If you are using a named instance, then set the Microsoft SQL Server Browser service to start automatically. Otherwise, set a static port on the TCP/IP sockets.

- Create a user account with dbowner rights to all three databases that MVE uses to connect to and set up the database. If the user is a Microsoft SQL Server account, then enable the Microsoft SQL Server and the Windows Authentication modes on the Microsoft SQL Server.

  Note: Uninstalling MVE that is configured to use Microsoft SQL Server does not drop the created tables or databases. After uninstalling, the FRAMEWORK, MONITOR, and QUARTZ databases must be dropped manually.

- Assign the dbo rights to the database user, and then set the dbo schema as the default schema.

Setting up a run-as user

During installation, you can specify MVE to execute either as a local system account or as a domain user account. Executing MVE as a run-as domain user account provides a more secure installation. The domain user account has limited privileges compared to a local system account.

	Run-as domain user account	Run-as local system

Local system permissions	• File all access to the following:
	  – *$MVE_INSTALL*/tomcat/logs
	  – *$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
	  – *$MVE_INSTALL*/apps/dm-mve/download
	  Where *$MVE_INSTALL* is the installation directory.
	• Windows privilege: LOGON_AS_A_SERVICE
		Administrator permissions

Database connection authentication	• Windows Authentication with Microsoft SQL Server • SQL Authentication	SQL Authentication
Configuration	A domain user must be configured before installation.	Configured automatically during installation

If you set up MVE as a run-as domain user account, then create the user on the same domain as the MVE server.

Installing MVE

1 Download the executable file into a path that does not contain any spaces.

2 Run the file as an administrator, and then follow the instructions on the computer screen.

Notes:

- Passwords are hashed and stored securely. Make sure that you remember your passwords, or store them in a secure location because passwords cannot be decrypted once stored.
- If you are connecting to the Microsoft SQL Server using Windows Authentication, then no connection verification occurs during installation. Make sure that the user designated to execute the MVE windows service has a corresponding account in the Microsoft SQL Server instance. The designated user must have dbowner rights to the FRAMEWORK, MONITOR, and QUARTZ databases.

Installing MVE silently

Database settings for silent installation

Setting	Description	Value
`--help`	Shows the list of valid options.	
`--version`	Shows the product information.	
`--unattendedmodeui <unattendedmodeui>`	The user interface for unattended mode.	Default: **none** Allowed: • **none** • **minimal** • **minimalWithDialogs**
`--optionfile <optionfile>`	The installation option file.	Default:
`--debuglevel <debuglevel>`	The debug information level of verbosity.	Default: **2** Allowed: • **0** • **1** • **2** • **3** • **4**
`--mode <mode>`	The installation mode.	Default: **win32** Allowed: • **win32** • **unattended**
`--debugtrace <debugtrace>`	The debug file name.	Default:

Setting	Description	Value
`--installer-language <installer-language>`	The language selection.	Default: `en` Allowed: • `en` • `es` • `de` • `fr` • `it` • `pt_BR` • `zh_CN`
`--encryptionKey <encryptionKey>`	The encryption key.	Encryption key: Default:
`--prefix <prefix>`	The installation directory.	Default: `C:\Program Files`
`--mveLexmark_runas <mveLexmark_runas>`	The run-as user options.	Default: `LOCAL_SYSTEM` Allowed: • `LOCAL_SYSTEM` • `SPECIFIC_USER`
`--serviceRunAsUsername <serviceRunAsUsername>`	The run-as user name.	User name: Default:
`--serviceRunAsPassword <serviceRunAsPassword>`	The run-as user password.	Password: Default:
`--mveLexmark_database <mveLexmark_database>`	The database type.	Default: Allowed: • `FIREBIRD` • `SQL_SERVER`
`--firebirdUsername <firebirdUsername>`	The Firebird database user name.	User name: Default:
`--firebirdPassword <firebirdPassword>`	The Firebird database password.	Password: Default:
`--firebirdFWDbName <firebirdFWDbName>`	The Firebird database name for FRAMEWORK.	Database names: Default: `FRAMEWORK`
`--firebirdMNDbName <firebirdMNDbName>`	The Firebird database name for MONITOR.	Default: `MONITOR`
`--firebirdQZDbName <firebirdQZDbName>`	The Firebird database name for QUARTZ.	Default: `QUARTZ`
`--databaseIPAddress <databaseIPAddress>`	The database IP address or host name.	IP address or host name: Default:
`--databasePort <databasePort>`	The database port number.	Port number: Default:

Setting	Description	Value
`--instanceName <instanceName>`	The instance name.	Instance name: Default:
`--instanceIdentifier <instanceIdentifier>`	The instance.	Default: `databasePort` Allowed: • `databasePort` • `instanceName`
`--databaseUsername <databaseUsername>`	The database user name.	User name: Default:
`--databasePassword <databasePassword>`	The database password.	Password: Default:
`--sqlServerAuthenticationMethod <sqlServerAuthenticationMethod>`	The Microsoft SQL server authentication method.	Default: `sqlServerDbAuthentication` Allowed: • `sqlServerDbAuthentication` • `sqlServerWindowsAuthentication`
`--fWDbName <fWDbName>`	The database name for FRAMEWORK.	Database names: Default: `FRAMEWORK`
`--mNDbName <mNDbName>`	The database name for MONITOR.	Default: `MONITOR`
`--qZDbName <qZDbName>`	The database name for QUARTZ.	Default: `QUARTZ`
`--mveAdminUsername <mveAdminUsername>`	The administrator user name.	User name: Default: `admin`
`--mveAdminPassword <mveAdminPassword>`	The administrator password.	Password: Default:

Accessing MVE

To access MVE, use the login credentials that you created during installation. You can also set up other login methods, such as LDAP, Kerberos, or other local accounts. For more information, see <u>"Setting up user access" on page 27</u>.

1 Open a web browser, and then type `https://MVE_SERVER/mve/`, where **MVE_SERVER** is the host name or IP address of the server hosting MVE.

2 If necessary, accept the disclaimer.

3 Enter your credentials.

4 Click **Log In**.

Notes:

- After logging in, make sure that you change the default administrator password that was used during installation. For more information, see <u>"Changing your password" on page 22</u>.

- If MVE is idle for more than 30 minutes, then the user is logged out automatically.

Changing the language

1 Open a web browser, and then type **https://MVE_SERVER/mve/**, where **MVE_SERVER** is the host name or IP address of the server hosting MVE.

2 If necessary, accept the disclaimer.

3 On the upper-right corner of the page, select a language.

Changing your password

1 Open a web browser, and then type **https://MVE_SERVER/mve/**, where **MVE_SERVER** is the host name or IP address of the server hosting MVE.

2 If necessary, accept the disclaimer.

3 Enter your credentials.

4 Click **Log In**.

5 On the upper-right corner of the page, click your user name, and then click **Change password**.

6 Change the password.

Maintaining the application

Upgrading to MVE 4.0

Before you begin the upgrade, do the following:

- Back up the database and application files. For more information, see "Backing up and restoring the database" on page 24.
- If necessary, provide custom database names.

If you are upgrading from version 1.x, then upgrade to version 2.0 first, and then to version 3.3 before upgrading to version 4.0. The policy migration process is performed only when upgrading to MVE 2.0.

Valid upgrade path	**3.3** to **4.0**
Invalid upgrade path	**1.6.x** to **4.0**
	2.0 to **4.0**

1 Back up your database and application files. Any upgrade or uninstallation creates a risk of unrecoverable data loss. You can use the backup files to restore the application to its previous state in case the upgrade fails.

   Warning—Potential Damage: When you upgrade MVE, the database is changed. Do not restore a database backup that was created from a previous version.

   Note: For more information, see "Backing up and restoring the database" on page 24.

2 Download the executable file into a temporary location.

3 Run the installer as an administrator, and then follow the instructions on the computer screen.

   Notes:

   - When you upgrade to MVE 2.0, policies that are assigned to printers are migrated into a single configuration for each printer model. For example, if fax, copy, paper, and print policies are assigned to an X792 printer, then those policies are consolidated into an X792 configuration. This process does not apply to policies that are not assigned to printers. MVE generates a log file confirming that the policies are migrated to a configuration successfully. For more information, see "Where can I find the log files?" on page 110.
   - After upgrading, make sure to clear the browser cache before accessing the application again.
   - When MVE is upgraded to version 3.5 or later, the advanced security components are factored out of the configurations they are in. If one or more advanced security components are the same, then they are combined into one component. The created advanced security component is added to the advanced security components library automatically.

Backing up and restoring the database

Note: There is potential data loss when performing backup and restore procedures. Make sure to perform the steps properly.

Backing up the database and application files

We recommend backing up your database regularly.

1 Stop the Firebird service and the Markvision Enterprise service.

   a Open the Run dialog box, and then type `services.msc`.

   b Right-click **Firebird Guardian - DefaultInstance**, and then click **Stop**.

   c Right-click **Markvision Enterprise**, and then click **Stop**.

2 Browse to the folder where Markvision Enterprise is installed.

For example, `C:\Program Files\`

3 Back up the application and database files.

Backing up the application files

Copy the following files to a safe 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

Note: Make sure that these files are properly stored. Without the encryption keys in the mve_encryption.jceks file, data stored in an encrypted format in the database and on the file system cannot be recovered.

Backing up the database files

Do either of the following:

Note: The following files are using the default database names. These instructions also apply to customized database names.

- If you are using a Firebird database, then copy the following files to a safe repository. These files must be backed up regularly to avoid data loss.

    – Lexmark\Markvision Enterprise\firebird\security2.fdb

      If you are using custom database names, then update the following:

       - 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
- If you are using Microsoft SQL Server, then create a backup for FRAMEWORK, MONITOR, and QUARTZ. For more information, contact your Microsoft SQL Server administrator.

4 Restart the Firebird service and the Markvision Enterprise service.

   a Open the Run dialog box, and then type **services.msc**.

   b Right-click **Firebird Guardian - DefaultInstance**, and then click **Restart**.

   c Right-click **Markvision Enterprise**, and then click **Restart**.

Restoring the database and application files

Warning—Potential Damage: When you upgrade MVE, the database may be changed. Do not restore a database backup that was created from a previous version.

1 Stop the Markvision Enterprise service.

For more information, see <u>step 1</u> of <u>"Backing up the database and application files" on page 24</u>.

2 Browse to the folder where Markvision Enterprise is installed.

For example, **C:\Program Files**

3 Restore the application files.

Replace the following files with the files that you saved during the backup process:
- 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

Note: You can restore a database backup to a new MVE installation only if the new MVE installation is the same version.

4 Restore the database files.

Do either of the following:
- If you are using a Firebird database, then replace the following files that you saved during the backup process:

  Note: The following files are using the default database names. This instruction also applies to customized database names.

- Lexmark\Markvision Enterprise\firebird\security2.fdb

  If you are using custom database names, then the following files are also restored:
  - 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
- If you are using Microsoft SQL Server, then contact your Microsoft SQL Server administrator.

5 Restart the Markvision Enterprise service.

For more information, see step 4 of "Backing up the database and application files" on page 24.

Updating the installer settings after installation

The Markvision Enterprise Password Utility lets you update the Microsoft SQL Server settings that have been configured during installation without reinstalling MVE. The utility also lets you update the run-as user domain account credentials, such as user name and password. You can also use the utility to create another Admin user if you forget your previous Admin user credentials.

1 Browse to the folder where Markvision Enterprise is installed.

For example, **C:\Program Files**

2 Launch the **mvepwdutility-windows.exe** file in the Lexmark\Markvision Enterprise\ directory.

3 Select a language, and then click **OK** > **Next**.

4 Follow the instructions on the computer screen.

Setting up user access

Overview

MVE lets you add internal users directly to the MVE server or use the user accounts registered in an LDAP server. For more information on adding internal users, see "Managing users" on page 28. For more information on using LDAP user accounts, see "Enabling LDAP server authentication" on page 29.

When adding users, roles must be assigned. For more information, see "Understanding user roles" on page 27.

During authentication, the system checks the user credentials of the internal users present in the MVE server. If MVE cannot authenticate the user, then it tries to authenticate the user in the LDAP server. If the user name exists in both the MVE server and the LDAP server, then the password in the MVE server is used.

Understanding user roles

MVE users can be assigned to one or more roles. Depending on the role, users can perform the following tasks:
- **Admin**—Access and perform tasks in all menus. They also have administrative privileges, such as adding users to the system or configuring the system settings. Only users with an Admin role can stop any running task no matter what user type started it.
- **Printers**
  - Manage discovery profiles.
  - Set the printer states.
  - Perform an audit.
  - Manage categories and keywords.
  - Schedule an audit, data export, and printer discovery.
- **Configurations**
  - Manage configurations, including importing and exporting configuration files.
  - Upload files to the resource library.
  - Assign and enforce configurations to printers.
  - Schedule a conformance check and configurations enforcement.
  - Deploy files to printers.
  - Update the printer firmware.
  - Generate printer certificate signing requests.
  - Download printer certificate signing requests.
- **Event Manager**
  - Manage actions and events.
  - Assign events to printers.
  - Test actions.
- **Service Desk**
  - Update the printer status.
  - Reboot printers.

- **–** Run a conformance check.
- **–** Enforce configurations to printers.

Notes:

- All users in MVE can view the printer information page, and manage saved searches and views.
- For more information on assigning user roles, see "Managing users" on page 28.

Managing users

1 Click ⚙ on the upper-right corner of the page.

2 Click **User**, and then do any of the following:

Add a user

a Click **Create**.

b Type the user name, user ID, and password.

c Select the roles.

Note: For more information, see "Understanding user roles" on page 27.

d Click **Create User**.

Edit a user

a Select a user ID.

b Configure the settings.

c Click **Save Changes**.

Delete users

a Select one or more users.

b Click **Delete**, and then confirm deletion.

Note: A user account is locked out after three consecutive failed login attempts. Only an Admin user can reactivate the user account. If the Admin user is locked out, then the system reactivates it automatically after five minutes.

Enabling LDAP server authentication

LDAP is a standards-based, cross-platform, extensible protocol that runs directly on top of TCP/IP. It is used to access specialized databases called directories.

To avoid maintaining multiple user credentials, you can use the company LDAP server to authenticate user IDs and passwords.

As a prerequisite, the LDAP server must contain user groups that correspond to the required user roles. For more information, see "Understanding user roles" on page 27.

1 Click ⚙ on the upper-right corner of the page.

2 Click **LDAP**, and then select **Enable LDAP for authentication**.

3 In the LDAP server hostname field, type the IP address or the host name of the LDAP server where the authentication occurs.

   Note: If you want to use encrypted communication between the MVE server and the LDAP server, then use the fully qualified domain name (FQDN).

4 Specify the server port number according to the encryption protocol selected.

5 Select the encryption protocol.

   - **None**
   - **TLS**—A security protocol that uses data encryption and certificate authentication to protect the communication between a server and a client. If this option is selected, then a START_TLS command is sent to the LDAP server after the connection is established. Use this setting if you want a secure communication over port 389.
   - **SSL/TLS**—A security protocol that uses public-key cryptography to authenticate the communication between a server and a client. Use this option if you want a secured communication from the start of the LDAP bind. This option is typically used for port 636 or other secured LDAP ports.

6 Select the binding type.

   - **Anonymous**—This option is selected by default. The MVE server does not produce its identity or credentials to the LDAP server to use the LDAP server lookup facility. This option is depreciated in nearly all LDAP implementations and must never be used.
   - **Simple**—The MVE server produces the specified credentials to the LDAP server to use the LDAP server lookup facility.
     a Type the bind user name.
     b Type the bind password, and then confirm the password.
   - **Kerberos**—To configure the settings, do the following:
     a Type the bind user name.
     b Type the bind password, and then confirm the password.
     c Click **Choose File**, and then browse to the krb5.conf file.
   - **SPNEGO**—To configure the settings, do the following:
     a Type the service principal name.
     b Click **Choose File**, and then browse to the krb5.conf file.
     c Click **Choose File**, and then browse to the Kerberos keytab file.

     This option is used only for configuring the Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) to support the Single Sign-On functionality.

7 From the Advanced Options section, configure the following:

- **Search Base**—The base distinguished name (DN) of the root node. In the LDAP community server hierarchy, this node must be the ancestor of the user node and group node. For example, **dc=mvptest,dc=com**.

  Note: When specifying the root DN, make sure that only **dc** and **o** are part of the root DN. If **ou** or **cn** is the ancestor of the user and group nodes, then use **ou** or **cn** in the user and group search bases.

- **User search base**—The node in the LDAP community server where the user object exists. This node is under the root DN where all the user nodes are listed. For example, **ou=people**.

- **User search filter**—The parameter for locating a user object in the LDAP community server. For example, **(uid={0})**.

  Examples of allowed multiple conditions and complex expressions

Log in using	In the User search filter field, type
Common name	**(CN={0})**
Login name	**(sAMAccountName={0})**
User Principal Name	**(userPrincipalName={0})**
Telephone number	**(telephoneNumber={0})**
Login name or common name	**(|(sAMAccountName={0})(CN={0}))**

  Note: The only valid pattern is **{0}**, which means that MVE searches for the MVE user login name.

- **Search User base object and whole subtree**—The system searches all the nodes under the user search base.

- **Group search base**—The node in the LDAP community server containing the user groups that correspond to the MVE roles. This node is under the root DN where all the group nodes are listed. For example, **ou=group**.

- **Group search filter**—The parameter for locating a user within a group that corresponds to a role in MVE.

  Note: Only the **{0}** and **{1}** patterns can be used. If **{0}** is used, then MVE searches for the LDAP user DN. If **{1}** is used, then MVE searches for the MVE user login name.

- **Group role attribute**—Type the LDAP attribute for the full name of the group. An LDAP attribute has a specific meaning and defines a mapping between the attribute and a field name. For example, the LDAP attribute **cn** is associated with the Full Name field. The LDAP attribute **commonname** is also mapped to the Full Name field. Generally, this attribute must be left to the default value of **cn**.

- **Search User base object and whole subtree**—The system searches all the nodes under the group search base.

8 From the LDAP Groups to MVE Role Mapping section, type the names of the LDAP groups that correspond to the MVE roles.

Notes:

- For more information, see .
- You can assign one LDAP group to multiple MVE roles. You can also type more than one LDAP group in a role field, using the vertical bar character (**\|**) to separate multiple groups. For example, to include the **admin** and **assets** groups for the Admin role, type **admin\|assets** in the LDAP groups for Admin role field.

- If you want to use only the Admin role and not the other MVE roles, then leave the fields blank.

9 Click **Save Changes**.

Installing LDAP server certificates

To establish an encrypted communication between the MVE server and the LDAP server, MVE must trust the LDAP server certificate. In the MVE architecture, when MVE is authenticating with an LDAP server, MVE is the client and the LDAP server is the peer.

1 Click on the upper-right corner of the page.

2 Click **LDAP**, and then configure the LDAP settings. For more information, see .

3 Click **Test LDAP**.

4 Enter a valid LDAP user name and password, and then click **Start Test**.

5 Examine the certificate for validity, and then accept it.

Discovering printers

Creating a discovery profile

Use a discovery profile to find printers in your network and add them to the system. In a discovery profile, you can include or exclude a list or range of IP addresses or host names by doing either of the following:

- Adding entries one at a time
- Importing entries using a TXT or CSV file

You can also assign and enforce a configuration automatically to a compatible printer model. A configuration may contain printer settings, applications, licenses, firmware, and CA certificates that can be deployed to the printers.

1 From the Printers menu, click **Discovery Profiles** > **Create**.

2 From the General section, type a unique name and description for the discovery profile, and then configure the following:

- **Timeout**—The duration the system waits for a printer to respond.
- **Retries**—The number of times the system attempts to communicate with a printer.
- **Automatically manage discovered printers**—Newly discovered printers are set to a Managed state automatically, and the New state is skipped during discovery.

3 From the Addresses section, do either of the following:

Add the addresses

a Select **Include** or **Exclude**.

b Type the IP address, host name, subnet, or IP address range.

Add only one entry at a time. Use the following formats for the addresses:

- **`10.195.10.1`** (single IPv4 address)
- **`myprinter.example.com`** (single host name)
- **`10.195.10.3–10.195.10.255`** (IPv4 address range)
- **`10.195.*.*`** (wildcards)
- **`10.195.10.1/22`** (IPv4 Classless Inter-Domain Routing or CIDR notation)
- **`2001:db8:0:0:0:0:2:1`** (full IPv6 address)
- **`2001:db8::2:1`** (collapsed IPv6 address)

Note: If separate discovery profiles are created for the IPv6 address and the IPv4 address for the same printer, then the last discovered address is shown. For example, if a printer is discovered using IPv6, and is discovered again using IPv4, then only the IPv4 address is shown in the printer list.

c Click **Add**.

Import the addresses

a Click **Import**.

b Select whether to include or exclude IP addresses during the discovery.
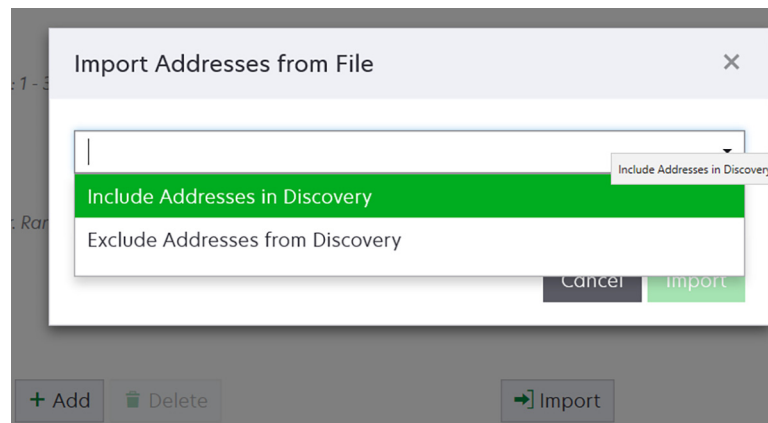
c Browse to the text file that contains a list of addresses. Each address entry must be placed on a separate line.

Sample text file

```
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 Click **Import**.

4 From the SNMP section, select **Version 1, 2c** or **Version 3**, and then set the access permissions.

Note: To discover printers using SNMP version 3, create a user name and password in the printer Embedded Web Server, and then restart the printer. If a connection cannot be established, then rediscover the printers. For more information, see the *Embedded Web Server—Security Administrator's Guide* for the printer.

5 If necessary, from the Enter Credentials section, select the authentication method that the printers are using, and then enter the credentials.

Note: This feature lets you establish communication with secured printers during discovery. The correct credentials must be provided to perform tasks on the secured printers, such as audit, status update, or firmware update.

6 If necessary, from the Assign Configurations section, associate a configuration with a printer model. For information on creating a configuration, see <u>"Creating a configuration" on page 63</u>.

7 Click **Save Profile** or **Save and Run Profile**.

Note: A discovery can be scheduled to occur regularly. For more information, see <u>"Creating a schedule" on page 105</u>.

Managing discovery profiles

1 From the Printers menu, click **Discovery Profiles**.

2 Do any of the following:

Edit a profile

a Select a profile, and then click **Edit**.

b Configure the settings.

c Click **Save Profile** or **Save and Run Profile**.

Copy a profile

a Select a profile, and then click **Copy**.

b Configure the settings.

c Add the IP addresses. For more information, see .

d Click **Save Profile** or **Save and Run Profile**.

Delete a profile

a Select one or more profiles.

b Click **Delete**, and then confirm deletion.

Run a profile

a Select one or more profiles.

b Click **Run**. Check the discovery status from the Tasks menu.

Sample scenario: Discovering printers

Company ABC is a large manufacturing company occupying a nine-story building. The company just bought 30 new Lexmark printers, distributed among the nine floors. As the IT personnel, you must add these new printers to MVE. The printers are already connected to the network, but you do not know all the IP addresses.

You want to secure the following new printers in the Accounting department.

```
10.194.55.60
10.194.56.77
10.194.55.71
10.194.63.27
10.194.63.10
```

Sample implementation

1 Create a discovery profile for the printers in the Accounting department.

2 Add the five IP addresses.

3 Create a configuration that secures the specified printers.

4 Include the configurations in the discovery profile.

5 Save and run the profile.

6 Create another discovery profile for the rest of the printers.

7 Include the IP addresses using a wildcard. Use the following: `10.194.*.*`

8 Exclude the five printer IP addresses in the Accounting department.

9 Save, and then run the profile.

Viewing printers

Viewing the printer list

The Printer Listing page is the default landing page when you access MVE. The table shows the list of the printers that are added in MVE.

1 From the Printers menu, click **Printer Listing**.

2 From the Printer Listing page, do any of the following:

- To search for specific printers, do any of the following:
    - Use the search box to search for an IP address, host name, system name, or serial number.

– Change the printer listing view. For more information, see "Changing the printer listing view" on page 42.
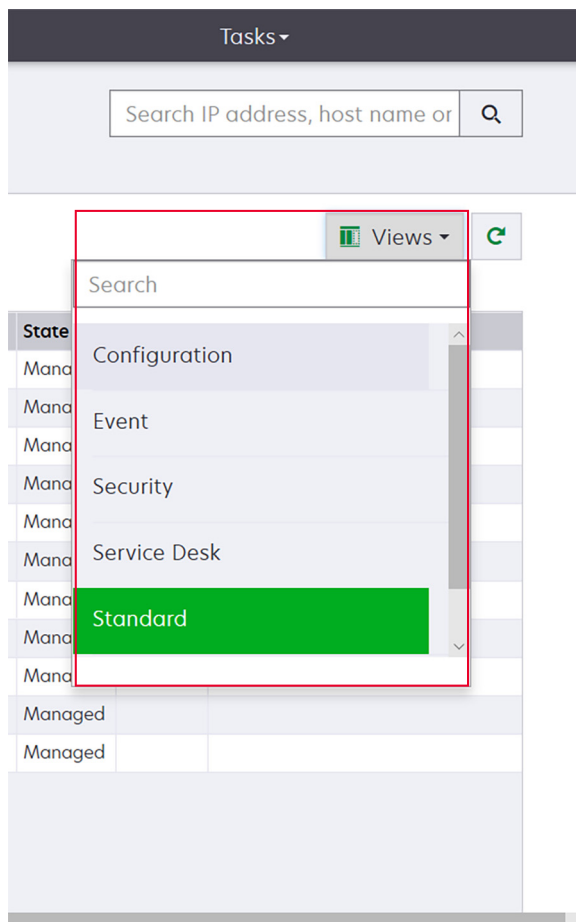
Note: If you are using the search box, then the application searches for all the printers in the system. The selected filters and saved searches are ignored. If you run a saved search, then the criteria specified in the saved search are used. The selected filters and the IP address or host name typed in the search box are ignored. You can also use the filters to narrow down the current search results.

– Use the filters.

– Run a saved search. For more information, see .

- To sort the printers, from the printer list table, click any column header. The printers are sorted according to the selected column header.
- To view more information about the printers, resize the columns. Place your cursor over the vertical border of the column header, and then drag the border to the left or to the right.

Viewing the printer information

To see the complete list of information, make sure that an audit is performed on the printer. For more information, see .

1 From the Printers menu, click **Printer Listing**.

2 Click the IP address of the printer.

3 View the following information:

- **Status**—The status of the printer.
- **Supplies**—The supply details and remaining supply percentage.
- **Identification**—The printer network identification information.

  Note: The time zone information is available only in some printer models.

- **Dates**—The date the printer is added to the system, the discovery date, and the most recent audit date.
- **Firmware**—The printer firmware properties and code levels.
- **Capabilities**—The printer features.
- **Memory Options**—The hard disk size and user flash free space.
- **Input Options**—The settings for the available trays.
- **Output Options**—The settings for the available bins.
- **eSF Applications**—The information about the installed Embedded Solutions Framework (eSF) applications on the printer.
- **Printer Statistics**—The specific values for each of the printer properties.
- **Change Details**—The information about the changes in the printer.

  Note: This information is available only in printers that are in a Managed (Changed) state. For more information, see .

- **Printer Credentials**—The credentials used in the configuration assigned to the printer.
- **Default Printer Certificate**—The properties of the printer certificate.

  Notes:

  - This information is available only in some printer models.
  - An Expiring Soon validity status indicates that the certificate expires within 30 days.

- **Configuration Properties**—The properties of the configuration assigned to the printer.
- **Active Alerts**—The printer alerts that are waiting to be cleared.
- **Assigned Events**—The events assigned to the printer.

Exporting printer data

MVE lets you export the printer information that is available in your current view.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Printer** > **Export data**.

Notes:

- The exported data is saved in a CSV file.
- Exporting data can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.
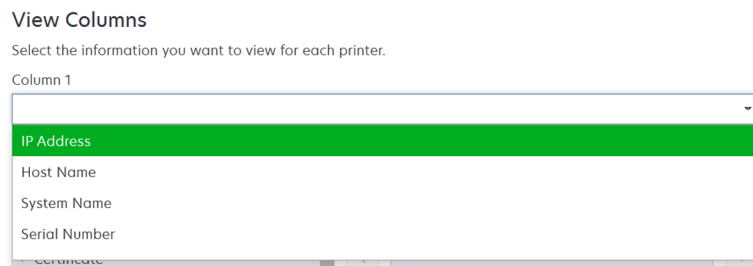
Managing views

The Views feature lets you customize the information that is shown in the printer listing page.

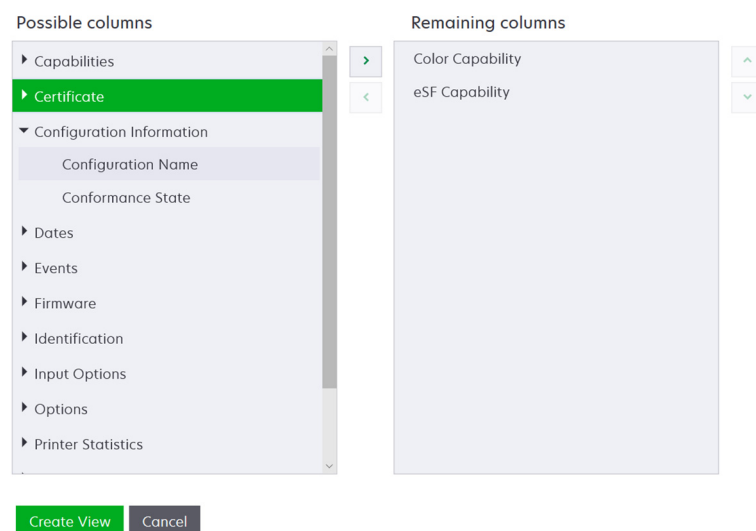**1** From the Printers menu, click **Views**.

2 Do any of the following:

Create a view

a Click **Create**.

b Type a unique name for the view and its description.

c From the View Columns section, in the Column 1 menu, select the identifier column.

d From the Possible columns section, expand a category, select the information that you want to show as a column, and then click **>**.

- **Capabilities**—Shows whether the selected features are supported on the printer.
- **Certificate**—Shows the printer certificate creation date, enrolment status, expiration date, renewal date, revision number, certificate subject, validity, and signing status.

- **Configuration Information**—Shows configuration-related printer information, such as conformance, configuration name, and state.
- **Dates**—Shows the last audit, last conformance check, last discovery, and the date the printer was added to the system.
- **Events**—Shows event-related printer information.
- **Firmware**—Shows firmware-related information, such as the firmware version.
- **Identification**—Shows information about the printer, such as the IP address, host name, and serial number.
- **Input Options**—Shows information about the input options, such as the tray size and media type.
- **Options**—Shows information about the printer options, such as hard disk and flash drive.
- **Printer Statistics**—Shows information about the printer usage, such as the number of printed or scanned pages, and total number of faxed jobs.
- **Solutions**—Shows the eSF applications installed on the printer, and their version numbers.
- **Status**—Show the printer and supplies status.
- **Supplies**—Shows supplies-related information.

e Click **Create View**.

Edit a view

a Select a view.

b Click **Edit**, and then edit the settings.

c Click **Save Changes**.

Copy a view

a Select a view.

b Click **Copy**, and then configure the settings.

c Click **Create View**.

Delete views

a Select one or more views.

b Click **Delete**, and then confirm deletion.

Set a default view

a Select a view.

b Click **Set As Default**.

The following views are system-generated, and cannot be edited or deleted:

- Configuration
- Printer List
- Event
- Security
- Service Desk
- Standard

Changing the printer listing view

For more information, see .

1 From the Printers menu, click **Printer Listing**.

2 Click **Views**, and then select a view.

Filtering printers using the search bar

Note the following when using the search bar to search for printers.

- To search for an IP address, make sure to type the complete IP address or range.

    For example:

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

- If the search string is not a full IP address, then the printers are searched according to their host name, system name, or serial number.

- The underscore character (_) can be used as a wildcard character.

Managing keywords

Keywords let you create custom tags and assign them to printers.

1 From the Printers menu, click **Keywords**.

2 Do either of the following:

- Add, edit, or delete a category.

    Note: Categories group keywords together.

- Add, edit, or delete a keyword.

For information on assigning keywords to printers, see .

Using saved searches

Understanding printer life cycle states

System-generated saved searches show the printers in the following printer life cycle states:

- **All Printers**—All printers in the system.
- **Managed Printers**—Printers that appear can be in any of the following states:
    - Managed (Normal)
    - Managed (Changed)
    - Managed (Missing)
    - Managed (Found)

- **Managed (Changed) Printers**—Printers in the system whose following properties were changed at the last audit:
  - Property tag
  - Host name
  - Contact name
  - Contact location
  - Memory size
  - Duplex
  - Supplies (excluding levels)
  - Input options
  - Output options
  - eSF applications
  - Default printer certificate
- **Managed (Found) Printers**—Printers that were reported as missing, but have now been found.
- **Managed (Missing) Printers**—Printers that the system was unable to communicate with.
- **Managed (Normal) Printers**—Printers in the system whose properties have remained the same since the last audit.
- **New Printers**—Printers that are newly discovered and are not set to a Managed state automatically.
- **Retired Printers**—Printers marked as no longer active in the system.
- **Unmanaged Printers**—Printers marked for exclusion from activities performed in the system.
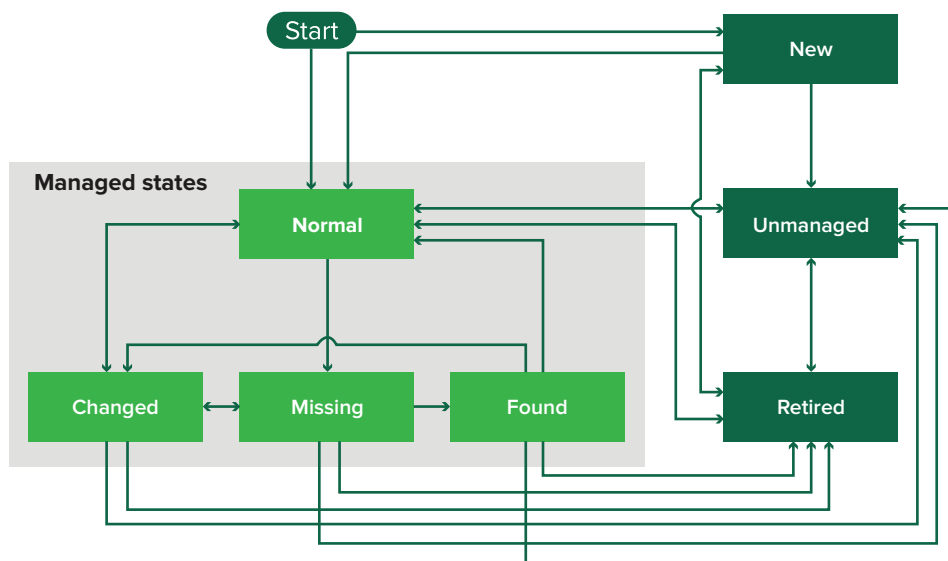
Beginning state	Ending state	Transition
Start	Normal	Discovered.[1]
Start	New	Discovered.[2]
Any	Normal, Unmanaged, or Retired	Manual (Missing does not change to Normal).
[1] The "Automatically manage discovered printers" setting is enabled in the discovery profile.		
[2] The "Automatically manage discovered printers" setting is disabled in the discovery profile.		

| Beginning state	Ending state	Transition
Retired	Normal	Discovered.[1]
Retired	New	Discovered.[2]
Normal, Missing, or Found	Changed	New address when discovered.
Normal	Changed	Audit properties do not match the database properties.
Normal, Changed, or Found	Missing	Not found on audit or update status.
Changed	Normal	Audit properties match the database properties.
Missing	Found	Discovered, audit, or update status.
Found	Normal	Discovered, audit, or update status.
[1] The "Automatically manage discovered printers" setting is enabled in the discovery profile.		
[2] The "Automatically manage discovered printers" setting is disabled in the discovery profile.		

Running a saved search

A saved search is a saved set of parameters that returns the latest printer information that meets the parameters.

You can create and run a customized saved search, or run the default system-generated saved searches. The system-generated saved searches show the printers in their life cycle states. For more information, see .

1 From the Printers menu, click **Printer Listing**.

2 In the drop-down menu, select a saved search.
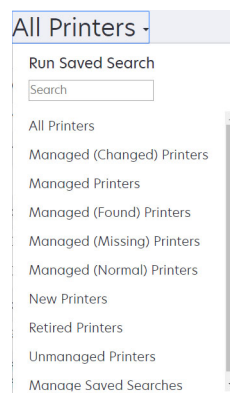
Creating a saved search

Using filters

1 From the Printers menu, click **Printer Listing**.

2 On the left side of the page, select the filters.

   Note: The selected filters are listed above the search results header.
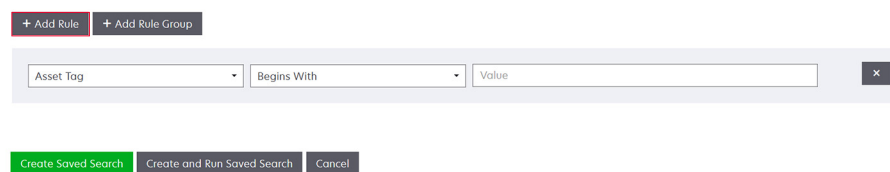
3 Click **Save**, and then type a unique name for your saved search and its description.

4 Click **Create Saved Search**.

Using the Saved Search page

1 From the Printers menu, click **Saved Searches** > **Create**.

2 From the General section, type a unique name for your saved search and its description.

3 From the Rules and Rule Groups section, in the Match menu, specify whether the search results must match all or any of the rules.

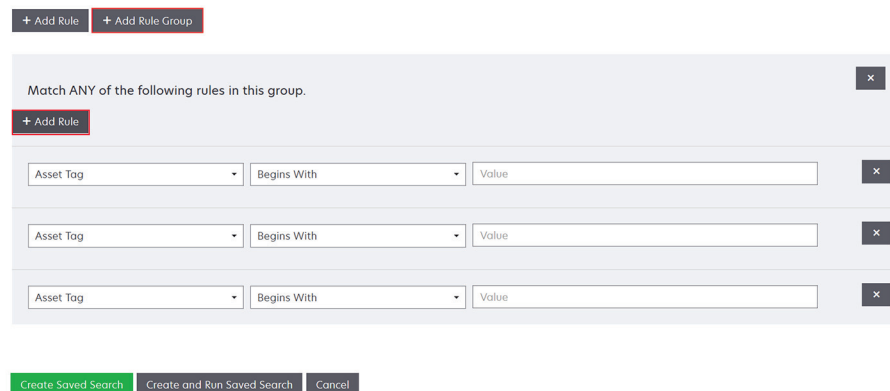**4** Do either of the following:

Add a rule

a Click **Add Rule**.

b Specify the parameter, operation, and value for your search rule. For more information, see "Understanding search rules settings" on page 46.

Add a rule group

A rule group may contain a combination of rules. If the Match menu is set to **ANY rules and rule groups**, then the system searches for printers that match all the rules in the rule group. If the Match menu is set to **ALL rules and rule groups**, then the system searches for printers that match any of the rules in the rule group.

a Click **Add Rule Group**.

b Specify the parameter, operation, and value for your search rule. For more information, see "Understanding search rules settings" on page 46.

c To add another rule, click **Add Rule**.

5 Click **Create Saved Search** or **Create and Run Saved Search**.

Understanding search rules settings

Search for printers using one or more of the following parameters:

Parameter	Description
Asset Tag	The value of the asset tag setting on the printer.
Certificate Creation Date	The date that the certificate was created.
Certificate Enrolment Status	The enrolment status of the certificate.
Certificate Expiration Date	The date that the certificate expires.
Certificate Renewal Date	The date that the certificate is renewed.
Certificate Revision Number	The revision number of the certificate.
Certificate Signing Status	The status of the certificate.
Certificate Validity Status	The validity of the certificate. **Note:** An Expiring Soon status indicates that the certificate expires within 30 days.
Color Capability	The printer prints in color or in black and white.
Configuration	The configuration name assigned to the printer.
Configuration Conformance	The conformance status of the printer against the assigned configuration.
Contact Location	The value of the contact location setting on the printer.
Contact Name	The value of the contact name setting on the printer.
Copy	The printer supports the copy function.
Date: Added to System	The date that the printer was added to the system.
Date: Last Audited	The date that the printer was last audited.
Date: Last Conformance Check	The date that the printer configuration conformance was last checked.
Date: Last Discovered	The date that the printer was last discovered.
Disk Encryption	The printer is configured for disk encryption.
Disk Wiping	The printer is configured for disk wiping.
Duplex	The printer supports two-sided printing.
eSF Capability	The printer supports managing eSF applications.
eSF Information	The information about the eSF application installed on the printer, such as name, state, and version.
Event Name	The name of the assigned events.
Fax Name	The value of the fax name setting on the printer.
Fax Number	The value of the fax number setting on the printer.
Fax Receive	The printer supports receiving fax.

Parameter	Description
Firmware Information	The information about the firmware installed on the printer. • **Name**—The name of the firmware. For example, **Base** or **Kernel**. • **Version**—The printer firmware version.
Host Name	The printer host name.
IP Address	The printer IP address. **Note:** You can use an asterisk in the last three octets to search for multiple entries. For example, **123.123.123.***, **123.123.*.***, **123.*.*.***, **2001:db8::2:1**, and **2001:db8:0:0:0:0:2:1**.
Keyword	The assigned keywords.
Lifetime Page Count	The lifetime page count value of the printer.
MAC Address	The printer MAC address.
Maintenance Counter	The value of the printer maintenance counter.
Manufacturer	The printer manufacturer name.
Marking Technology	The marking technology that the printer supports.
MFP Capability	The printer is a multifunction product (MFP).
Model	The printer model name.
Modular Serial Number	The modular serial number.
Printer Status	The printer status. For example, **Ready**, **Paper Jam**, **Tray 1 Missing**.
Printer Status Severity	The value of the most severe status present on the printer. For example, **Unknown**, **Ready**, **Warning**, or **Error**.
Profile	The printer supports profiles.
Scan to E-mail	The printer supports Scan to E-mail.
Scan to Fax	The printer supports Scan to Fax.
Scan to Network	The printer supports Scan to Network.
Secure Communication State	The printer security or authentication state.
Serial Number	The printer serial number.
State	The current printer state in the database.
Supply Status	The printer supplies status.
Supply Status Severity	The value of the most severe supply status present on the printer. For example, **Unknown**, **OK**, **Warning**, or **Error**.
System Name	The printer system name.
Time Zone	The time zone of the region where the printer is located.
TLI	The value of the TLI setting on the printer.

Use the following operators when searching for printers:

• **Exactly Matches**—A parameter is equivalent to a specified value.
• **Is Not**—A parameter is not equivalent to a specified value.

- **Contains**—A parameter contains a specified value.
- **Does Not Contain**—A parameter does not contain a specified value.
- **Begins With**—A parameter begins with a specified value.
- **Ends With**—A parameter ends with a specified value.

Note: To search for printers that have parameters with empty values, use **_EMPTY_OR_NULL_**. For example, to search for printers that have empty Fax Name, in the Value field, type **_EMPTY_OR_NULL_**.

Managing saved searches

1 From the Printers menu, click **Saved Searches**.

2 Do any of the following:

Edit a saved search

a Select a saved search, and then click **Edit**.

  Note: System-generated saved searches cannot be edited. For more information, see "Understanding printer life cycle states" on page 42.

b Configure the settings.

c Click **Save Changes** or **Save and Run**.

Copy a saved search

a Select a saved search, and then click **Copy**.

b Configure the settings.

c Click **Create Saved Search** or **Create and Run Saved Search**.

Delete saved searches

a Select one or more saved searches.

  Note: System-generated saved searches cannot be deleted. For more information, see "Understanding printer life cycle states" on page 42.

b Click **Delete**, and then confirm deletion.

Sample scenario: Monitoring the toner levels of your fleet

As the IT personnel of Company ABC, you must organize the printer fleet to monitor them easily. You want to monitor the toner usage of the printers to determine whether the supplies need replacement.

Sample implementation

1 Create a saved search that retrieves the printers whose supplies have errors or warnings.

  Sample rule for your saved search
    Parameter: **Supply Status Severity**
    Operation: **Is Not**
    Value: **Supplies OK**

2 Create a view that shows the supply status, capacity, and level for each printer.

Sample columns to show in your supplies view

Supply Status
Black Cartridge Capacity
Black Cartridge Level
Cyan Cartridge Capacity
Cyan Cartridge Level
Magenta Cartridge Capacity
Magenta Cartridge Level
Yellow Cartridge Capacity
Yellow Cartridge Level

3 Run the saved search while using the view.

Note: The information shown in the printer listing view is based on the last audit. Perform an audit and status update to get the current printer status.

Securing printer communications

Understanding printer security states

During discovery, the printer can be in any of the following security states:

- **Unsecured**—MVE does not need credentials to communicate with the device.
- **Secured**—MVE needs credentials and they were provided.
- **Missing credentials**—MVE needs credentials but they were not provided.
- **Invalid credentials**—MVE needs credentials but incorrect credentials were provided.
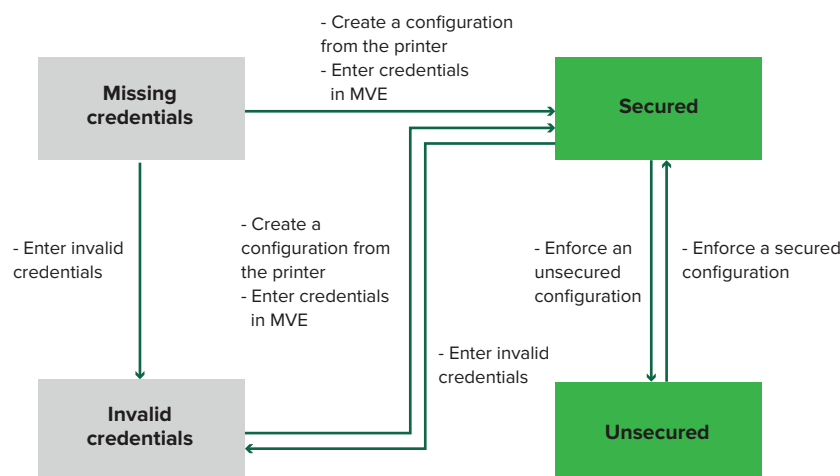
A printer is in the Invalid credentials state when the credentials are found to be invalid during discovery, audit, status update, conformance check, or configuration enforcement.

The printer is in an Unsecured state only when it does not require credentials during discovery.
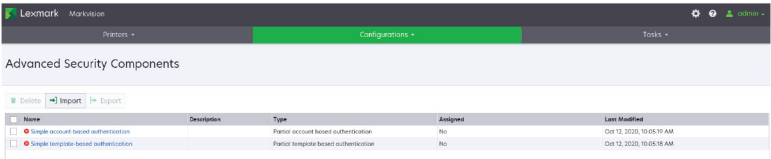
To change the status from Unsecured to Secured, enforce a secured configuration.

To move a printer from the Missing credentials or Invalid credentials state, enter the credentials in MVE manually or create a configuration from the printer.

Securing printers using the default configurations

On some printer models, there is no default administrator user. The Guest user has open access and is not logged in. This setup grants the user access to all printer permissions and access controls. MVE handles this risk through default configurations. After a fresh installation, two advanced security components are created automatically. Each component contains the default security settings and preconfigured local administrator account. You can use these security components when creating a configuration, and then deploy and enforce the configuration to the new printers.
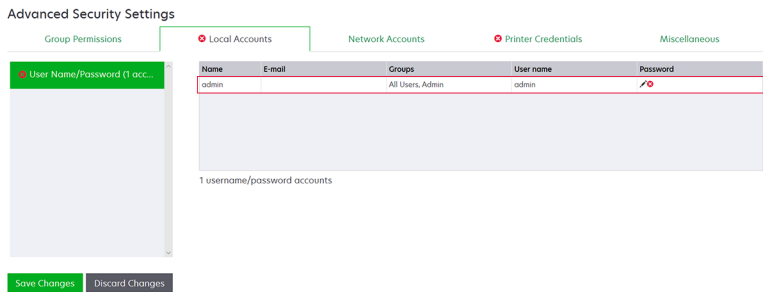
From the Configurations menu, click **All Advanced Security Components**.

Simple account-based authentication
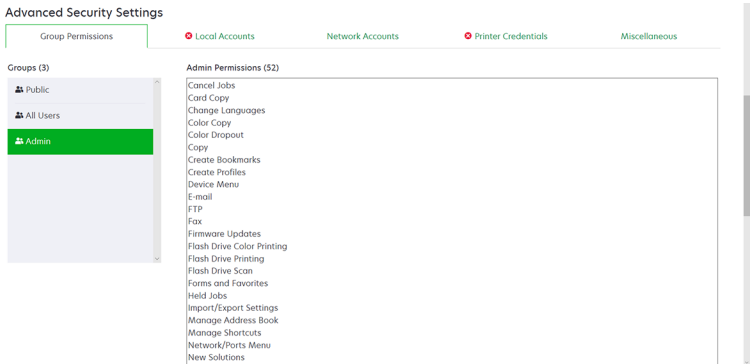
This security component contains a User Name/Password Local Account called **admin**.

The **admin** account is a member of the Admin Group, whose permissions include function access controls and permissions to secure the printer and restrict public access. For more information, see "Understanding permissions and function access controls" on page 53.

Before adding this component to a configuration, make sure to set the **admin** password and the printer credentials.

Simple template-based authentication

This security component contains a security template called Admin Password Protected that is configured with a Password Local Account.

This security template is applied to the following access controls:

- Firmware Updates
- Remote Management
- Security Menu remotely

The remaining access controls are set to **No Security**. However, you can always set the other administrative printer menus to use the security template for more protection. For more information on the access controls, see .

Before adding this component to a configuration, make sure to set the password and the printer credentials.

Understanding permissions and function access controls

Printers can be configured to restrict public access to administrative menus and device management features. In newer printer models, permissions to access printer functions can be secured through different types of authentication methods. In older printer models, a security template can be applied to a function access control (FAC).

To communicate with these secured printers and manage them, MVE requires certain permissions or FACs, depending on the printer model.

The following table explains what printer management functions can be managed in MVE and what permissions or FACs are required.

Note that MVE requires the authentication credentials when Remote Management is secured. If other administrative menus and device management permissions or FACs are secured, then Remote Management must also be secured. Otherwise, MVE cannot perform the functions.

These permissions and function access controls are predefined in MVE as default advanced security components, and can readily be used in a configuration. For more information, see "Securing printers using the default configurations" on page 51.

If you are not using the default advanced security components, then make sure that these permissions and function access controls are configured in the printer manually. For more information, see "Configuring printer security" on page 53.

Permissions or FACs	Description
Remote Management	The ability to read and write settings remotely. If any other permissions or FACs listed in this table are secured, then Remote Management must also be secured.
Firmware Updates	The ability to update firmware from any method.
Apps Configuration	The ability to install or remove applications from the printer and send application settings files to the printer.
Import / Export All Settings or **Configuration File Import / Export**	The ability to send configuration files to the printer.
Security Menu or **Security Menu Remotely**	The ability to manage login methods and configure printer security options.

To secure newer printer models in MVE, disable public access for the Remote Management and Security Menu permissions. For older printer models, apply a security template to the Remote Management FAC.

Configuring printer security

1 From the Printers menu, click **Printer Listing**.

2 Click the IP address of the printer, and then click **Open Embedded Web Server**.

3 Click **Settings** or **Configuration**.

4 Depending on your printer model, do either of the following:

- Click **Security** > **Login Methods**, and then do the following:

For newer printer models

a From the Security section, create a login method.

b Click **Manage Group/Permissions** or **Manage Permissions** beside the login method.

c Expand **Administrative Menus**, and then select **Security Menu**.

d Expand **Device Management**, and then select the following permissions:

- **Remote Management**
- **Firmware Updates**
- **Apps Configuration**
- **Import / Export All Settings**

e Click **Save**.

f From the Public section, click **Manage Permissions**.

g Expand **Administrative Menus**, and then clear **Security Menu**.

h Expand **Device Management**, and then clear **Remote Management**.

i Click **Save**.

- Click **Security** > **Security Setup** or **Edit Security Setup**, and then do the following:

For older printer models

a From the Advanced Security Setup section, create a building block and a security template.

b Click **Access Controls**, and then expand **Administrative Menus**.

c In the Security Menu Remotely menu, select the security template.

d Expand **Management**, and then select the security template for the following function access controls:

- **Apps Configuration**
- **Remote Management**
- **Firmware Updates**
- **Configuration File Import / Export**

e Click **Submit**.

Securing printer communications on your fleet

1 Discover a secured printer. For more information, see "Discovering printers" on page 32.

Notes:

- A printer is secured when ![lock] appears next to it. For information on securing a printer, see the **help document**.
- For more information on printer security states, see "Understanding printer security states" on page 50.

2 Create a configuration from a printer. For more information, see "Creating a configuration from a printer" on page 65.

3 Assign the configuration to your fleet. For more information, see "Assigning configurations to printers" on page 57.

4 Enforce the configuration. For more information, see "Enforcing configurations" on page 57. A padlock symbol appears next to the secured printer.

Other ways to secure your printers

For more information on configuring printer security settings, see the *Embedded Web Server Administrator's Guide* for your printer.

Check your printers for the following settings:
- Disk encryption is enabled.
- The following ports are restricted:
  - TCP 79 (Finger)
  - TCP 21 (FTP)
  - UDP 69 (TFTP)
  - TCP 5001 (IPDS)
  - TCP 9600 (IPDS)
  - TCP 10000 (Telnet)
- The default cipher list is the OWASP Cipher String 'B.'

Managing printers

Restarting the printer

1 From the Printers menu, click **Printer Listing**.

2 Click the IP address of the printer.

3 Click **Restart Printer**.

Viewing the printer Embedded Web Server

The Embedded Web Server is a software built into the printer that provides a control panel for configuring the printer from any web browser.

1 From the Printers menu, click **Printer Listing**.

2 Click the IP address of the printer.

3 Click **Open Embedded Web Server**.

Auditing printers

An audit collects information from any printers in the Managed state, and then stores the information in the system. To make sure that the information in the system is current, perform an audit regularly.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Printer** > **Audit**.

Note: An audit can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.

Updating printer status

The Update Status feature lets you update the printer status and supplies information. To make sure that the printer status and supplies information is current, update the status regularly.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Printer** > **Update status**.

Note: A status update can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.

Setting the printer state

For more information on the printer states, see "Understanding printer life cycle states" on page 42.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Printer**, and then select one of the following:

- **Set state to managed**—The printer is included in all activities that can be performed in the system.
- **Set state to unmanaged**—The printer is excluded in all activities that can be performed in the system.
- **Set state to retired**—The printer is removed from the network. The system retains the printer information, but does not expect to see the printer on the network again.

Assigning configurations to printers

Before you begin, make sure that a configuration for the printer is created. Assigning a configuration to a printer allows the system to run conformance checks and enforcements. For more information, see "Creating a configuration" on page 63.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Assign configurations**.

4 From the Configuration section, select a configuration.

Note: If the system is set to **Use Markvision to manage device certificates**, then select **Trust the selected devices**. This confirmation is the way for the user to verify that the printers are real devices and not spoofed.

5 Click **Assign Configurations**.

Unassigning configurations

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Unassign configurations**.

4 Click **Unassign Configurations**.

Enforcing configurations

MVE runs a conformance check against the printer. If some settings are out of conformance, then MVE changes those settings on the printer. MVE runs a final conformance check after changing the settings. Updates that require the printer to reboot, such as firmware updates, may require a second enforcement to complete.

Before you begin, make sure that a configuration is assigned to the printer. For more information, see "Assigning configurations to printers" on page 57.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Enforce configurations**.

Notes:

- If the printer is in an error state, then some settings may not be updated.
- For MVE to deploy firmware and solution files to a printer, the Firmware Updates function access control must be set to **No Security**. If security is applied, then the Firmware Updates function access control must use the same security template as the Remote Management function access control. For more information, see "Deploying files to printers" on page 58.
- An enforcement can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.

Checking the printer conformance with a configuration

During a conformance check, MVE checks the printer settings, and verifies whether they match the assigned configuration. MVE does not make changes to the printer during this operation.

Before you begin, make sure that a configuration is assigned to the printer. For more information, see "Assigning configurations to printers" on page 57.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Check conformance**.

   Notes:

   - You can view the results in the task status page.
   - A conformance check can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.

Deploying files to printers

You can deploy the following files to the printer:

- **CA Certificates**—**.cer** or **.pem** files that are added to the printer trust store.
- **Configuration bundle**—**.zip** files that are exported from a supported printer or obtained directly from Lexmark.
- **Firmware update**—An **.fls** file that is flashed to the printer.
- **Generic file**—Any file that you want to send to the printer.
  - **Raw socket**—Sent over port 9100. The printer treats it like any other print data.
  - **FTP**—Send file over FTP. This deployment method is not supported on secured printers.
- **Printer certificate**—A signed certificate that is installed on the printer as the default certificate.

- **Universal Configuration File (UCF)**—A configuration file exported from a printer.
  - **Web service**—The HTTPS web service is used when the printer model supports it. Otherwise, the printer uses the HTTP web service.
  - **FTP**—Send file over FTP. This deployment method is not supported on secured printers.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Deploy file to printers**.

4 Click **Choose File**, and then browse to the file.

5 Select a file type, and then select a deployment method.

6 Click **Deploy File**.

Notes:

- For MVE to deploy firmware and solution files to a printer, the Firmware Updates function access control must be set to **No Security**. If security is applied, then the Firmware Updates function access control must use the same security template as the Remote Management function access control.
- A file deployment can be scheduled to occur regularly. For more information, see "Creating a schedule" on page 105.

Updating the printer firmware

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Update firmware to printers**.

4 Select a firmware file from the resource library, or click **Choose File**, and then browse to the firmware file.

   Note: For more information on adding firmware files to the library, see "Importing files to the resource library" on page 69.

5 If necessary, to schedule the update, select **Define update window**, and then select the start date, start and pause time, and days of the week.

   Note: The firmware is sent to the printers within the specified start time and pause time. The task is paused after the pause time, and then resumes at the next start time until it is completed.

6 Click **Update Firmware**.

Note: For MVE to update the printer firmware, the Firmware Updates function access control must be set to **No Security**. If security is applied, then the Firmware Updates function access control must use the same security template as the Remote Management function access control. In this case, MVE must manage the printer securely. For more information, see "Securing printer communications" on page 50.

Uninstalling applications from printers

MVE can uninstall only applications that have been added to the system. For more information on uploading applications to the system, see .

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Configure** > **Uninstall Apps from printers**.

4 Select the applications.

5 Click **Uninstall Apps**.

Assigning events to printers

Assigning events to printers lets MVE perform the associated action whenever one of the associated alerts occurs on the assigned printer. For more information on creating events, see .

Note: Events can be assigned only to unsecured printers.

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Assign** > **Events**.

4 Select one or more events.

   Note: If some of the selected printers already have the event assigned to them, then a dash in the check box appears. If you leave it as a dash, then the event does not change. If you select the check box, then the event is assigned to all the selected printers. If you clear the check box, then the event is unassigned from the printers it was previously assigned to.

5 Click **Assign Events**.

Assigning keywords to printers

Assigning keywords to printers lets you organize your printers. For more information on creating keywords, see .

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Assign** > **Keywords**.

4 If necessary, in the View menu, select a category.

5 Select one or more keywords.

Note: Keywords are listed following a category. If some of the selected printers already have the keyword assigned to them, then a dash in the check box appears. If you leave it as a dash, then the keyword is not assigned or unassigned to the selected printers. If you select the check box, then the keyword is assigned to all the selected printers. If you clear the check box, then the keyword is unassigned from the printers it was previously assigned to.

6 Click **Assign Keywords**.

Entering credentials to secured printers

Secured printers can be discovered and enrolled. To communicate with these printers, you can either enforce a configuration or enter the credentials in MVE directly.

Note: A printer is secured when a 🔒 appears next to it.

To enter the credentials, do the following:

1 From the Printers menu, click **Printer Listing**.

2 Select one or more secured printers.

3 Click **Security** > **Enter Credentials**.

4 Select the authentication method, and then enter the credentials.

5 Click **Enter Credentials**.

Note: Enrolled printers that are secured but do not have the correct credentials saved in MVE are tagged as Missing credentials under the Communications filter. After the correct credentials are entered, the printers are tagged as Secured.

Configuring printer certificates manually

When not using the automated certificate management feature, MVE can help facilitate the process of signing the default printer certificate on a fleet of printers. MVE gathers the certificate signing requests from the fleet, and then deploys the signed certificates to the proper printers after they are signed.

A system administrator must do the following:

1 Generate the printer certificate signing requests.

    a From the Printers menu, click **Printer Listing**.

    b Select one or more printers.

    c Click **Security** > **Generate printer certificate signing requests**.

Note: This process lets only one printer certificate signing request to exist on the server at a time. If another request is generated, then the previous request is overwritten. Make sure to download the existing request before generating a new one.

2 Wait for the task to finish, and then download the printer certificate signing requests.

    a From the Printers menu, click **Printer Listing**.

    b Click **Security** > **Download printer certificate signing requests**.

3 Use a trusted CA to sign the certificate signing requests.

4 Save the signed certificates in a ZIP file.

Note: All the signed certificates must be in the root location of the ZIP file. Otherwise, MVE cannot parse the file.

5 From the Printers menu, click **Printer Listing**.

6 Select one or more printers.

7 Click **Configure** > **Deploy file to printers**.

8 Click **Choose File**, and then browse to the ZIP file.

9 In the File type menu, select **Printer Certificates**.

10 Click **Deploy File**.

Removing printers

1 From the Printers menu, click **Printer Listing**.

2 Select one or more printers.

3 Click **Printer**.

4 If necessary, to remove the printer certificate, select **Delete device default certificate(s)**.

Note: Removing a printer from MVE only deletes the certificate from MVE, and does not affect the CA server.

5 Do either of the following:

- To retain the printer information, click **Retire Printer**.
- To remove the printer from the system, click **Delete Printer**.

Managing configurations

Overview

MVE uses configurations to manage the printers in your fleet.

A configuration is a collection of settings that can be assigned and enforced to a printer or a group of printer models. Within a configuration, you can modify printer settings and deploy applications, licenses, firmware, and printer certificates.

You can create a configuration that is composed of the following:

- Basic printer settings
- Advanced security settings
- Color print permissions

  Note: This setting is available only in configurations for supported color printers.

- Printer firmware
- Applications
- CA certificates

Using configurations, you can do the following to manage the printers:

- Assign a configuration to printers.
- Enforce the configuration to the printers. The settings that are specified in the configuration are applied to the printers, and the firmware, applications, and CA certificates are installed.
- Check whether the printers are in conformance against a configuration. If a printer is out of conformance, then the configuration can be enforced to the printer.

  Note: Configuration enforcement and conformance checking can be scheduled to occur regularly.

- If the printer supports the configuration settings but the values are not supported, then the printer shows as out of conformance.

Creating a configuration

A configuration is a collection of settings that can be assigned and enforced to a printer or a group of printer models. Within a configuration, you can modify printer settings and deploy applications, licenses, firmware, and CA certificates to printers.

1 From the Configurations menu, click **All Configurations** > **Create**.

2 Type a unique name for the configuration and its description.

3 Do one or more of the following:

- From the Basic tab, in the Setting list, select one or more settings, and then specify the values. If the value is a variable setting, then enclose the header with `${}`. For example, `${Contact_Name}`. To use a variable setting file, select the file from the Use variable setting data file menu, or import the file. For more information, see "Understanding variable settings" on page 67.

- From the Advanced Security tab, select an advanced security component.

    Notes:

    – To create an advanced security component, see "Creating an advanced security component from a printer" on page 66.

    – You can manage the advanced security settings only when creating a configuration from a selected printer. For more information, see "Creating a configuration from a printer" on page 65.

- From the Color Print Permissions tab, configure the settings. For more information, see "Configuring the color print permissions" on page 67.

    Note: This setting is available only in configurations for supported color printers.

- From the Firmware tab, select a firmware file. To import a firmware file, see "Importing files to the resource library" on page 69.

- From the Apps tab, select one or more applications to deploy. For more information, see "Creating an applications package" on page 68.

    Note: MVE does not support deploying applications with trial licenses. You can deploy only free applications or applications with production licenses.

- From the Certificates tab, select one or more certificates to deploy. To import a certificate file, see "Importing files to the resource library" on page 69.

    Note: Select **Use Markvision to manage device certificates** for MVE to assess missing, invalid, revoked, and expired certificates, and then replace them automatically. For more information, see "Configuring MVE for automated certificate management" on page 71.

4 Click **Create Configuration**.

Sample scenario: Deploying a configuration to printers

Company ABC has more than 50 Lexmark MX710 printers. As the IT personnel, you must set the tray paper size to **Letter**.

Note: You can also deploy a configuration to a group of printer models.

Sample implementation

1 Create a configuration for Lexmark MX710.

2 From the Basic tab, set Tray Paper Size to **Letter**.

3 Filter the printer listing view or use a saved search that shows the Lexmark MX710 printers.

4 Assign, and then enforce the configuration to the printers.

Creating a configuration from a printer

The following components are not included:
- Printer firmware
- Applications
- Certificates

To add the firmware, applications, and certificates, edit the configuration in MVE.

1 From the Printers menu, click **Printer Listing**.

2 Select the printer, and then click **Configure** > **Create configuration from printer**.

3 If necessary, select **Include advanced security settings** to create an advanced security component from the selected printer.

4 If the printer is secured, then select the authentication method, and then enter the credentials.

5 Type a unique name for the configuration and its description, and then click **Create Configuration**.

6 From the Configurations menu, click **All Configurations**.

7 Select the configuration, and then click **Edit**.

8 If necessary, edit the settings.

9 Click **Save Changes**.

Sample scenario: Cloning a configuration

Fifteen Lexmark MX812 printers were added to the system after discovery. As the IT personnel, you must apply the settings of the existing printers to the newly discovered printers.

Note: You can also clone a configuration from a printer, and then enforce the configuration to a group of printer models.

Sample implementation

1 From the existing printers list, select a Lexmark MX812 printer.

2 Create a configuration from the printer.

   Note: To secure the printers, include the advanced security settings.

3 Assign, and then enforce the configuration to the newly discovered printers.

Creating an advanced security component from a printer

Create an advanced security component from a printer to manage the advanced security settings. MVE reads all the settings from that printer, and then creates a component that includes the settings. The component can be associated to multiple configurations for printer models that have the same security framework.

1 From the Printers menu, click **Printer Listing**.

2 Select the printer, and then click **Configure** > **Create advanced security component from printer**.

3 Type a unique name for the component and its description.

4 If the printer is secured, then select the authentication method, and then enter the credentials.

5 Click **Create Component**.

   Note: When you create and enforce a configuration with an advanced security component that contains local accounts, the local accounts are added to the printers. Any existing local accounts that are preconfigured in the printer are retained.

Generating a printable version of the configuration settings

1 Edit a configuration or advanced security component.

2 Click **Printer-friendly version**.

Understanding variable settings

Variable settings let you manage settings across your fleet that are unique to each printer, such as host name or asset tag. When creating or editing a configuration, you can select a CSV file to be associated with the configuration.

Sample CSV format:

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

In the header row of the variable file, the first column is a unique printer identifier token. The token must be one of the following:

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

Each subsequent column in the header row of the variable file is a user-defined replacement token. This token must be referenced within the configuration using the ${HEADER} format. It is replaced with the values in the subsequent rows when the configuration is enforced. Make sure that the tokens do not contain any spaces.

You can import the CSV file containing the variable settings when creating or editing a configuration. For more information, see .

Configuring the color print permissions

MVE lets you restrict color printing for host computers and specific users.

Note: This setting is available only in configurations for supported color printers.

1 From the Configurations menu, click **All Configurations**.

2 Create or edit a configuration.

3 From the Color Print Permissions tab, do either of the following:

Configure the color print permissions for host computers

a In the View menu, select **Host computers**, and then select **Include color print permissions for host computers**.

b Click **Add**, and then type the host computer name.

c To let the host computer print in color, select **Allow color printing**.

d To let users that log in to the host computer print in color, select **Override user permission**.

e Click **Save and Add** or **Save**.

Configure the color print permissions for users

a In the View menu, select **Users**, and then select **Include color print permissions for users**.

b Click **Add**, and then type the user name.

c Select **Allow color printing**.

d Click **Save and Add** or **Save**.

Creating an applications package

1 Export the Printer List view from MVE using the Export Data feature.

a From the Printers menu, click **Views**.

b Select **Printer List**, and then click **Export Data**.

c Select a saved search.

d In the "Select file type for data export" menu, select **CSV**.

e Click **Export Data**.

2 Access Package Builder.

Note: If you need access to Package Builder, then contact your Lexmark representative.

a Log in to Package Builder at **cdp.lexmark.com/package-builder**.

b Import the printer list, and then click **Next**.

c Type the package description, and then type your e‑mail address.

d In the Product menu, select the applications, and then if necessary, add licenses.

e Click **Next** > **Finish**. The package download link is sent to your e‑mail.

3 Download the package.

Notes:

- MVE does not support deploying applications with trial licenses. You can deploy only free applications or applications with production licenses. If you need activation codes, then contact your Lexmark representative.
- To add the applications to a configuration, import the applications package to the resource library. For more information, see .

Importing or exporting a configuration

Before you begin, when importing a configuration file, make sure that it is exported from an MVE of the same version.

1 From the Configurations menu, click **All Configurations**.

2 Do either of the following:

- To import a configuration file, click **Import**, browse to the configuration file, and then click **Import**.
- To export a configuration file, select a configuration, and then click **Export**.

Note: When exporting a configuration, the passwords are excluded. After importing, manually add the passwords.

Importing files to the resource library

The resource library is a collection of firmware files, CA certificates, and application packages that are imported to MVE. These files can be associated with one or more configurations.

1 From the Configurations menu, click **Resource Library**.

2 Click **Import** > **Choose File**, and then browse to the file.

Note: Only firmware files (.fls), application packages or configuration bundles (.zip), CA certificates (.pem), and universal configuration files (.ucf) can be imported.

3 Click **Import Resource**.

Managing certificates

Setting up MVE to manage certificates automatically

Understanding the automated certificate management feature

You can configure MVE to manage printer certificates automatically, and then install them to the printers through configuration enforcement. The following diagram describes the end-to-end process of the automated certificate management feature.
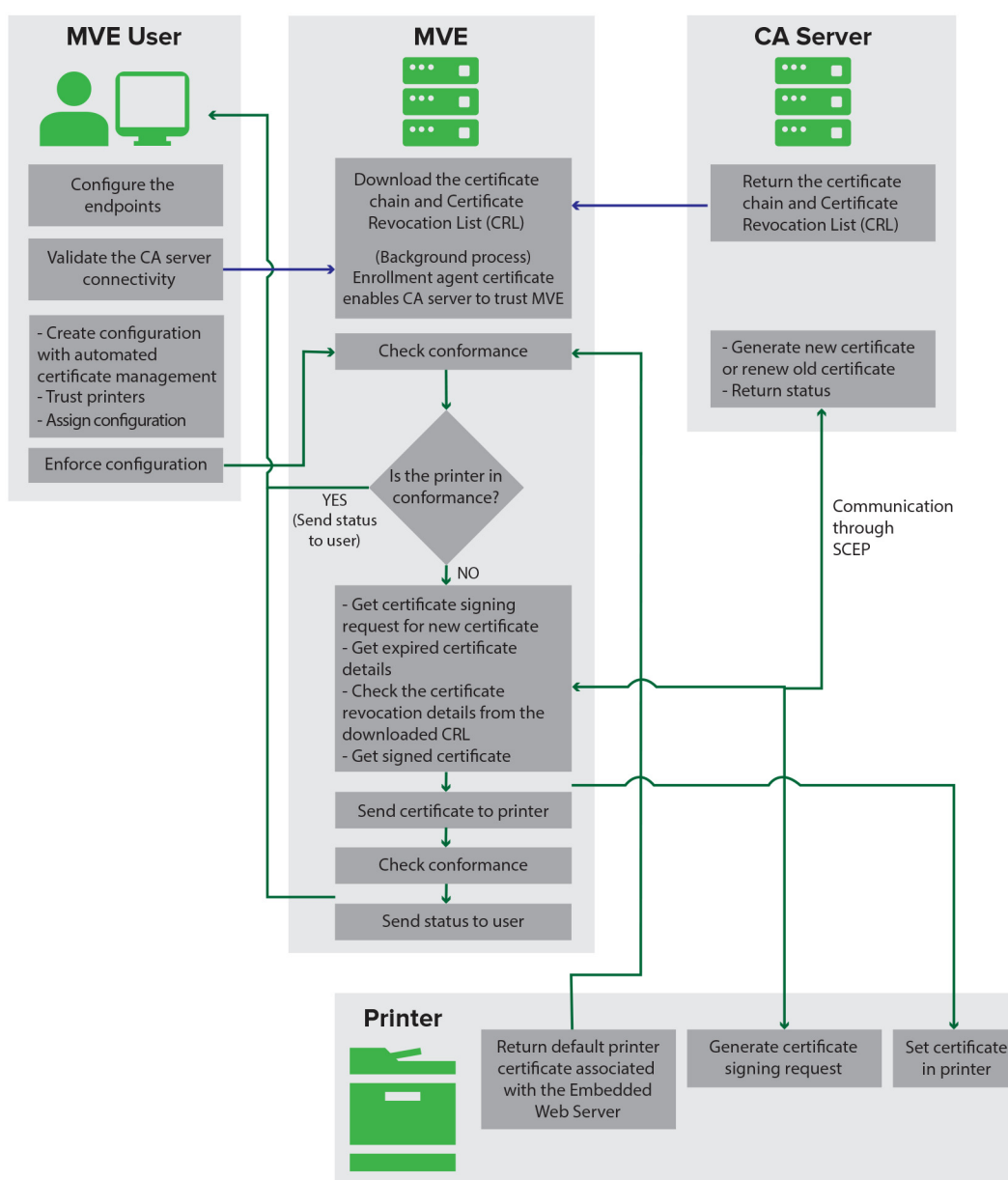
The certificate authority endpoints, such as the CA server and server address, must be defined in MVE.

The following CA servers are supported:

- **OpenXPKI CA**—For more information, see <u>"Managing certificates using OpenXPKI Certificate Authority" on page 78</u>.
- **Microsoft CA Enterprise**—For more information, see <u>"Managing certificates using Microsoft Certificate Authority" on page 72</u>.

The connection between MVE and the CA servers must be validated. During validation, MVE communicates with the CA server to download the certificate chain and the Certificate Revocation List (CRL). The enrolment agent certificate is also generated. This certificate enables the CA server to trust MVE.

For more information on defining the endpoints and validation, see <u>"Configuring MVE for automated certificate management" on page 71</u>.

A configuration that is set to **Use Markvision to manage device certificates** must be assigned and enforced to the printer.

For more information, see the following topics:

- <u>"Creating a configuration" on page 63</u>
- <u>"Enforcing configurations" on page 57</u>

During enforcement, MVE checks the printer for conformance. The default printer certificate is validated against the certificate chain downloaded from the CA server. If the printer is out of conformance, a certificate signing request (CSR) is requested for the printer. MVE communicates with the CA server through the Simple Certificate Enrollment Protocol (SCEP). The CA server generates the new certificate, and then MVE sends the certificate to the printer.

Configuring MVE for automated certificate management

1 Click ![gear icon] on the upper-right corner of the page.

2 Click **Certificate Authority** > **Use Certificate Authority Server**.

   Note: The Use Certificate Authority Server button appears only when configuring the certificate authority for the first time, or when the certificate is deleted.

3 Configure the server endpoints.

   - **CA Server**—The Certificate Authority (CA) server that generates the printer certificates. You can select either OpenXPKI CA or Microsoft CA Enterprise.
   - **CA Server Address**—The IP address or host name of your CA server. Include the full URL.
   - **Challenge Password**—The password that is required to assert the identity of MVE to the CA server. The challenge password is not supported in Microsoft CA Enterprise.

   Note: Depending on your CA server, see <u>"Managing certificates using OpenXPKI Certificate Authority" on page 78</u> or <u>"Managing certificates using Microsoft Certificate Authority" on page 72</u>.

4 Click **Save Changes and Validate** > **OK**.

   Note: The connection between MVE and the CA servers must be validated. During validation, MVE communicates with the CA server to download the certificate chain and the Certificate Revocation List (CRL). The enrolment agent certificate is also generated. This certificate enables the CA server to trust MVE.

5 Navigate back to the System Configuration page, and then review the CA certificate.

   Note: You can also download or delete the CA certificate.

Managing certificates using Microsoft Certificate Authority

This section provides instructions on the following:

- Configuring Microsoft Enterprise Certificate Authority (CA) using Microsoft Network Device Enrollment Service (NDES)
- Create a root CA server

Note: The Windows Server 2016 operating system is used for all setups in this document.

Configuring root CA server

Overview

The root CA server is the main CA server in any organization, and is the top of the PKI infrastructure. The root CA authenticates the subordinate CA server. This server is generally kept in offline mode to prevent any intrusion and to secure the private key.

To configure the root CA server, do the following:

1 Make sure that the root CA server is installed. For more information, see <u>"Installing the root CA server" on page 72</u>.

2 Configure the Certification Distribution Point and Authority Information Access settings. For more information, see <u>"Configuring the Certification Distribution Point and Authority Information Access settings" on page 75</u>.

3 Configure the CRL accessibility. For more information, see <u>"Configuring CRL accessibility" on page 76</u>.

Installing the root CA server

1 From Server Manager, click **Manage > Add Roles and Feature**.

2 Click **Server Roles**, select **Active Directory Certificate Services** and all its features, and then click **Next**.

3 From the AD CS Role Services section, select **Certification Authority**, and then click **Next > Install**.

4 After installation, click **Configure Active Directory Certificate Services on the destination server**.

5 From the Role Services section, select **Certification Authority > Next**.

6 From the Setup Type section, select **Standalone CA**, and then click **Next**.

7 From the CA Type section, select **Root CA**, and then click **Next**.

8 Select **Create a new private key**, and then click **Next**.

9 From the Select a cryptographer provider menu, select **RSA#Microsoft Software Key Storage Provider**.

10 From the Key length menu, select **4096**.

11 In the hash algorithm list, select **SHA512**, and then click **Next**.

12 In the Common name for this CA field, type the hosting server name.

13 In the Distinguished name suffix field, type the domain component.

Sample CA name configuration

Machine Fully Qualified Domain Name (FQDN): `test.dev.lexmark.com`

Common Name (CN): `TEST`

Distinguished name suffix: `DC=DEV,DC=LEXMARK,DC=COM`

14 Click **Next**.

15 Specify the validity period, and then click **Next**.

Note: Generally, the validity period is 10 years.

16 Do not change anything in the database locations window.

17 Complete the installation.

Configuring Microsoft Enterprise CA with NDES

Overview

In the following deployment scenario, all permissions are based on permissions set on certificate templates that are published in the domain controller. The certificate requests sent to the CA are based on certificate templates.

For this setup, make sure that you have the following:

- A machine hosting the subordinate CA (may also be the root CA)
- A machine hosting the NDES service
- A domain controller

Required users

Create the following users in the domain controller:

- Service Administrator
  - Named as **SCEPAdmin**
  - Must be a member of the **local admin** and **Enterprise Admin** groups
  - Must be logged locally when the installation of NDES role is triggered
  - Has **Enroll permission** for the certificate templates
  - Has **Add template permission** on CA
- Service Account
  - Named as **SCEPSvc**
  - Must be member of the local **IIS_IUSRS** group
  - Must be a domain user and has **read** and **enroll** permissions on the configured templates
  - Has **request** permission on CA
- Device Administrator
  - Named as **DeviceAdmin**
  - Has **Enroll permission** on all templates configured in the registry

Configuring subordinate CA server

Overview

The subordinate CA server is the intermediate CA server and is always online. It generally handles the management of certificates.

To configure the subordinate CA server, do the following:

1 Make sure that the subordinate CA server is installed. For more information, see "Installing the subordinate CA server" on page 74.

2 Configure the Certification Distribution Point and Authority Information Access settings. For more information, see "Configuring the Certification Distribution Point and Authority Information Access settings" on page 75.

3 Configure the CRL accessibility. For more information, see "Configuring CRL accessibility" on page 76.

Installing the subordinate CA server

1 From the server, log in as an **SCEPAdmin** domain user.

2 From Server Manager, click **Manage** > **Add Roles and Feature**.

3 Click **Server Roles**, select **Active Directory Certificate Services** and all its features, and then click **Next**.

4 From the AD CS Role Services section, select **Certification Authority** and **Certificate Authority Web Enrollment**, and then click **Next**.

   Note: Make sure that all the features of Certificate Authority Web Enrollment are added.

5 From the Web Server Role (IIS) Role Services section, retain the default settings.

6 After installation, click **Configure Active Directory Certificate Services on the destination server**.

7 From the Role Services section, select **Certification Authority** and **Certificate Authority Web Enrollment**, and then click **Next**.

8 From the Setup Type section, select **Enterprise CA**, and then click **Next**.

9 From the CA Type section, select **Subordinate CA**, and then click **Next**.

10 Select **Create a new private key**, and then click **Next**.

11 From the Select a cryptographer provider menu, select **RSA#Microsoft Software Key Storage Provider**.

12 From the Key length menu, select **4096**.

13 In the hash algorithm list, select **SHA512**, and then click **Next**.

14 In the Common name for this CA field, type the host server name.

15 In the Distinguished name suffix field, type the domain component.

   Sample CA name configuration
   Machine Fully Qualified Domain Name (FQDN): `test.dev.lexmark.com`
   Common Name (CN): `TEST`
   Distinguished name suffix: `DC=DEV,DC=LEXMARK,DC=COM`

16 In the Certificate Request dialog box, save the request file, and then click **Next**.

17 Do not change anything in the database locations window.

18 Complete the installation.

19 Sign the CA request of the root CA, and then export the signed certificate in PKCS7 format.

20 From the subordinate CA, open **Certification Authority**.

21 From the left panel, right-click the CA, and then click **All Tasks** > **Install CA Certificate**.

22 Select the signed certificate, and then start the CA service.

Configuring the Certification Distribution Point and Authority Information Access settings

Note: Configure the Certification Distribution Point (CDP) and Authority Information Access (AIA) settings for Certificate Revocation List (CRL).

1 From Server Manager, click **Tools** > **Certification Authority**.

2 From the left panel, right-click the CA, and then click **Properties** > **Extensions**.

3 In the Select extension menu, select **CRL Distribution Point (CDP)**.

4 In the certificate revocation list, select the **C:\Windows\system32** entry, and then do the following:

   a Select **Publish CRLs to this location**.

   b Clear **Publish Delta CRLs to this location**.

5 Delete all other entries except for **C:\Windows\system32**.

6 Click **Add**.

7 In the Location field, add
http://*serverIP*/CertEnroll/<CAName><CRLNameSuffix><DeltaCRLAllowed>.crl, where ***serverIP*** is the IP address of the server.

   Note: If your server is reachable using the FQDN, then use the DNS of the server instead of its IP address.

8 Click **OK**.

9 Select **Include in the CDP extension of issued certificates** for the created entry.

10 In the Select extension menu, select **Authority Information Access (AIA)**.

11 Delete all other entries except for **C:\Windows\system32**.

12 Click **Add**.

13 In the Location field, add
http://*serverIP*/CertEnroll/<ServerDNSName>_<CAName><CertificateName>.crt, where ***serverIP*** is the IP address of the server.

   Note: If your server is reachable using the FQDN, then use the DNS of the server instead of its IP address.

14 Click **OK**.

15 Select **Include in the AIA extension of issued certificates** for the created entry.

16 Click **Apply** > **OK**.

   Note: If necessary, restart the certification service.

17 From the left panel, expand the CA, right-click **Revoked Certificates**, and then click **Properties**.

18 Specify the value for CRL publication interval and for Publish Delta CRLs Publication interval, and then click **Apply** > **OK**.

19 From the left panel, right-click **Revoked Certificates**, click **All Tasks**, and then publish the New CRL.

Configuring CRL accessibility

Note: Before you begin, make sure that Internet Information Services (IIS) Manager is installed.

1 From IIS Manager, expand the CA, and then expand **Sites**.

2 Right-click **Default Web Site**, and then click **Add Virtual Directory**.

3 In the Alias field, type **CertEnroll**.

4 In the Physical path field, type **C:\Windows\System32\CertSrv\CertEnroll**.

5 Click **OK**.

6 Right-click **CertEnroll**, and then click **Edit Permissions**.

7 From the Security tab, remove any write access except for the system.

8 Click **OK**.

Configuring the NDES server

1 From the server, log in as an **SCEPAdmin** domain user.

2 From Server Manager, click **Manage** > **Add Roles and Feature**.

3 Click **Server Roles**, select **Active Directory Certificate Services** and all its features, and then click **Next**.

4 From the AD CS Role Services section, clear **Certification Authority**.

5 Select **Network Device Enrollment Service** and all its features, and then click **Next**.

6 From the Web Server Role (IIS) Role Services section, retain the default settings.

7 After installation, click **Configure Active Directory Certificate Services on the destination server**.

8 From the Role Services section, select **Network Device Enrollment Service**, and then click **Next**.

9 Select the **SCEPSvc** service account.

10 From the CA for NDES section, select either **CA name** or **Computer name**, and then click **Next**.

11 From the RA Information section, specify the information, and then click **Next**.

12 From the Cryptography for NDES section, do the following:
   - Select the appropriate signature and encryption key providers.
   - From the Key length menu, select the same key length as the CA server.

13 Click **Next**.

14 Complete the installation.

You can now access the NDES server from a web browser as an SCEPSvc user. From the NDES server, you can view the CA certificate thumbprint, the enrollment challenge password, and the validity period of the challenge password.

Accessing the NDES server

Open a web browser, and then type **http://*NDESserverIP*/certsrv/mscep_admin**, where ***NDESserverIP*** is the IP address of the NDES server.

Configuring NDES for MVE

Note: Before you begin, make sure that the NDES server is working properly.

Creating a certificate template

1 From the subordinate CA (certserv), open **Certification Authority**.

2 From the left panel, expand the CA, right-click **Certificate Templates**, and then click **Manage**.

3 In Certificate Templates Console, create a copy of **Web Server**.

4 From the General tab, type **MVEWebServer** as the template name.

5 From the Security tab, give the **SCEPAdmin** and **SCEPSvc** users the appropriate permissions.

> **Note:** For more information, see <u>"Required users" on page 73</u>.

6 From the Subject Name tab, select **Supply in the request**.

7 From the subordinate CA (certserv), open **Certification Authority**.

8 From the Extensions tab, select **Application Policies > Edit**.

9 Click **Add >Client Authentication > OK**.

10 From the left panel, expand the CA, right-click **Certificate Templates**, and then click **New > Certificate Template to Issue**.

11 Select the newly created certificates, and then click **OK**.

You can now access the templates using the CA web enrollment portal.

Accessing the templates

1 Open a web browser, and then type **http://*CAserverIP*/certsrv/certrqxt.asp**, where ***CAserverIP*** is the IP address of the CA server.

2 In the Certificate template menu, view the templates.

Setting certificate templates for NDES

1 From your computer, launch the registry editor.

2 Navigate to **HKEY_LOCAL_MACHINE >SOFTWARE >Microsoft > Cryptography > MSCEP**.

3 Configure the following, and then set them to **MVEWebServer**:
  - EncryptionTemplate
  - GeneralPurposeTemplate
  - SignatureTemplate

4 Give the SCEPSvc user full permission to MSCEP.

5 From IIS Manager, expand the CA, and then click **Application Pools**.

6 From the right panel, click **Recycle** to restart the SCEP application pool.

7 From IIS Manager, expand the CA, and then expand **Sites > Default Web Site**.

8 From the right panel, click **Restart**.

Disabling Challenge Password in Microsoft CA server

1 From your computer, launch the registry editor.

2 Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**.

3 Set EnforcePassword to **0**.

4 From IIS Manager, expand the CA, click **Application Pools**, and then select **SCEP**.

5 From the right panel, click **Advanced Settings**.

6 Set Load User Profile to **True**, and then click **OK**.

7 From the right panel, click **Recycle** to restart the SCEP application pool.

8 From IIS Manager, expand the CA, and then expand **Sites > Default Web Site**.

9 From the right panel, click **Restart**.

When opening the NDES from web browser, you can now only view the CA thumbprint.

Managing certificates using OpenXPKI Certificate Authority

This section provides instructions on how to configure OpenXPKI CA version 2.5.x using Simple Certificate Enrollment Protocol (SCEP).

Notes:

  - Make sure that you are using the Debian 8 Jessie operating system.
  - For more information on OpenXPKI, go to **www.openxpki.org**.

Configuring OpenXPKI CA

Installing OpenXPKI CA

1 Connect the machine using PuTTY or another client.

2 From the client, run the `sudo su -` command to go to the root user.

3 Enter the root password.

4 In **nano /etc/apt/sources.list**, change the source for installing the updates.

5 Update the file. For example:

```
#

# 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 Save the file.

7 Run the following commands:

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

8 Update the CA certificate lists in the server using **apt-get install ca-certificates**.

9 Install **en_US.utf8 locale** using **dpkg-reconfigure locales**.

10 Select the **en_US.UTF-8 UTF-8** locale, and then make it the default locale for the system.

   Note: Use the Tab and spacebar keys for selecting and navigating the menu.

11 Check the locales that you have generated using **locale -a**.

Sample output

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

12 Copy the fingerprint of the OpenXPKI package using **nano /home/Release.key**. For this instance, copy the key in **/home**.

13 Type **9B156AD0 F0E6A6C7 86FABE7A D8363C4E 1611A2BE 2B251336 01D1CDB4 6C24BEF3** as the value.

14 Run the following command:

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

15 Add the package using the **wget https://packages.openxpki.org/v2/debian/Release.key -O - | apt-key add -** command.

16 Add the repository to your source list (jessie) using **echo "deb http://packages.openxpki.org/v2/debian/jessie release" > /etc/apt/sources.list.d/openxpki.list**, and then **aptitude update**.

17 Install MySQL and Perl MySQL binding using **aptitude install mysql-server libdbd-mysql-perl**.

18 Install apache2.2-common using **aptitude install apache2.2-common**.

19 In **nano /etc/apt/sources.list**, install the fastcgi module to speed up the user interface.

   Note: We recommend using **mod_fcgid**.

20 Add the **deb http://http.us.debian.org/debian/jessie main** line in the file, and then save it.

21 Run the following commands:

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

22 Enable the fastcgi module using **a2enmod fcgid**.

23 Install the OpenXPKI core package using **aptitude install libopenxpki-perl openxpki-cgi-session-driver openxpki-i18n**.

24 Restart the Apache® server using **service apache2 restart**.

25 Check whether the installation is successful using **openxpkiadm version**.

   Note: If the installation is successful, then the system shows the version of the installed OpenXPKI. For example, **Version (core): 2.5.5**.

26 Create the empty database, and then assign the database user using **mysql -u root –p**.

   Notes:

   - This command must be typed in the client. Otherwise, you cannot enter the password.
   - Type the password for the MySQL. For this instance, **root** is the MySQL user.
   - **openxpki** is the user on which OpenXPKI is installed.

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

   If the MySQL service is not running, then run **/etc/init.d/mysql start** to start the service.

27 Type **quit** to exit from MySQL.

28 Store the used credentials in **/etc/openxpki/config.d/system/database.yaml**.

Sample file content

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

   Note: Change **user** and **passwd** to match the MySQL user name and password.

29 Save the file.

30 For empty database schema, run `zcat /usr/share/doc/libopenxpki-perl/examples/schema-mysql.sql.gz | \mysql -u root --password --database openxpki` from the provided schema file.

31 Enter the password for the database.

Configuring OpenXPKI CA using default script

Note: The default script configures only the default realm, **ca-one**. The CDP and CRLs are not configured.

1 Unzip the sample script for installing the certificate using `gunzip -k /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh.gz`.

2 Run the script using `bash /usr/share/doc/libopenxpki-perl/examples/sampleconfig.sh`.

3 Confirm the setup using `openxpkiadm alias --realm ca-one`.

Sample output

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

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

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

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

upcoming root ca:
  not set
```

4 Check whether the installation is successful using `openxpkictl start`.

Sample output

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

5 Do the following to access the OpenXPKI server:

a From a web browser, type `http://ipaddress/openxpki/`.

b Log in as **Operator**. The default password is `openxpki`.

   Note: The Operator login has two preconfigured operator accounts, **raop** and **raop2**.

6 Create one certificate request, and then test it.

Configuring OpenXPKI CA manually

Overview

Note: Before you begin, make sure that you have a basic knowledge on creating OpenSSL certificates.

To configure OpenXPKI CA manually, create the following:

1 Root CA certificate. For more information, see .

2 CA signer certificate, signed by the root CA. For more information, see .

3 Data vault certificate, self-signed. For more information, see .

4 SCEP certificate, signed by the signer certificate.

Notes:

- When selecting the signature hash, use either SHA256 or SHA512.
- Changing the public key size is optional.

For this instance, we are using the **/etc/certs/openxpki_ca-one/** directory for certificate generation. However, you can use any directory.

Creating an OpenSSL configuration file

1 Run the following command:

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

Note: If your server is reachable using the Fully Qualified Domain Name (FQDN), then use the DNS of the server instead of its IP address.

Sample file

```
# 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://10.195.0.111/CertEnroll/MYOPENXPKI.crl
authorityInfoAccess     = caIssuers;URI:http://10.195.0.111/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.dhcp.indiadev.lexmark.com
crlDistributionPoints   = URI:http://10.195.0.111/CertEnroll/MYOPENXPKI_ISSUINGCA.crl
authorityInfoAccess     =
caIssuers;URI:http://10.195.0.111/CertEnroll/MYOPENXPKI_ISSUINGCA.crt
```

2 Change the IP address and CA certificate name with your setup information.

3 Save the file.

Creating a password file for certificate keys

1 Run the following command:

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

2 Type your password.

3 Save the file.

Creating a root CA certificate

Note: You can create a self-signed root CA certificate or generate a certificate request, and then get it signed by the root CA.

Run the following commands:

Note: Replace the key length, signature algorithm, and certificate name with the appropriate values.

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`

Creating a signer certificate

Note: Replace the key length, signature algorithm, and certificate name with the appropriate values.

1 Run the following command:

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

2 Change the subject in the request with your CA information using `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 Get the certificate signed by the root CA using `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`.

Creating a vault certificate

Notes:

- The vault certificate is self-signed.
- Replace the key length, signature algorithm, and certificate name with the appropriate values.

1 Run the following command:

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

2 Change the subject in the request with your CA information using `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 Run the following command:

```
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
```

Creating an SCEP certificate

Note: The SCEP certificate is signed by the signer certificate.

Run the following commands:

Note: Replace the key length, signature algorithm, and certificate name with the appropriate values.

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
```

Copying the key file and creating a symlink

1 Copy the key files to **/etc/openxpki/ca/ca-one/**.

> **Note:** The key files must be readable by OpenXPKI.

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

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

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

2 Create the symlink.

> **Note:** Symlinks are aliases used by the default configuration.

```
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
```

Importing certificates

Import the root certificate, signer certificate, vault certificate, and SCEP certificate into the database with the appropriate tokens.

Run the following commands:

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 Check whether the import is successful using `openxpkiadm alias --realm ca-one`.

Sample output

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

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

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

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

upcoming root ca:
  not set
```

Starting OpenXPKI

1 Run the `openxpkictl start` command.

Sample output

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

2 Do the following to access the OpenXPKI server:

    a From a web browser, type `http://ipaddress/openxpki/`.

    b Log in as **Operator**. The default password is `openxpki`.

        Note: The Operator login has two preconfigured operator accounts, **raop** and **raop2**.

3 Create one certificate request, and then test it.

Generating CRL information

Note: If your server is reachable using the FQDN, then use the DNS of the server instead of its IP address.

1 Stop the OpenXPKI service using **Openxpkictl stop**.

2 In **nano /etc/openxpki/config.d/realm/ca-one/publishing.yaml**, update the **connectors: cdp** section to the following:

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

a In **nano /etc/openxpki/config.d/realm/ca-one/profile/default.yaml**, update the following:

- **crl_distribution_points:** section

```
critical: 0
uri:
    - http://10.195.0.111/CertEnroll/[% ISSUER.CN.0 %].crl
    - ldap://localhost/[% ISSUER.DN %]
```

- **authority_info_access:** section

```
critical: 0
ca_issuers: http://10.195.0.111/CertEnroll/MYOPENXPKI.crt
ocsp: http://ocsp.openxpki.org/
```

Change the IP address and CA certificate name according to your CA server.

b In **nano /etc/openxpki/config.d/realm/ca-one/crl/default.yaml**, do the following:

- If necessary, update **nextupdate** and **renewal**.
- Add **ca_issuers** to the following section:

```
extensions:
            authority_info_access:
                    critical: 0
                    # ca_issuers and ocsp can be scalar or list
                    ca_issuers: http://10.195.0.111/CertEnroll/MYOPENXPKI.crt
                #ocsp: http://ocsp.openxpki.org/
```

Change the IP address and CA certificate name according to your CA server.

3 Start the OpenXPKI service using **Openxpkictl start**.

Configuring CRL accessibility

1 Stop the Apache service using **service apache2 stop**.

2 Create a **CertEnroll** directory for crl in the **/var/www/openxpki/** directory.

3 Set **openxpki** as the owner of this directory, and then configure the permissions to let Apache read and execute, and other services to read only.

chown openxpki /var/www/openxpki/CertEnroll

chmod 755 /var/www/openxpki/CertEnroll

4 Add a reference to the Apache alias.conf file using **nano /etc/apache2/mods-enabled/alias.conf**.

5 After the `<Directory "/usr/share/apache2/icons">` section, add the following:

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

6 Add a reference in the apache2.conf file using **nano /etc/apache2/apache2.conf**.

7 Add the following in the **Apache2 HTTPD server** section:

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

8 Start the Apache service using **service apache2 start**.

Enabling the SCEP service

1 Stop the OpenXPKI service using **openxpkictl stop**.

2 Install the openca-tools package using **aptitude install openca-tools**.

3 Start the OpenXPKI service using **openxpkictl start**.

Test the service using any client, such as certnanny with SSCEP.

Note: SSCEP is a command line client for SCEP. You can download SSCEP from **https://github.com/certnanny/sscep**.

Enabling the Signer on Behalf (enrollment agent) certificate

For automatic certificate requests, we are using the Signer on Behalf certificate feature of OpenXPKI.

1 Stop the OpenXPKI service using **openxpkictl stop**.

2 In **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, from the **authorized_signer:** section, add a rule for the subject name of the signer certificate.

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

Notes:

- In this rule, any certificate CN starting with **Markvision_** is the Signer on Behalf certificate.
- The subject name is set in MVE for generating the Signer on Behalf certificate.
- Review the space and indention in the script file.
- If the CN is changed in MVE, then add the updated CN in OpenXPKI.
- You can specify only one certificate as Signer on Behalf, and then specify the full CN.

3 Save the file.

4 Start the OpenXPKI service using **openxpkictl start**.

Enabling automatic approval of certificate requests in OpenXPKI CA

1 Stop the OpenXPKI service using **`openxpkictl stop`**.

2 In **nano /etc/openxpki/config.d/realm/ca-one/scep/generic.yaml**, update the **`eligible:`** section:

Old content

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

New content

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

Notes:

- Review the space and indention in the script file.
- To approve certificates manually, comment **`value: 1`**, and then uncomment the other lines that are previously commented.

3 Save the file.

4 Start the OpenXPKI service using **`openxpkictl start`**.

Creating a second realm

In OpenXPKI, you can configure multiple PKI structures in the same system. The following topics show how to create another realm for MVE named **ca-two**.

Copying and setting the directory

1 Copy the **/etc/openxpki/config.d/realm/ca-one** sample directory tree to a new directory (**cp -avr /etc/openxpki/config.d/realm/ca-one /etc/openxpki/config.d/realm/ca-two**) within the realm directory.

2 In **/etc/openxpki/config.d/system/realms.yaml**, update the following section:

Old content

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

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

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

New content

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

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

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

3 Save the file.

Creating certificates

The following instructions show how to generate the signer certificate, vault certificate, and SCEP certificate. The root CA signs the signer certificate, and then the signer certificate signs the SCEP certificate. The vault certificate is self-signed.

1 Generate, and then sign the certificates. For more information, see "Configuring OpenXPKI CA manually" on page 82.

   Note: Change the certificate common name so that the user can easily distinguish between different certificates for different realms. You may change **DC=CA-ONE** to **DC=CA-TWO**. The certificate files are created in the **/etc/certs/openxpki_ca-two/** directory.

2 Copy the key files to **/etc/openxpki/ca/ca-two/**.

   Note: The key files must be readable by OpenXPKI.

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

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

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

3 Create the symlink. Also, create a symlink for the root CA certificate.

   Note: Symlinks are aliases used by the default configuration.

   ```
   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 Import the signer certificate, vault certificate, and SCEP certificate into the database with the appropriate tokens for **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 Check whether the import is successful using **openxpkiadm alias --realm ca-two**.

Sample output

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

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

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

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

upcoming root ca:
  not set
```

In this instance, the root CA information is the same for **ca-one** and **ca-two**.

6 If you changed the certificate key password during certificate creation, then update **nano /etc/openxpki/config.d/realm/ca-two/crypto.yaml**.

7 Generate the CRLs for this realm. For more information, see <u>"Generating CRL information" on page 87</u>.

8 Publish the CRLs for this realm. For more information, see <u>"Configuring CRL accessibility" on page 87</u>.

9 Restart the OpenXPKI service using **openxpkictl restart**.

Sample output

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

10 Do the following to access the OpenXPKI server:

a From a web browser, type **http://ipaddress/openxpki/**.

b Log in as **Operator**. The default password is **openxpki**.

Note: The Operator login has two preconfigured operator accounts, **raop** and **raop2**.

Configuring SCEP endpoint for multiple realms

The default realm SCEP endpoint is **http://<ipaddress>/scep/scep**. If you have multiple realms, then configure a unique SCEP endpoint (different configuration file) for each realm. In the following instructions, we use two PKI realms, **ca-one** and **ca-two**.

1 Copy the default configuration file in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-one.conf**.

   Note: Name the file as **ca-one.conf**.

2 In **nano /etc/openxpki/scep/ca-one.conf**, change the realm value to **realm=ca-one**.

3 Create another configuration file in **cp /etc/openxpki/scep/default.conf /etc/openxpki/scep/ca-two.conf**.

   Note: Name the file as **ca-two.conf**.

4 In **nano /etc/openxpki/scep/ca-two.conf**, change the realm value to **realm=ca-two**.

5 Restart the OpenXPKI service using **openxpkictl restart**.

The SCEP endpoints are the following:

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

If you want to differentiate between login credentials and default certificate templates for different PKI realms, then you may need advanced configuration.

Setting the default port number for OpenXPKI CA

By default, Apache listens in port number 80. Set the default port number for OpenXPKI CA to avoid conflicts.

1 In **/etc/apache2/ports.conf**, add or modify a port. For example, **Listen 8080**.

2 In **/etc/apache2/sites-enabled/000-default.conf**, add or modify the **VirtualHost** section to map new port. For example, **<VirtualHost *:8080>**.

3 Restart the Apache server using **systemctl restart apache2**.

To check the status, run **netstat -tlpn| grep apache**. The OpenXPKI SCEP URL is now **http://ipaddress: 8080/scep/ca-one**, and the web URL is **http://ip address:8080/openxpki**.

Disabling Challenge Password in OpenXPKI CA

By default, OpenXPKI accepts requests without checking the challenge password. The certificate request is not rejected, and the CA and CA administrator determine whether to approve or reject the request. To avoid potential security concerns, disable this feature so that any certificate requests that contain invalid passwords are rejected immediately. In MVE, Challenge Password is required only when generating the enrollment agent certificate.

1 In **etc/openxpki/config.d/realm/REALM NAME/scep/generic.yaml**, from the **policy** section, change the value of **allow_man_authen** from **1** to **0**.

   Notes:

   - REALM NAME is the name of the realm. For example, **ca-one**.
   - Review the space and indentation in the script file.

2 Restart the OpenXPKI service using **openxpkictl restart**.

Adding client authentication EKU in certificates

1 In **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, from the **extended_key_usage:** section, change the value of **client_auth:** to **1**.

Notes:

- REALM NAME is the name of the realm. For example, **ca-one**.
- Review the space and indentation in the script file.

2 Restart the OpenXPKI service using **openxpkictl restart**.

Getting the full certificate subject when requesting through SCEP

By default, OpenXPKI reads only the CN of the subject of the requesting certificate. The rest of the information, such as country, locality, and DC, are hard-coded. For example, if a certificate subject is **C=US**, **ST=KY**, **L=Lexington**, **O=Lexmark**, **OU=ISS**, **CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**, then after signing the certificate through SCEP, the subject is changed to **DC=Test Deployment**, **DC= OpenXPKI**, **CN=ET0021B7C34AEC.dhcp.dev.lexmark.com**.

Note: REALM NAME is the name of the realm. For example, **ca-one**.

1 In **/etc/openxpki/config.d/realm/REALM NAME/profile/I18N_OPENXPKI_PROFILE_TLS_SERVER.yaml**, from the **enroll** section, change the value of **dn** to the following:

```
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 Save the file.

3 Create a file titled **l.yaml** in the **/etc/openxpki/config.d/realm/REALM NAME/profile/template** directory.

4 Add the following:

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

5 Save the file.

6 Create a file titled **st.yaml** in the **/etc/openxpki/config.d/realm/REALM NAME/profile/template** directory.

7 Add the following:

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

8 Save the file.

Note: OpenXPKI must own both files and must be readable, writable, and executable.

9 Restart the OpenXPKI service using **openxpkictl restart**.

Revoking certificates and configuring CRL accessibility

1 Access the OpenXPKI server.

   a From a web browser, type **`http://ipaddress/openxpki/`**.

   b Log in as **Operator**. The default password is **`openxpki`**.

      Note: The Operator login has two preconfigured operator accounts, **raop** and **raop2**.

2 Click **Workflow Search > Search now**.

3 Click a certificate to revoke, and then click the certificate link.

4 From the Action section, click **revocation request**.

5 Type the appropriate values, and then click **Continue > Submit request**.

6 On the next page, approve the request. The certificate revocation is waiting for the next CRL publish.

7 From the PKI Operation section, click **Issue a certificate revocation list (CRL)**.

8 Click **Enforce creation of revocation lists > Continue**.

9 From the PKI Operation section, click **Publish CA/CRL**.

10 Click **Workflow Search > Search now**.

11 Click the revoked certificate with a **certificate_revocation_request_v2** type.

12 Click **Force wake up**.

In the new CRL, you can find the serial number and the revocation reason of the revoked certificate.

Managing printer alerts

Overview

Alerts are triggered when a printer requires attention. Actions let you send customized e-mails or run scripts when an alert occurs. Events define which actions are executed when specific alerts are active. To register for alerts from a printer, create actions and then associate them with an event. Assign the event to the printers that you want to monitor.

Note: This feature is not applicable to secured printers.

Creating an action

An action is either an e-mail notification or an event viewer log. Actions assigned to events are triggered when a printer alert occurs.

1 From the Printers menu, click **Events & Actions** > **Actions** > **Create**.

2 Type a unique name for the action and its description.

3 Select an action type.

E-mail

Note: Before you begin, make sure that the e-mail settings are configured. For more information, see .

a In the Type menu, select **E-mail**.

b Type the appropriate values in the fields. You can also use the available placeholders as the entire or part of the subject title, or as part of an e-mail message. For more information, see .

Type

E-mail

From (Optional)

admin@mycompany.com

To

scott.summers@mycompany.com

CC (Optional)

Subject (Optional)

${alert.type}   alert.type

Body

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

Create Action   Cancel

c Click **Create Action**.

Log event

a In the Type menu, select **Log event**.

b Type the event parameters. You can also use the available placeholders in the drop-down menu. For more information, see "Understanding action placeholders" on page 96.

General

Name

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

Description (Optional)

Type

Log event

Event parameters (Optional)

${alert.type}

Maximum length for field is 255

Create Action   Cancel

alert.type
alert.location
alert.state
alert.name
configurationItem.manufacturer

About

c Click **Create Action**.

Understanding action placeholders

Use the available placeholders in the subject title or e-mail message. Placeholders represent variable elements, and are replaced with actual values when used.

- **${eventHandler.timestamp}**—The date and time that MVE processed the event. For example, `Mar 14, 2017 1:42:24 PM`.
- **${eventHandler.name}**—The name of the event.
- **${configurationItem.name}**—The system name of the printer that triggered the alert.
- **${configurationItem.address}**—The MAC address of the printer that triggered the alert.
- **${configurationItem.ipAddress}**—The IP address of the printer that triggered the alert.
- **${configurationItem.ipHostname}**—The host name of the printer that triggered the alert.
- **${configurationItem.model}**—The model name of the printer that triggered the alert.
- **${configurationItem.serialNumber}**—The serial number of the printer that triggered the alert.
- **${configurationItem.propertyTag}**—The property tag of the printer that triggered the alert.
- **${configurationItem.contactName}**—The contact name of the printer that triggered the alert.
- **${configurationItem.contactLocation}**—The contact location of the printer that triggered the alert.
- **${configurationItem.manufacturer}**—The manufacturer of the printer that triggered the alert.
- **${alert.name}**—The name of the alert that is triggered.
- **${alert.state}**—The state of the alert. It can be active or cleared.
- **${alert.location}**—The location within the printer where the triggered alert occurred.
- **${alert.type}**—The severity of the triggered alert, such as `Warning` or `Intervention Required`.

Managing actions

1 From the Printers menu, click **Events & Actions** > **Actions**.

2 Do any of the following:

Edit an action

a Select an action, and then click **Edit**.

b Configure the settings.

c Click **Save Changes**.

Delete actions

a Select one or more actions.

b Click **Delete**, and then confirm deletion.

Test an action

a Select an action, and then click **Test**.

b To verify the test results, see the tasks logs.

   Notes:

   - For more information, see <u>"Viewing logs" on page 103</u>.
   - If you are testing an e-mail action, then verify if the e-mail was sent to the recipient.

Creating an event

You can monitor alerts in your printer fleet. Create an event, and then set an action to execute when the specified alerts occur. Events are not supported in secured printers.

1 From the Printers menu, click **Events & Actions** > **Events** > **Create**.

2 Type a unique name for the event and its description.

3 From the Alerts section, select one or more alerts. For more information, see <u>"Understanding printer alerts" on page 98</u>.

4 From the Actions section, select one or more actions to execute when the selected alerts are active.

   Note: For more information, see <u>"Creating an action" on page 95</u>.

5 Enable the system to execute selected actions when alerts are cleared on the printer.

6 Set a grace period before executing any selected actions.

   Note: If the alert is cleared during the grace period, then the action is not executed.

7 Click **Create Event**.

Understanding printer alerts

Alerts are triggered when a printer requires attention. The following alerts can be associated with an event in MVE:

- **Automatic Document Feeder (ADF) jam**—A paper is jammed in the ADF and must be physically removed.
  - Scanner ADF Exit Jam
  - Scanner ADF Feeder Jam
  - Scanner ADF Inverter Jam
  - Scanner ADF Paper Cleared
  - Scanner ADF Paper Missing
  - Scanner ADF PreRegistration Jam
  - Scanner ADF Registration Jam
  - Scanner Alert - Replace All Originals if Restarting Job
- **Door or cover open**—A door is open on the printer and must be closed.
  - Check Door/Cover - Mailbox
  - Door Open
  - Cover Alert
  - Cover Closed
  - Cover Open
  - Cover Open Or Cartridge Missing
  - Duplex Cover Open
  - Scanner ADF Cover Open
  - Scanner Jam Access Cover Open
- **Incorrect media size or type**—A job is printing and requires certain paper to be loaded in a tray.
  - Incorrect Envelope Size
  - Incorrect Manual Feed
  - Incorrect Media
  - Incorrect Media Size
  - Load Media
- **Memory full or error**—The printer is running low on memory and must apply changes.
  - Complex Page
  - Files Will Be Deleted
  - Insufficient Collation Memory
  - Insufficient Defrag Memory
  - Insufficient Fax Memory
  - Insufficient Memory
  - Insufficient Memory - Held Jobs May Be Lost
  - Insufficient Memory For Resource Save
  - Memory Full
  - PS Memory Shortage

- Scanner Too Many Pages - Scan Job Canceled
- Resolution Reduction

- **Option malfunction**—An option attached to the printer is in an error state. Options include input options, output options, font cards, user flash cards, disks, and finishers.
  - Check Alignment/Connection
  - Check Duplex Connection
  - Check Finisher/Mailbox Installation
  - Check Power
  - Corrupted Option
  - Defective Option
  - Detach Device
  - Duplex Alert
  - Duplex Tray Missing
  - External Network Adapter Lost
  - Finisher Alert
  - Finisher Door Or Interlock Open
  - Finisher Paper Wall Open
  - Incompatible Duplex Device
  - Incompatible Input Device
  - Incompatible Output Device
  - Incompatible Unknown Device
  - Incorrect Option Installation
  - Input Alert
  - Input Configuration Error
  - Option Alert
  - Output Bin Full
  - Output Bin Nearly Full
  - Output Configuration Error
  - Option Full
  - Option Missing
  - Paper Feed Mechanism Missing
  - Print Jobs On Option
  - Reattach Device
  - Reattach Output Device
  - Too Many Inputs Installed
  - Too Many Options Installed
  - Too Many Outputs Installed
  - Tray Missing
  - Tray Missing During Power On
  - Tray Sensing Error
  - Uncalibrated Input

- – Unformatted Option
- – Unsupported Option
- – Reattach Input Device
- **Paper jam**—A paper is jammed in the printer and must be physically removed.
  - – Internal Paper Jam
  - – Jam Alert
  - – Paper Jam
- **Scanner error**—The scanner has a problem.
  - – Scanner Back Cable Unplugged
  - – Scanner Carriage Locked
  - – Scanner Clean Flatbed Glass/Backing Strip
  - – Scanner Disabled
  - – Scanner Flatbed Cover Open
  - – Scanner Front Cable Unplugged
  - – Scanner Invalid Scanner Registration
- **Supplies error**—A printer supply has a problem.
  - – Abnormal Supply
  - – Cartridge Region Mismatch
  - – Defective Supply
  - – Fuser Unit Or Coating Roller Missing
  - – Invalid Or Missing Left Cartridge
  - – Invalid Or Missing Right Cartridge
  - – Invalid Supply
  - – Priming Failure
  - – Supply Alert
  - – Supply Jam
  - – Supply Missing
  - – Toner Cartridge Eject Handle Pulled
  - – Toner Cartridge Not Installed Correctly
  - – Uncalibrated Supply
  - – Unlicensed Supply
  - – Unsupported Supply
- **Supplies or consumable empty**—A printer supply must be replaced.
  - – Input Empty
  - – Life Exhausted
  - – Printer Ready for Maintenance
  - – Scheduled Maintenance
  - – Supply Empty
  - – Supply Full
  - – Supply Full or Missing

Note: The printer sends the alert as an error and a warning. If one of these alerts is triggered, then its associated action occurs twice.

- **Supplies or consumable low**—A printer supply is running low.
  - Early Warning
  - First Low
  - Input Low
  - Life Warning
  - Nearly Empty
  - Nearly Low
  - Supply Low
  - Supply Nearly Full
- **Uncategorized alert or condition**
  - Color Calibration Failure
  - Data Transmission Error
  - Engine CRC Failure
  - External Alert
  - Fax Connection Lost
  - Fan Stall
  - Hex Active
  - Insert Duplex Page and Press Go
  - Internal Alert
  - Internal Network Adapter Needs Service
  - Logical Unit Alert
  - Offline
  - Offline for Warning Prompt
  - Operation Failed
  - Operator Intervention Alert
  - Page Error
  - Port Alert
  - Port Communication Failure
  - Port Disabled
  - Power Saver
  - Powering Off
  - PS Job Timeout
  - PS Manual Timeout
  - Setup Required
  - SIMM Checksum Error
  - Supply Calibrating
  - Toner Patch Sensing Failed
  - Unknown Alert Condition
  - Unknown Configuration

- Unknown Scanner Alert Condition
- User(s) Locked Out
- Warning Alert

Managing events

1 From the Printers menu, click **Events & Actions** > **Events**.

2 Do either of the following:

Edit an event

a Select an event, and then click **Edit**.

b Configure the settings.

c Click **Save Changes**.

Delete events

a Select one or more events.

b Click **Delete**, and then confirm deletion.

Viewing task status and history

Overview

Tasks are any printer management activities performed in MVE, such as printer discovery, audit, and configurations enforcement. The Status page shows the status of all currently running tasks and the tasks run in the last 72 hours. Information on the currently running tasks is entered into the log. Tasks older than 72 hours can be viewed only as individual log entries in the Log page, and can be searched using the task IDs.

Viewing the task status

From the Tasks menu, click **Status**.

Note: The task status is updated in real time.

Stopping tasks

1 From the Tasks menu, click **Status**.

2 From the Currently Running Tasks section, select one or more tasks.

3 Click **Stop**.

Viewing logs

1 From the Tasks menu, click **Logs**.

2 Select task categories, task types, or a time period.

   Notes:

   - Use the search field to search for multiple Task IDs. Use commas to separate multiple Task IDs or a hyphen to indicate a range. For example, `11, 23, 30-35`.
   - To export the search results, click **Export to CSV**.

Clearing logs

1 From the Tasks menu, click **Log**.

2 Click **Clear Log**, and then select a date.

3 Click **Clear Log**.

Exporting logs

1 From the Tasks menu, click **Log**.

2 Select task categories, task types, or a time period.

3 Click **Export to CSV**.

Scheduling tasks

Creating a schedule

1 From the Tasks menu, click **Schedule** > **Create**.

2 From the General section, type a unique name for the scheduled tasks and its description.

3 From the Task section, do one of the following:

Schedule an audit

a Select **Audit**.

b Select a saved search.

Schedule a conformance check

a Select **Conformance**.

b Select a saved search.

Schedule a printer status check

a Select **Current Status**.

b Select a saved search.

c Select an action.

Schedule a configuration deployment

a Select **Deploy File**.

b Select a saved search.

c Browse to the file, and then select the file type.

d If necessary, select a deployment method or protocol.

Schedule a discovery

a Select **Discovery**.

b Select a discovery profile.

Schedule a configuration enforcement

a Select **Enforcement**.

b Select a saved search.

Schedule a certificate validation

Select **Validate Certificate**.

Note: During validation, MVE communicates with the CA server to download the certificate chain and the Certificate Revocation List (CRL). The enrolment agent certificate is also generated. This certificate enables the CA server to trust MVE.

Schedule a view export

a Select **View Export**.

b Select a saved search.

c Select a view template.

d Type the list of e‑mail addresses where the exported files are sent.

4 From the Schedule section, set the date, time, and frequency of the task.

5 Click **Create Scheduled Task**.

Managing scheduled tasks

1 From the Tasks menu, click **Schedule**.

2 Do either of the following:

Edit a scheduled task

a Select a task, and then click **Edit**.

b Configure the settings.

c Click **Edit Scheduled Task**.

Note: The Last Run information is removed when a scheduled task is edited.

Delete a scheduled task

a Select a task, and then click **Delete**.

b Click **Delete Scheduled Task**.

Performing other administrative tasks

Configuring general settings

1 Click ⚙ on the upper-right corner of the page.

2 Click **General**, and then select a host name source.

- **Printer**—The system retrieves the host name from the printer.
- **Reverse DNS Lookup**—The system retrieves the host name from the DNS table using the IP address.

3 Set the alert reregistration frequency.

Note: Printers may lose the alert registration state when changes are made, such as rebooting or updating the firmware. MVE attempts to recover the state automatically on the next interval set in the alert reregistration frequency.

4 Click **Save Changes**.

Configuring e-mail settings

The SMTP configuration must be enabled to let MVE send data export files and event notifications through e-mail.

1 Click ⚙ on the upper-right corner of the page.

2 Click **E-mail**, and then select **Enable E-mail SMTP configuration**.

3 Type the SMTP mail server and port.

4 Type the e-mail address of the sender.

5 If a user must log in before e-mailing, then select **Login required**, and then type the user credentials.

6 Click **Save Changes**.

Adding a login disclaimer

You can configure a login disclaimer to be shown when users log in with a new session. Users must accept the disclaimer before they can access MVE.

1 Click ⚙ on the upper-right corner of the page.

2 Click **Disclaimer**, and then select **Enable disclaimer prior to login**.

3 Type the disclaimer text.

4 Click **Save Changes**.

Signing the MVE certificate

Secure Socket Layer (SSL) or Transport Layer Security (TLS) is a security protocol that uses data encryption and certificate authentication to protect server-client communication. In MVE, TLS is used to protect the sensitive information shared between the MVE server and the web browser. The protected information can be printer passwords, security policies, MVE user credentials, or printer authentication information, such as LDAP or Kerberos.

TLS enables the MVE server and the web browser to encrypt the data before sending it, and then decrypt it after it is received. SSL also requires the server to present the web browser with a certificate that proves that the server is who it claims to be. This certificate is either self-signed or signed using a trusted third-party CA. By default, MVE is configured to use a self-signed certificate.

1 Download the certificate signing request.

   a Click ![gear] on the upper-right corner of the page.

   b Click **TLS** > **Download**.

   c Select **Certificate signing request**.

   Note: The certificate signing request includes Subject Alternative Names (SANs).

2 Use a trusted CA to sign the certificate signing request.

3 Install the CA-signed certificate.

   a Click ![gear] on the upper-right corner of the page.

   b Click **TLS** > **Install Signed Certificate**.

   c Upload the CA-signed certificate, and then click **Install Certificate**.

   d Click **Restart MVE Service**.

   Note: Restarting the MVE service reboots the system, and the server may be unavailable for the next few minutes. Before restarting the service, make sure that no tasks are currently running.

Removing user information and references

MVE is compliant with the data protection rules under General Data Protection Regulation (GDPR). MVE can be configured to apply the right to be forgotten and remove private user information from the system.

Removing users

1 Click ![gear] on the upper-right corner of the page.

2 Click **User**, and then select one or more users.

3 Click **Delete** > **Delete Users**.

Removing user references in LDAP

1 Click ![gear] on the upper-right corner of the page.

2 Click **LDAP**.

3 Remove any user-related information in the search filters and binding settings.

Removing user references in the e-mail server

1 Click ⚙ on the upper-right corner of the page.

2 Click **E-mail**.

3 Remove any user-related information, such as user credentials used for authenticating with the e-mail server.

Removing user references in the task logs

For more information, see "Clearing logs" on page 103.

Removing user references in a configuration

1 From the Configurations menu, click **All Configurations**.

2 Click the configuration name.

3 From the Basic tab, remove any user-related values from the printer settings, such as contact name and contact location.

Removing user references in an advanced security component

1 From the Configurations menu, click **All Advanced Security Components**.

2 Click the component name.

3 From the Advanced Security Settings section, remove any user-related values.

Removing user references in saved searches

1 From the Printers menu, click **Saved Searches**.

2 Click a saved search.

3 Remove any search rule that uses any user-related values, such as contact name and contact location.

Removing user references in keywords

1 From the Printers menu, click **Printer Listing**.

2 Unassign user-related keywords from the printers.

3 From the Printers menu, click **Keywords**.

4 Remove any keyword that uses user-related information.

Removing user references in events and actions

1 From the Printers menu, click **Events & Actions**.

2 Remove any actions that contain e-mail references to users.

Frequently asked questions

Markvision Enterprise FAQ

Why can I not choose multiple printers in the supported models list when creating a configuration?

Configuration settings and commands differ between printer models.

Can other users access my saved searches?

Yes. All users can access saved searches.

Where can I find the log files?

You can find the installation log files in the hidden directory of the user installing MVE. For example, `C:\Users\Administrator\AppData\Local\Temp\mveLexmark-install.log`.

You can find the *.log application log files in the *installation_dir*`\Lexmark\Markvision Enterprise\tomcat\logs` folder, where *installation_dir* is the installation folder of MVE.

What is the difference between host name and reverse DNS lookup?

A host name is a unique name assigned to a printer on a network. Each host name corresponds to an IP address. Reverse DNS lookup is used to determine the designated host name and domain name of a given IP address.

Where can I find reverse DNS lookup in MVE?

Reverse DNS lookup can be found in the general settings. For more information, see .

How do I manually add rules to the Windows firewall?

Run the command prompt as an administrator, and then type the following:

```
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"
```

Where *installation_dir* is the installation folder of MVE.

How do I set up MVE to use a different port other than port 443?

1 Stop the Markvision Enterprise service.

    a Open the Run dialog box, and then type `services.msc`.

    b Right-click **Markvision Enterprise**, and then click **Stop**.

2 Open the *installation_dir***\Lexmark\Markvision Enterprise\tomcat\conf\server.xml** file.

Where *installation_dir* is the installation folder of MVE.

3 Change the **Connector port** value to another unused port.

```
<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 Change the **redirectPort** value to the same port number used as the connector port.

```
<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 Restart the Markvision Enterprise service.

a Open the Run dialog box, and then type **services.msc**.

b Right-click **Markvision Enterprise**, and then click **Restart**.

6 Access MVE using the new port.

For example, open a web browser, and then type **https://*MVE_SERVER*:*port*/mve**.

Where *MVE_SERVER* is the host name or IP address of the server hosting MVE, and *port* is the connector port number.

How do I customize the ciphers and TLS versions that MVE uses?

1 Stop the Markvision Enterprise service.

a Open the Run dialog box, and then type **services.msc**.

b Right-click **Markvision Enterprise**, and then click **Stop**.

2 Open the *installation_dir***\Lexmark\Markvision Enterprise\tomcat\conf\server.xml** file.

Where *installation_dir* is the installation folder of MVE.

3 Configure the ciphers and TLS versions.

For more information on the configuration, see the **Apache Tomcat SSL/TLS configuration instructions**.

For more information on the protocols and cipher values, see the **Apache Tomcat SSL support information documentation**.

4 Restart the Markvision Enterprise service.

a Open the Run dialog box, and then type **services.msc**.

b Right-click **Markvision Enterprise**, and then click **Restart**.

How do I manage CRL files when using Microsoft CA Enterprise?

1 Obtain the CRL file from the CA server.

> **Notes:**
>
> - For Microsoft CA Enterprise, the CRL is not automatically downloaded through SCEP.
> - For more information, see the *Microsoft Certificate Authority Configuration Guide*.

2 Save the CRL file in the **installation_dir\Lexmark\Markvision Enterprise\apps\library \crl** folder. Where **installation_dir** is the installation folder of MVE.

3 Configure the certificate authority in MVE.

Troubleshooting

User has forgotten the password

Reset the user password

You need administrative rights to reset the password.

1 Click ⚙ on the upper-right corner of the page.

2 Click **User**, and then select a user.

3 Click **Edit**, and then change the password.

4 Click **Save Changes**.

If you have forgotten your own password, then do either of the following:

- Contact another Admin user to reset your password.
- Contact Lexmark Customer Support Center.

Admin user has forgotten the password

Create another Admin user, and then delete the previous account

You can use the Markvision Enterprise Password Utility to create another Admin user.

1 Browse to the folder where Markvision Enterprise is installed.

For example, `C:\Program Files\`

2 Launch the **mvepwdutility-windows.exe** file in the Lexmark\Markvision Enterprise\ directory.

3 Select a language, and then click **OK** > **Next**.

4 Select **Add User Account** > **Next**.

5 Enter the user credentials.

6 Click **Next**.

7 Access MVE, and then delete the previous Admin user.

Note: For more information, see .

Page does not load

This problem may occur if you have closed the web browser without logging out.

Try one or more of the following:

Clear the cache, and delete the cookies in your web browser

Access the MVE login page, and then log in using your credentials

Open a web browser, and then type `https://MVE_SERVER/mve/login`, where `MVE_SERVER` is the host name or IP address of the server hosting MVE.

Cannot discover a network printer

Try one or more of the following:

Make sure that the printer is turned on

Make sure that the power cord is securely plugged into the printer and into a properly grounded electrical outlet

Make sure that the printer is connected to the network

Restart the printer

Make sure that TCP/IP is enabled on the printer

Make sure that the ports used by MVE are open, and SNMP and mDNS are enabled

For more information, see .

Contact your Lexmark representative

Incorrect printer information

Perform an audit

For more information, see .

MVE does not recognize a printer as a secured printer

Make sure that the printer is secured

For more information on securing printers, see the *Embedded Web Server—Security Administrator's Guide* for the printer.

Make sure that mDNS is turned on and is not blocked

Delete the printer, and then rerun the printer discovery

For more information, see .

Enforcement of configurations with multiple applications fails in the first attempt but succeeds in the subsequent attempts

Increase the timeouts

1 Browse to the folder where Markvision Enterprise is installed.

For example, `C:\Program Files\`

2 Navigate to the Lexmark\Markvision Enterprise\apps\dm-mve\WEB-INF\classes folder.

3 Using a text editor, open the *platform.properties* file.

4 Edit the `cdcl.ws.readTimeout` value.

Note: The value is in milliseconds. For example, 90000 milliseconds is equal to 90 seconds.

5 Using a text editor, open the *devCom.properties* file.

6 Edit the `1st.responseTimeoutsRetries` values.

Note: The value is in milliseconds. For example, 10000 milliseconds is equal to 10 seconds.

For example, `1st.responseTimeoutsRetries=10000 15000 20000`. The first connection retry is after 10 seconds, the second connection retry is after 15 seconds, and the third connection retry is after 20 seconds.

7 If necessary, when you are using LDAP GSSAPI, then create a *parameters.properties* file.

Add the following setting: `1st.negotiation.timeout=400`

Note: The value is in seconds.

8 Save the changes.

Enforcement of configurations with printer certificate fails

Sometimes, no new certificate is issued during enforcement.

Increase the number of enrolment retries

Add the following key in the **platform.properties** file:

```
enrol.maxEnrolmentRetry=10
```

The retry value must be greater than five.

OpenXPKI Certificate Authority

Certificate issuance failed using the OpenXPKI CA server

Make sure that the "signer on behalf" key in MVE matches the authorized signer key in the CA server

For example:

If the following is the **ca.onBehalf.cn** key in the **platform.properties** file in MVE,

```
ca.onBehalf.cn=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

then the following must be the **authorized_signer** key in the **generic.yaml** file in the CA server.

```
rule1:
            # Full DN
                    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

For more information on configuring the OpenXPKI CA server, see the *OpenXPKI Certificate Authority Configuration Guide*.

An internal server error occurs

Install the en_US.utf8 locale

1 Run the **dpkg-reconfigure locales** command.

2 Install the **en_US.utf8** (locale -a | grep en_US) locale.

The login prompt does not appear

When accessing **http://yourhost/openxpki/**, you get only the Open Source Trustcenter banner, without a login prompt.

Enable `fcgid`

Run the following commands:

1 `a2enmod fcgid`

2 `service apache2 restart`

A nested connector without class error occurs

An **EXCEPTION: Nested connector without class (scep.scep-server-1.connector.initial)** error at /usr/share/perl5/Connector/Multi.pm line 201 appears.

Update `scep.scep-server-1`

In **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, replace **`scep.scep-server-1`** with **`scep.generic`**.

Note: Replace **REALM** with the name of your realm. For example, when using the default realm, use **`ca-one`**.

```
eligible:
    initial:
          value@: connector:scep.generic.connector.initial
```

Cannot manually approve certificates

The Manual Approve button does not appear when approving certificates manually.

Update `scep.scep-server-1`

In **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, replace **`scep.scep-server-1`** with **`scep.generic`**.

Note: Replace **REALM** with the name of your realm. For example, when using the default realm, use **`ca-one`**.

```
eligible:
    initial:
          value@: connector:scep.generic.connector.initial
```

A Perl error occurs when approving enrollment requests

Update `scep.scep-server-1`

In **/etc/openxpki/config.d/realm/REALM/scep/generic.yaml**, replace **`scep.scep-server-1`** with **`scep.generic`**.

Note: Replace **REALM** with the name of your realm. For example, when using the default realm, use **`ca-one`**.

```
eligible:
    initial:
          value@: connector:scep.generic.connector.initial
```

The `ca-signer-1` and `vault-1` tokens are offline

The System Status page shows that the **`ca-signer-1`** and **`vault-1`** tokens are offline.

Try one or more of the following:

Change the certificate key password

In **/etc/openxpki/config.d/realm/ca-one/crypto.yaml**, change the certificate key password.

Create correct symlinks and copy the key file

For more information, see <u>"Copying the key file and creating a symlink" on page 85</u>.

Make sure that the key file is readable by OpenXPKI

Appendix

Understanding ports and protocols

MVE uses different ports and protocols for several types of network communication, as shown in the following diagram:
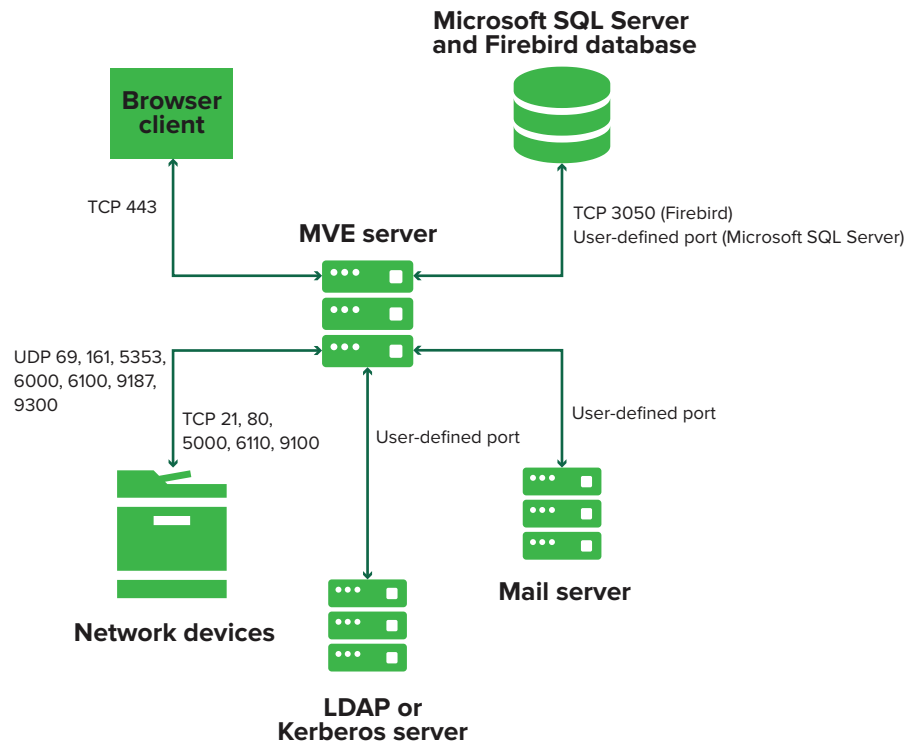
Notes:

- The ports are bidirectional and must be open or active for MVE to function properly. Make sure that all the printer ports are enabled.
- Some communications require an ephemeral port, which is an allocated range of available ports on the server. When a client requests a temporary communication session, the server assigns a dynamic port to the client. The port is valid only for a short duration and can become available for reuse when the previous session expires.

Server-to-printer communication

Ports and protocols used during communication from the MVE server to network printers

Protocol	MVE server	Printer	Used for
Network Printing Alliance Protocol (NPAP)	UDP 9187	UDP 9300	Communicating with Lexmark network printers.
XML Network Transport (XMLNT)	UDP 9187	UDP 6000	Communicating with some Lexmark network printers.

Protocol	MVE server	Printer	Used for
Lexmark Secure Transport (LST)	UDP 6100 Ephemeral Transmission Control Protocol (TCP) port (handshaking)	UDP 6100 TCP 6110 (handshaking)	Communicating securely with some Lexmark network printers.
Multicast Domain Name System (mDNS)	Ephemeral User Datagram Protocol (UDP) port	UDP 5353	Discovering Lexmark network printers and determining the security capabilities of printers. **Note:** This port is required to allow MVE to communicate with secured printers.
Simple Network Management Protocol (SNMP)	Ephemeral UDP port	UDP 161	Discovering and communicating with Lexmark and third-party network printers.
File Transfer Protocol (FTP)	Ephemeral TCP port	TCP 21 TCP 20	Deploying files.
Hypertext Transfer Protocol (HTTP)	Ephemeral TCP port	TCP 80	Deploying files or enforcing configurations.
		TCP 443	Deploying files or enforcing configurations.
Hypertext Transfer Protocol over SSL (HTTPS)	Ephemeral TCP port	TCP 161 TCP 443	Deploying files or enforcing configurations.
RAW	Ephemeral TCP port	TCP 9100	Deploying files or enforcing configurations.

Printer-to-server communication

Port and protocol used during communication from network printers to the MVE server

Protocol	Printer	MVE server	Used for
NPAP	UDP 9300	UDP 9187	Generating and receiving alerts

Server-to-database communication

Ports used during communication from the MVE server to databases

MVE server	Database	Used for
Ephemeral TCP port	User-defined port. The default port is TCP 1433.	Communicating with an SQL Server database.
Ephemeral TCP port	TCP 3050	Communicating with a Firebird database.

Client-to-server communication

Port and protocol used during communication from the browser client to the MVE server

Protocol	Browser Client	MVE server
Hypertext Transfer Protocol over SSL (HTTPs)	TCP port	TCP 443

Server-to-mail-server communication

Port and protocol used during communication from the MVE server to a mail server

Protocol	MVE server	SMTP server	Used for
Simple Mail Transfer Protocol (SMTP)	Ephemeral TCP port	User-defined port. The default port is TCP 25.	Providing the e-mail functionality used to receive alerts from printers.

Server-to-LDAP-server communication

Ports and protocols used during communication from the MVE server to an LDAP server involving user groups and authentication functionality

Protocol	MVE server	LDAP server	Used for
Lightweight Directory Access Protocol (LDAP)	Ephemeral TCP port	User-defined port. The default port is TCP 389.	Authenticating MVE users using an LDAP server.
Lightweight Directory Access Protocol over TLS (LDAPS)	Ephemeral TCP port	User-defined port. The default port is TCP 636.	Authenticating MVE users using an LDAP server over TLS.
Kerberos	Ephemeral UDP port	User-defined port. The default port is UDP 88.	Authenticating MVE users using Kerberos.

Enabling automatic approval of certificate requests in Microsoft CA

By default, all CA servers are in pending mode and you must manually approve each signed certificate request. Since this method is not feasible for bulk requests, enable the automatic approval of signed certificates.

1 From Server Manager, click **Tools** > **Certification Authority**.

2 From the left panel, right-click the CA, and then click **Properties** > **Policy Module**.

3 From the Request Handling tab, click **Follow the settings in the certificate template if applicable**, and then click **OK**.

   Note: If **Set the certificate request status to pending** is selected, then you must manually approve the certificate.

4 Restart the CA service.

Revoking certificates

Note: Before you begin, make sure that the CA server is configured for CRLs and that they are available.

1 From the CA server, open **Certification Authority**.

2 From the left panel, expand the CA, and then click **Issued Certificates**.

3 Right-click a certificate to revoke, and then click **All Tasks > Revoke Certificate**.

4 Select a reason code and the date and time for revocation, and then click **Yes**.

5 From the left panel, right-click **Revoked Certificates**, and then click **All Tasks > Publish**.

Note: Make sure that the certificate that you revoked is in Revoked Certificates.

You can see the revoked certificate serial number in the CRL.

Notices

Edition notice

November 2020

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user's responsibility.

For Lexmark technical support, go to **http://support.lexmark.com**.

For information on Lexmark's privacy policy governing the use of this product, go to **www.lexmark.com/privacy**.

For information on supplies and downloads, go to **www.lexmark.com**.

© **2017 Lexmark International, Inc.**

All rights reserved.

Trademarks

Lexmark, the Lexmark logo, and Markvision are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Firebird is a registered trademark of the Firebird Foundation.

Google Chrome is a trademark of Google LLC.

Safari is a registered trademark of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software

Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

** JmDNS

Licensing notices

All licensing notices associated with this product can be viewed from the program folder.

Glossary

action	An e-mail notification or a command-line operation. Actions assigned to events are triggered when a printer alert occurs.
audit	The task of collecting printer data such as printer status, supplies, and capabilities.
configuration	A collection of settings that can be assigned and enforced to a printer or a group of printer models. Within a configuration, you can modify printer settings and deploy applications, licenses, firmware, and CA certificates to the printers.
discovery profile	A profile that contains a set of parameters used to find printers on a network. It may also contain predefined configurations that can be assigned and enforced to printers automatically during the discovery.
event	Defines which actions are executed when specific alerts are active.
keyword	A custom text assigned to printers that you can use to search for those printers within the system. When you filter a search using a keyword, only printers that are tagged with the keyword are shown.
secured printer	A printer that is configured to communicate through an encrypted channel, and requires authentication to access its functions or applications.
token	An identifier that represents printer data values for variable settings in a configuration.
variable settings	A set of printer settings containing dynamic values that can be integrated into a configuration.

Index