



LexmarkTM

Markvision Enterprise

Version 3.5

Administrator's Guide

February 2020

www.lexmark.com

Contents

- Change history..... 6**
- Overview..... 9**
- Getting started.....10**
 - Best practices.....10
 - System requirements..... 12
 - Supported languages.....13
 - Supported printer models..... 13
 - Setting up the database..... 16
 - Setting up a run-as user.....17
 - Installing MVE..... 17
 - Accessing MVE..... 18
 - Changing the language..... 18
 - Changing your password..... 18
- Maintaining the application..... 19**
 - Upgrading to MVE 3.5.....19
 - Backing up and restoring the database..... 19
 - Updating the installer settings after installation.....21
- Setting up user access.....23**
 - Understanding user roles.....23
 - Managing users..... 24
 - Enabling LDAP server authentication..... 24
 - Installing LDAP server certificates..... 26
- Discovering printers..... 28**
 - Creating a discovery profile..... 28
 - Managing discovery profiles..... 30
 - Sample scenario: Discovering printers.....30
- Viewing printers.....32**
 - Viewing the printer list..... 32
 - Viewing the printer information.....35

Exporting printer data.....	35
Managing views.....	36
Changing the printer listing view.....	38
Filtering printers using the search bar.....	38
Managing keywords.....	38
Using saved searches.....	38
Understanding printer life cycle states.....	38
Running a saved search	40
Creating a saved search.....	40
Understanding search rules settings	42
Managing saved searches	44
Sample scenario: Monitoring the toner levels of your fleet.....	44

Securing printer communications..... 46

Understanding printer security states.....	46
Securing printers using the default configurations.....	47
Understanding permissions and function access controls.....	49
Configuring printer security.....	49
Securing printer communications on your fleet.....	50
Other ways to secure your printers.....	51

Managing printers..... 52

Restarting the printer.....	52
Viewing the printer Embedded Web Server.....	52
Auditing printers.....	52
Updating printer status.....	52
Setting the printer state.....	53
Assigning configurations to printers.....	53
Unassigning configurations.....	53
Enforcing configurations.....	53
Checking the printer conformance with a configuration.....	54
Deploying files to printers.....	54
Updating the printer firmware.....	55
Uninstalling applications from printers.....	56
Assigning events to printers.....	56
Assigning keywords to printers.....	56
Entering credentials to secured printers.....	57
Configuring printer certificates manually.....	57

Removing printers.....	58
Managing configurations.....	59
Creating a configuration.....	59
Sample scenario: Deploying a configuration to printers.....	61
Creating a configuration from a printer.....	61
Sample scenario: Cloning a configuration.....	61
Creating an advanced security component from a printer.....	62
Generating a printable version of the configuration settings.....	62
Understanding variable settings.....	62
Configuring the color print permissions.....	63
Creating an applications package.....	63
Importing or exporting a configuration.....	64
Importing files to the resource library.....	64
Setting up MVE to manage certificates automatically.....	65
Understanding the automated certificate management feature.....	65
Configuring MVE for automated certificate management.....	66
Managing printer alerts.....	67
Creating an action.....	67
Understanding action placeholders.....	68
Managing actions.....	69
Creating an event.....	69
Understanding printer alerts.....	70
Managing events.....	74
Viewing task status and history.....	75
Viewing the task status.....	75
Stopping tasks.....	75
Viewing logs.....	75
Clearing logs.....	75
Exporting logs.....	75
Scheduling tasks.....	76
Creating a schedule.....	76
Managing scheduled tasks.....	77

Performing other administrative tasks..... 78

 Configuring general settings..... 78

 Configuring e-mail settings..... 78

 Adding a login disclaimer..... 78

 Signing the MVE certificate..... 79

 Removing user information and references..... 79

Frequently asked questions.....81

Troubleshooting.....84

 User has forgotten the password.....84

 Admin user has forgotten the password..... 84

 Page does not load.....85

 Cannot discover a network printer..... 85

 Incorrect printer information.....85

 MVE does not recognize a printer as a secured printer..... 86

 Enforcement of configurations with multiple applications fails in the first attempt but
 succeeds in the subsequent attempts..... 86

 Enforcement of configurations with printer certificate fails.....87

 Certificate issuance failed using the OpenXPKI CA server.....87

Appendix.....88

Notices..... 91

Glossary..... 93

Index..... 94

Change history

February 2020

- Updated information on the following:
 - Supported printer models
 - Supported servers
 - Supported databases
 - Valid 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 Markvision™ Enterprise (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 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

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 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 [“Setting up the database” on page 16](#).

User system requirements

Supported web browsers

- Microsoft Edge
- Internet Explorer 11 or later
- Mozilla Firefox (latest version)
- Google Chrome™ (latest version)
- 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 3330dn¹, 3333dn¹, 3335dn¹
- Dell 5230dn¹, 5350dn¹, 5530dn¹, 5535dn¹
- Dell B2360dn, B3460dn, B3465dn
- Dell B5460dn, B5465dnf, S5830dn
- Dell S2830dn
- Dell S5840cdn
- LexmarkTM 4600, 6500
- Lexmark B2338², B2442², B2546², B2650², B2865¹
- Lexmark B3440, B3442
- Lexmark C2132
- Lexmark C2240², C2325², C2425², C2535²
- Lexmark C3426
- Lexmark C4150², C6160², C9235²
- Lexmark C520¹, C522¹, C524¹, C530¹, C532¹, C534¹, C540³, C543³, C544³, C546³
- Lexmark C734¹, C736¹, C746, C748
- Lexmark C770¹, C772¹, C780¹, C782¹, C792
- Lexmark C920¹, C925¹, C935¹, C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS421², CS521², CS622²
- Lexmark CS431
- Lexmark CS720², CS725²
- Lexmark CS727², CS728², CX727²
- Lexmark CS820², CS827²
- Lexmark CS921², CS923², CS927²
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX421², CX522², CX622², CX625²
- Lexmark CX431
- Lexmark CX725

- Lexmark CX820², CX825², CX827², CX860²
- Lexmark CX920², CX921², CX922², CX923², CX924², CX927²
- Lexmark E250¹, E260³, E352¹, E360³, E450¹, E460¹, E462¹
- Lexmark Forms Printer 2580⁴, 2581⁴, 2590⁴, 2591⁴
- Lexmark M1140, M1145, M3150
- Lexmark M1242², M1246², M3250², M5255², M5265², M5270²
- Lexmark M5155, M5163, M5170
- Lexmark M5255², M5265², M5270²
- Lexmark MB2338², MB2442², MB2546², MB2650², MB2770²
- Lexmark MB3442
- Lexmark MC2325², MC2425², MC2535², MC2640²
- Lexmark MC3426
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321², MS421², MS521², MS621², MS622²
- Lexmark MS331, MS431
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725², MS821², MS822², MS823², MS824², MS825², MS826²
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611
- Lexmark MX317, MX417, MX517
- Lexmark MX321², MX421², MX521², MX522², MX622²
- Lexmark MX331, MX431
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721², MX722², MX725², MX822², MX824², MX826²
- Lexmark MX910, MX911, MX912
- Lexmark T640¹, T642¹, T644¹, T650¹, T652¹, T654¹, T656¹
- Lexmark W840¹, W850¹
- Lexmark X264³, X363³, X364³, X463¹, X464¹, X466¹
- Lexmark X543³, X544³, X546³, X548
- Lexmark X642¹, X644¹, X646¹, X651¹, X652¹, X654¹, X656¹, X658¹
- Lexmark X734¹, X736¹, X738¹, X746, X748, X792
- Lexmark X850¹, X852¹, X854¹, X860¹, X862¹, X864¹
- Lexmark X925, X940¹, X945¹, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235², XC2240², XC4240²
- Lexmark XC4140², XC4150², XC6152², XC8155², XC8160²
- Lexmark XC9225², XC9235², XC9245², XC9255², XC9265²

- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242², XM1246², XM3250²
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365², XM5370²
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355², MX7365², MX7370²
- 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 ST9530¹
- Source Technologies ST9620¹, ST9630¹
- Source Technologies ST9712, ST9715, ST9717, ST9720, ST9722, ST9730
- Source Technologies ST9815², ST9818², ST9820², ST9821², ST9822², ST9830²
- Toshiba e-Studio 305CP
- Toshiba e-Studio 388CP²
- Toshiba e-Studio 305CS, 306CS
- Toshiba e-Studio 338CS², 388CS², 389CS², 479CS²
- Toshiba e-Studio 385P, 470P
- Toshiba e-Studio 385S, 425S
- Toshiba e-Studio 408P², 478P²
- Toshiba e-Studio 408S², 448S², 478S²
- Toshiba e-Studio 520P, 525P
- Toshiba e-Studio 528P²

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:
 - 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	<ul style="list-style-type: none"> File write access to the following: <ul style="list-style-type: none"> – <code>\$MVE_INSTALL/tomcat/logs</code> – <code>\$MVE_INSTALL/tomcat/temp</code> – <code>\$MVE_INSTALL/tomcat/work</code> – <code>\$MVE_INSTALL/apps/library</code> – <code>\$MVE_INSTALL/apps/dm-mve/picture</code> – <code>\$MVE_INSTALL/./mve_truststore*</code> – <code>\$MVE_INSTALL/jre/lib/security/cacerts</code> – <code>\$MVE_INSTALL/apps/dm-mve/WEB-INF/ldap</code> – <code>\$MVE_INSTALL/apps/dm-mve/download</code> Where <code>\$MVE_INSTALL</code> is the installation directory. Windows privilege: LOGON_AS_A_SERVICE 	Administrator permissions
Database connection authentication	<ul style="list-style-type: none"> 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 make sure to 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.

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 [“Setting up user access” on page 23](#).

- 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 [“Changing your password” on page 18](#).
- 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 3.5

Before you begin the upgrade, make sure that you have a complete backup of the database and application files. For more information, see [“Backing up and restoring the database” on page 19](#).

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 3.5. The policy migration process is performed only when upgrading to MVE 2.0.

Valid upgrade path	1.6.x to 2.0 to 3.3 to 3.5 2.0 to 3.3 to 3.5
Invalid upgrade path	1.6.x to 3.5 2.0 to 3.5

- 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 19](#).

- 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 81](#).
- After upgrading, make sure to clear the browser cache before accessing the application again.
- When MVE is upgraded to version 3.5, 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 recommended that you back 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:

- 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\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 [step 1](#) of “[Backing up the database and application files](#)” on page 20.

- 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 Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB, Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB, and Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB files that you saved during the backup process.
- 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 20.

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

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 24](#). For more information on using LDAP user accounts, see [“Enabling LDAP server authentication” on page 24](#).

When adding users, roles must be assigned. For more information, see [“Understanding user roles” on page 23](#).

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 24](#).

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 23](#).

- 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 23](#).

- 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 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.

- **Allow nested user search**—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 should be left to the default value of **cn**.
- **Allow nested group search**—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 [“Understanding user roles” on page 23](#).
- 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, if you want to include the **admin** and **assets** groups for the Admin role, then 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 [“Enabling LDAP server authentication” on page 24](#).
- 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 text 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.

Address	Include/Exclude
10.194.25.70-77	Include
10.195.7.203	Include
10.195.0.208	Include

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

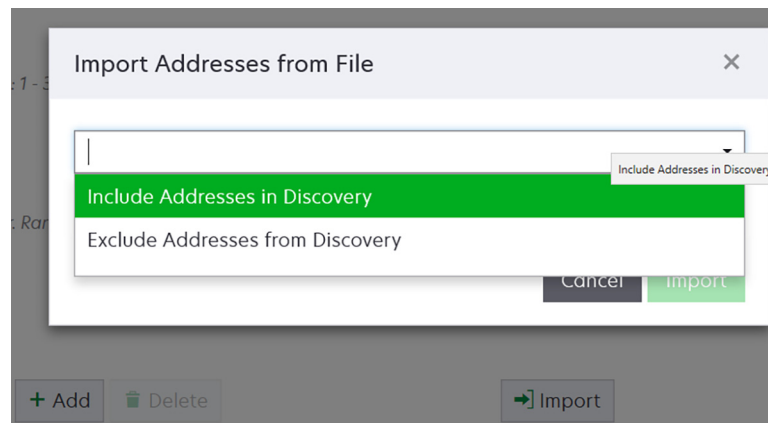
- **10.195.10.1** (single IPv4 address)
- **myprinter.example.com** (single host name)
- **10.195.10.3-10.195.10.255** (IPv4 address range)
- **10.195.*.*** (wildcards)
- **10.195.10.1/22** (IPv4 Classless Inter-Domain Routing or CIDR notation)
- **2001:db8:0:0:0:0:2:1** (full IPv6 address)
- **2001:db8::2:1** (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. 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 [“Creating a configuration” on page 59](#).

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

Note: A discovery can be scheduled to occur regularly. For more information, see [“Creating a schedule” on page 76](#).

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 [“Add the addresses” on page 28](#).
- 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.

Tasks ▾

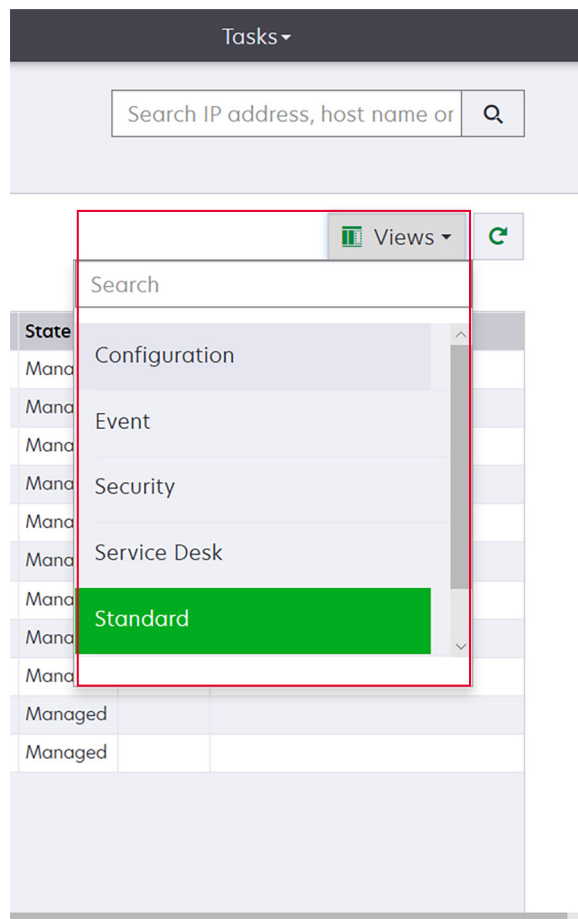
Search IP address, host name or

Q

Views ▾

State	Keyword	
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		
Managed		

- Change the printer listing view. For more information, see [“Changing the printer listing view” on page 38](#).



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.

The screenshot shows the 'Printers' configuration page. On the left, a sidebar contains filter categories: Keywords, Subnets, Supply Status Severity, Printer Status Severity, Configuration Conform..., and Model Names. The 'Subnets' filter is expanded, showing a list of subnets with checkboxes. The 'Supply Status Severity' filter is also expanded, showing 'Unknown supply status' selected. The main area displays a table of printers with columns for IP Address, Model, and Contact Name. The table shows 4 total items.

Filters: 157184.205* (4) ✕ Unknown supply status (4) ✕

4 total items

IP Address	Model	Contact Name
157184.205.135	Lexmark B2236dw	
157184.205.186	Lexmark CX922de	mvedev123
157184.205.212	Lexmark CX725	
157184.205.250	Lexmark MX611dhe	General > Contact Name123456

- Run a saved search. For more information, see [“Running a saved search” on page 40](#).

The screenshot shows the 'Printers' configuration page with the 'Run Saved Search' dropdown menu open. The menu lists various saved searches, including 'All Printers', 'Managed (Changed) Printers', 'Managed Printers', 'Managed (Found) Printers', 'Managed (Missing) Printers', 'Managed (Normal) Printers', 'New Printers', 'Retired Printers', 'Unmanaged Printers', and 'C2lite'. The 'All Printers' option is highlighted.

Run Saved Search

Search

All Printers

Managed (Changed) Printers

Managed Printers

Managed (Found) Printers

Managed (Missing) Printers

Managed (Normal) Printers

New Printers

Retired Printers

Unmanaged Printers

C2lite

- 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 [“Auditing printers” on page 52](#).

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 [“Understanding printer life cycle states” on page 38](#).

- **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 76](#).

Managing views

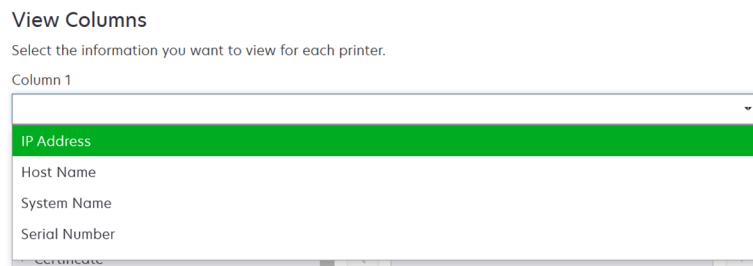
The Views feature lets you customize the information that is shown in the printer listing page.

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

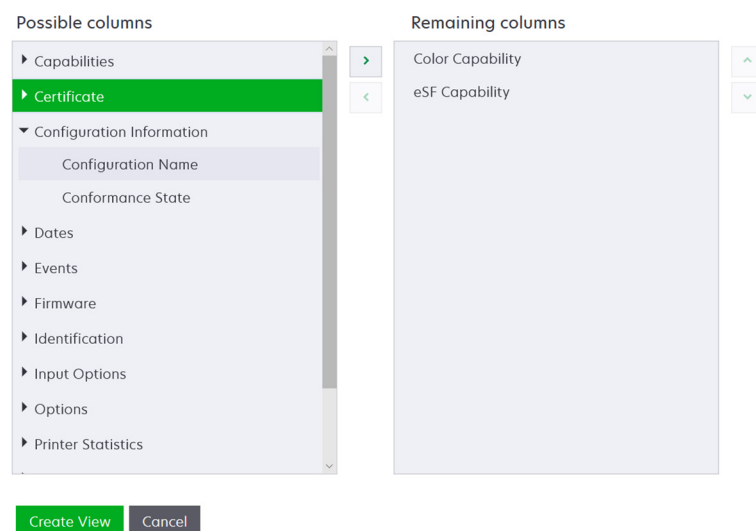
2 Do any of the following:

Create a view

- Click **Create**.
- Type a unique name for the view and its description.
- From the View Columns section, in the Column 1 menu, select the identifier column.



- 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 [“Managing views” on page 36](#).

- 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 **Manage 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 [“Assigning keywords to printers” on page 56](#).

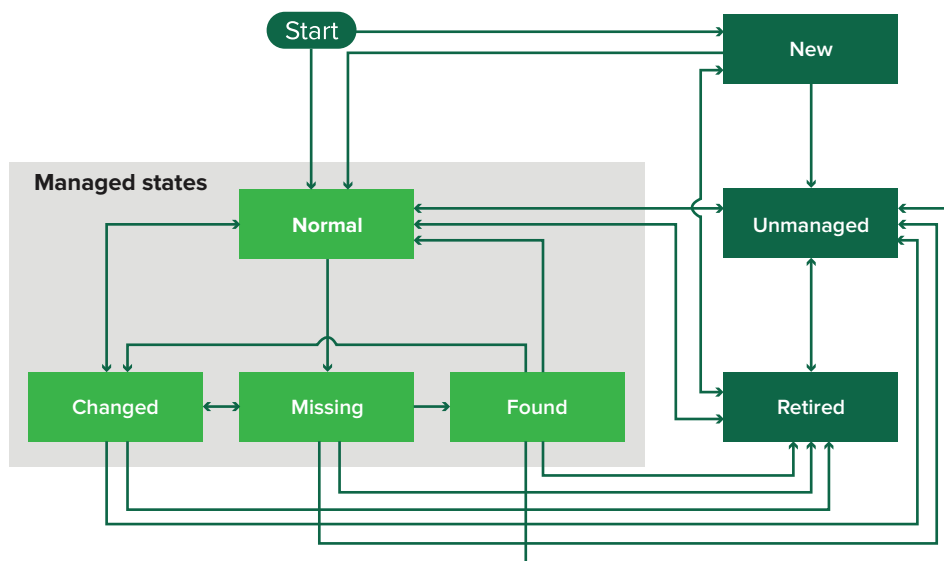
Using saved searches

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.

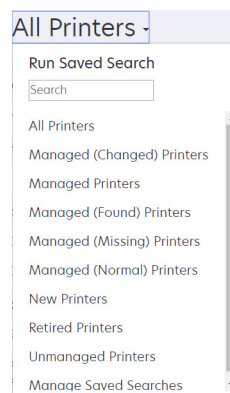
² The "Automatically manage discovered printers" setting is disabled in the discovery profile.

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 [“Understanding printer life cycle states” on page 38](#).

- 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.

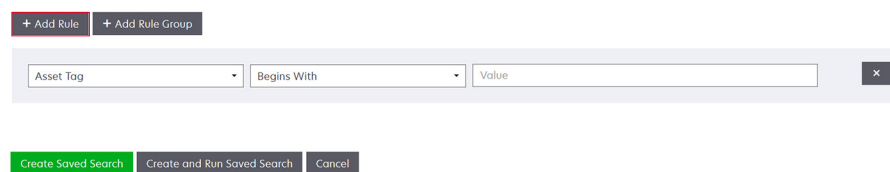
- 3 Click **Save**, and then type a unique name for your saved search and its description.
- 4 Click **Create Saved Search**.

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

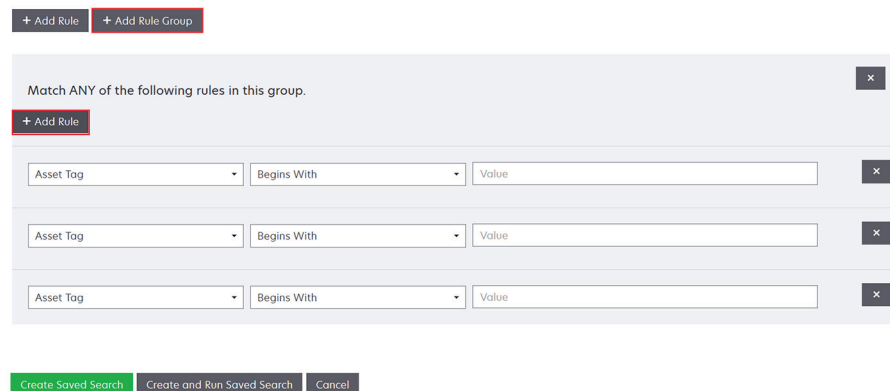
- a Click **Add Rule**.
- b Specify the parameter, operation, and value for your search rule. For more information, see [“Understanding search rules settings” on page 42](#).



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 42](#).
- 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. <ul style="list-style-type: none"> • 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.
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 whose parameters have 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 38](#).

- 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 38](#).

- 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.

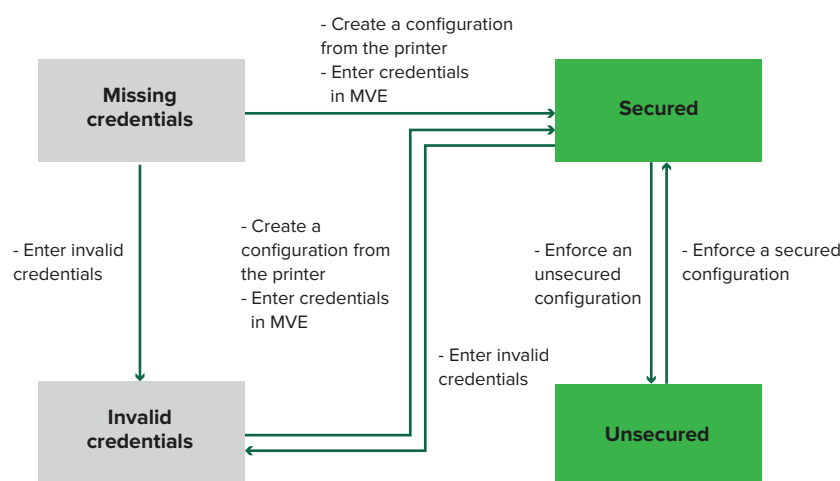
Note: The information shown in the printer listing view is based on the last audit. Perform an audit and status update to get the current printer status.

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**.

Printers ▾

Configurations ▾

Tasks ▾

Advanced Security Components

Delete Import Export

Name	Description	Type	Assigned	Last Modified
<input type="checkbox"/> Full account based authentication		Full account based authentication	No	Dec 12, 2019 1:15:48 PM
<input type="checkbox"/> Simple template based authentication		Partial template based authentication	No	Dec 12, 2019 1:15:47 PM

Full account-based authentication

This security component is not supported on the following printer models.

- Lexmark B3340, B3442, MS331, MS431
- Lexmark MB3442, MX331, MX431
- Lexmark C3426, CS431
- Lexmark CX431, MC3426

This security component contains a User Name/Password Local Account called **admin**.

Advanced Security Settings														
Group Permissions	Local Accounts	Network Accounts	Printer Credentials	Miscellaneous										
<div> <div>User Name/Password (1 accounts)</div> <table> <tr> <th>Name</th><th>E-mail</th><th>Groups</th><th>User name</th><th>Password</th></tr> <tr> <td>admin</td><td></td><td>All Users, Admin</td><td>admin</td><td>✓</td></tr> </table> <div>1 username/password accounts</div> </div>					Name	E-mail	Groups	User name	Password	admin		All Users, Admin	admin	✓
Name	E-mail	Groups	User name	Password										
admin		All Users, Admin	admin	✓										
Save Changes Discard Changes														

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 49](#).

Advanced Security Settings	
Group Permissions	Local Accounts
Groups (3)	Admin Permissions (52)
<div>Public</div> <div>All Users</div> <div>Admin</div>	Cancel Jobs Card Copy Change Languages Color Copy Color Dropout Copy Create Bookmarks Create Profiles Device Menu E-mail FTP Fax Firmware Updates Flash Drive Color Printing Flash Drive Printing Flash Drive Scan Forms and Favorites Held Jobs Import/Export Settings Manage Address Book Manage Shortcuts Network/Ports Menu New Solutions

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

Local Accounts
Network Accounts
Printer Credentials
Miscellaneous

Name	E-mail	Groups	User name	Password
admin		All Users, Admin	admin	

Advanced Security Settings

Group Permissions
Local Accounts
Network Accounts
Printer Credentials

Select the appropriate authentication method and enter the credentials. These credentials will be used by Markvision to communicate with the set configuration is assigned.

Authentication method

Password

Save Changes Discard Changes

Simple template-based authentication

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

Local Accounts
Network Accounts
Printer Credentials
Security Templates
Access Controls
Miscellaneous

Password (1 accounts)

Name	Admin Password	Password
Admin Password	Yes	

Advanced Security Settings

Local Accounts
Network Accounts
Printer Credentials
Security Templates
Access Controls
Miscellaneous

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

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 [“Understanding permissions and function access controls” on page 49](#).

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

Advanced Security Settings

Local Accounts
Network Accounts
Printer Credentials
Security Templates
Access Controls
Miscellaneous

Password (1 accounts)

Name	Admin Password	Password
Admin Password	Yes	

Advanced Security Settings

Local Accounts
Network Accounts
Printer Credentials
Security Templates

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

Authentication method

Password

Save Changes Discard Changes

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 47](#).

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 49](#).

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 28](#).

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

- 2 Create a configuration from a printer. For more information, see [“Creating a configuration from a printer” on page 61](#).
- 3 Assign the configuration to your fleet. For more information, see [“Assigning configurations to printers” on page 53](#).
- 4 Enforce the configuration. For more information, see [“Enforcing configurations” on page 53](#). 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 76](#).

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 76](#).

Setting the printer state

For more information on the printer states, see [“Understanding printer life cycle states” on page 38](#).

- 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 59](#).

- 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 53](#).

- 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 54](#).
- An enforcement can be scheduled to occur regularly. For more information, see [“Creating a schedule” on page 76](#).

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 53](#).

- 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 76](#).

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 76](#).

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 64](#).

- 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 46](#).

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 [“Importing files to the resource library” on page 64](#).

- 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 [“Managing printer alerts” on page 67](#).

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 [“Managing keywords” on page 38](#).

- 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**.
- 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

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 printers of the same model. 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
- Printer firmware
- Applications
- CA certificates

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

- Assign a configuration to printers of the same model. Configurations are model specific, and only one configuration can be assigned per printer.
- 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 if the printer is 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.

Creating a configuration

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

- 1 From the Configurations menu, click **All Configurations > Create**.
- 2 Select a printer model, and then click **Continue**.
- 3 Type a unique name for the configuration and its description.

4 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 62](#).

Settings

● Basic ● Advanced Security Firmware Apps Certificates

Use variable setting data file
None Import

☒ Show only included settings

View All settings Filter by setting name

Setting	Category	Value
<input checked="" type="checkbox"/> "Copy from" Size	Copy	Letter
<input checked="" type="checkbox"/> (Assign Type/Bin) Plain Paper Bin	Paper	Disabled

- 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 62](#).
- 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 61](#).
- From the Color Print Permissions tab, configure the settings. For more information, see [“Configuring the color print permissions” on page 63](#).

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 64](#).
- From the Apps tab, select one or more applications to deploy. For more information, see [“Creating an applications package” on page 63](#).

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

- From the CA Certificates tab, select one or more certificates to deploy. To import a certificate file, see [“Importing files to the resource library” on page 64](#).

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 66](#).

5 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**.

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.

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 Create or 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 [“Creating a configuration” on page 59](#).

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 files to the resource library” on page 64](#).

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.

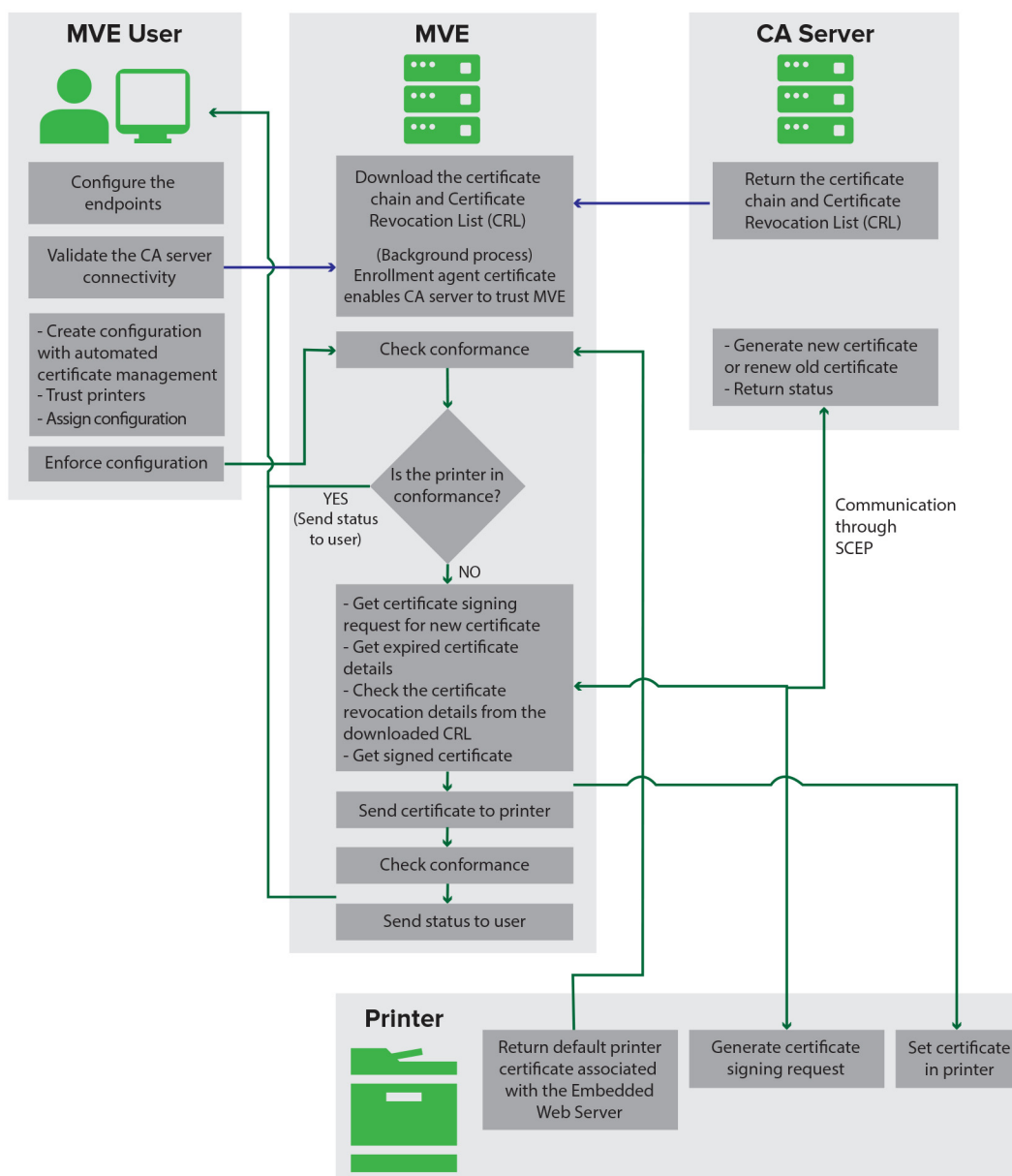
- 1** From the Configurations menu, click **Resource Library**.
- 2** Click **Choose File**, and then browse to the file.

Note: Only firmware files (.fls), application packages (.zip), and CA certificates (.pem) can be imported.
- 3** Click **Import Resource**.

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 the *OpenXPKI Certificate Authority Configuration Guide*.
- **Microsoft CA Enterprise**—For more information, see the *Microsoft Certificate Authority Configuration Guide*.

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 [“Configuring MVE for automated certificate management” on page 66](#).

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:

- [“Creating a configuration” on page 59](#)
- [“Enforcing configurations” on page 53](#)

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  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 the *OpenXPKI Certificate Authority Configuration Guide* or the *Microsoft Certificate Authority Configuration Guide*.

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 printer alerts

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 [“Configuring e-mail settings” on page 78](#).

- 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 [“Understanding action placeholders” on page 68](#).

The screenshot shows a web form for creating an action. At the top, there is a 'Type' dropdown menu with 'E-mail' selected. Below this are several input fields: 'From (Optional)' with the value 'admin@mycompany.com', 'To' with 'scott.summers@mycompany.com', and 'CC (Optional)' which is empty. The 'Subject (Optional)' field contains the placeholder '{alert.type}' and has a dropdown menu showing 'alert.type'. The 'Body' field contains the placeholder '{alert.type}\${alert.location}\${alert.name}' and has a dropdown menu showing 'alert.name'. At the bottom of the form are two buttons: 'Create Action' (green) and 'Cancel' (grey).

- 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 68](#).

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

About

alert.type
alert.location
alert.state
alert.name
configurationItem.manufacturer
configurationItem.contactLocation

- 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 [“Viewing logs” on page 75](#).
- 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 [“Understanding printer alerts” on page 70](#).

4 From the Actions section, select one or more actions to execute when the selected alerts are active.

Note: For more information, see [“Creating an action” on page 67](#).

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

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 of the currently running tasks are 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  on the upper-right corner of the page.
- b Click **TLS > Download**.
- c Select **Certificate signing request**.

Note: The certificate signing request does not include any Subject Alternative Names (SANs). To associate the server with multiple names, include the names when signing the certificate.

2 Use a trusted CA to sign the certificate signing request.

3 Install the CA-signed certificate.


- a Click  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  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  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 75](#).

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

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 [“Configuring general settings” on page 78](#).

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 [“Managing users” on page 24](#).

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 [“Understanding ports and protocols” on page 88](#).

Contact your Lexmark representative

Incorrect printer information

Perform an audit

For more information, see [“Auditing printers” on page 52](#).

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 [“Discovering printers” on page 28](#).

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.

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.

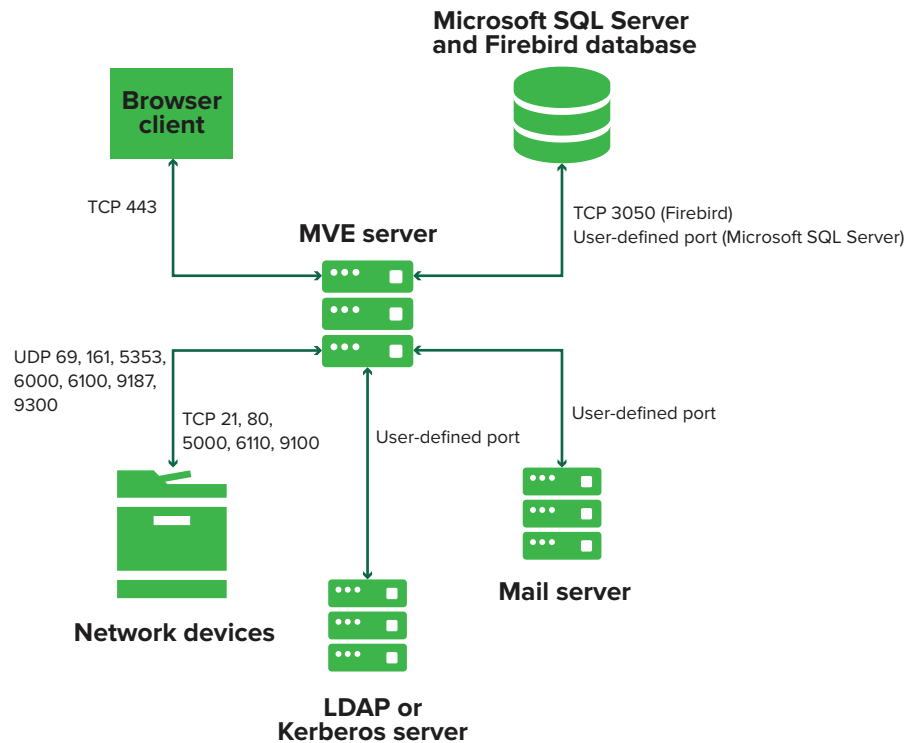
```
rule1:
    # Full DN
    Subject: CN=Markvision_SQA-2012-23AB.lrdc.lexmark.ds
```

For more information on configuring the OpenXPKI CA server, see the *OpenXPKI Certificate Authority Configuration Guide*.

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.

Notices

Edition notice

February 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 227.7202-4, 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 printers of the same model. 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

A

- accessing MVE 18
- action
 - placeholders 68
- action placeholders
 - understanding 68
- actions
 - creating 67
 - deleting 69
 - editing 69
 - managing 69
 - testing 69
- adding a login disclaimer 78
- admin user has forgotten the password 84
- advanced security component
 - creating 62
- AES256 encryption
 - configuring 81
- application log files
 - locating 81
- applications
 - uninstalling 56
- applications package
 - creating 63
- assigning a keyword 56
- assigning configurations to printers 53
- assigning events to printers 56
- auditing printers 52
- automated certificate management
 - configuring 66
- automated certificate management feature 65

B

- backing up and restoring the database 19
- best practices 10

C

- cannot discover a network printer 85
- certificate issuance failed using the OpenXPKI CA server 87
- certificate management 65

- change history 6
- changing the installer settings after installation 21
- changing the language 18
- changing the printer listing view 38
- changing your password 18
- checking printer conformance with a configuration 54
- ciphers
 - customizing 81
- clearing logs 75
- cloning configurations 61
- color print permissions
 - configuring 63
- configuration
 - conformance 54
 - creating 59, 61
 - exporting 64
 - importing 64
- configuration settings
 - printable version 62
- configurations
 - assigning 53
 - enforcing 53
 - unassigning 53
- configuring e-mail settings 78
- configuring general settings 78
- configuring MVE for automated certificate management 66
- configuring printer certificates manually 57
- configuring printer security 49
- configuring the color print permissions 63
- conformance
 - checking 54
- copying discovery profiles 30
- copying saved searches 44
- copying views 36
- creating a configuration 59
- creating a configuration from a printer 61
- creating a custom saved search 40
- creating a discovery profile 28
- creating a schedule 76
- creating an action 67

- creating an advanced security component from a printer 62
- creating an applications package 63
- creating an event 69
- creating keywords 38
- credentials
 - entering 57
- CSV
 - variable settings 62
- custom saved search
 - creating 40

D

- database
 - backing up 19
 - requirements 12
 - restoring 19
 - setting up 16
- database requirements 12
- default configurations 47
- deleting actions 69
- deleting discovery profiles 30
- deleting keywords 38
- deleting saved searches 44
- deleting schedules 77
- deleting views 36
- deploying configurations 61
- deploying files to printers 54
- discovering printers 30
- discovery profile
 - creating 28
- discovery profiles
 - copying 30
 - deleting 30
 - editing 30
 - managing 30
 - running 30

E

- editing actions 69
- editing discovery profiles 30
- editing keywords 38
- editing saved searches 44
- editing schedules 77
- editing views 36
- Embedded Web Server
 - viewing 52

- enabling LDAP server authentication 24
- enforcement of configurations with multiple applications fails in the first attempt but succeeds in the subsequent attempts 86
- enforcement of configurations with printer certificate fails 87
- enforcing configurations 53
- entering credentials to secured printers 57
- event
 - creating 69
- events
 - assigning 56
 - deleting 74
 - editing 74
 - managing 74
- exporting CSV
 - variable settings 62
- exporting logs 75
- exporting printer data 35
- e-mail action 67
- e-mail settings
 - configuring 78

F

- files
 - deploying 54
- filtering printers using the search bar 38
- Firebird database 16
- function access controls
 - understanding 49

G

- general settings
 - configuring 78

H

- host name lookup
 - reverse lookup 81

I

- importing CSV
 - variable settings 62
- importing files to the resource library 64
- importing or exporting a configuration 64
- incorrect printer information 85

- installation log files
 - locating 81
- installer settings
 - changing 21
- installing LDAP server certificates 26
- installing MVE 17

K

- keyword
 - assigning 56
- keywords
 - creating 38
 - deleting 38
 - editing 38
 - managing 38

L

- language
 - changing 18
- languages
 - supported 13
- LDAP server
 - enabling authentication 24
- LDAP server certificates
 - installing 26
- log event action 67
- log files
 - locating 81
- login disclaimer
 - adding 78
- logs
 - clearing 75
 - exporting 75
 - viewing 75

M

- managing actions 69
- managing discovery profiles 30
- managing events 74
- managing keywords 38
- managing saved searches 44
- managing schedules 77
- managing users 24
- managing views 36
- Microsoft Enterprise CA
 - configuring 81
- Microsoft SQL Server 16
- monitoring printers 44
- MVE
 - accessing 18

- installing 17
- upgrading to latest version 19
- MVE certificate
 - signing 79
- MVE does not recognize a printer as a secured printer 86

O

- overview 9

P

- page is loading infinitely 85
- password
 - changing 18
 - resetting 84
- permissions
 - understanding 49
- placeholders 67
- ports
 - configuring 81
 - understanding 88
- printer
 - conformance 54
 - restarting 52
- printer alerts
 - understanding 70
- printer certificates
 - configuring manually 57
- printer communications
 - securing 50
- printer data
 - exporting 35
- printer firmware
 - updating 55
- printer information
 - viewing 35
- printer life cycle states
 - understanding 38
- printer list
 - viewing 32
- printer listing view
 - changing 38
- printer security
 - configuring 49
- printer security states
 - understanding 46
- printer state
 - setting 53
- printer status
 - updating 52

- printers
 - auditing 52
 - deploying files 54
 - discovering 30
 - events 56
 - filtering 38
 - removing 58
 - securing 51
- protocols
 - understanding 88

R

- removing printers 58
- removing user information and references 79
- resource library
 - importing 64
- restarting the printer 52
- reverse DNS lookup 81
- run-as user
 - setting up 17
- running a saved search 40
- running discovery profiles 30

S

- saved searches
 - accessing 81
 - copying 44
 - deleting 44
 - editing 44
 - managing 44
 - running 40
- schedule
 - creating 76
- schedules
 - deleting 77
 - editing 77
 - managing 77
- search bar
 - filtering printers 38
- search rules
 - operators 42
 - parameters 42
- search rules settings
 - understanding 42
- secured printers
 - authenticating 57
- securing printer communications on your fleet 50
- securing printers 47, 51

- securing printers using the default configurations 47
- setting a default view 36
- setting the printer state 53
- setting up MVE as a run-as user 17
- setting up the database 16
- signing the MVE certificate 79
- stopping tasks 75
- supported databases 12
- supported languages 13
- supported models
 - configuration 81
- supported operating systems 12
- supported printer models 13
- supported servers 12
- supported web browsers 12

T

- task status
 - viewing 75
- tasks
 - stopping 75
- testing actions 69
- TLS versions
 - customizing 81
- troubleshooting
 - admin user has forgotten the password 84
 - cannot discover a network printer 85
 - certificate issuance failed using the OpenXPKI CA server 87
 - enforcement of configurations with multiple applications fails in the first attempt but succeeds in the subsequent attempts 86
 - enforcement of configurations with printer certificate fails 87
 - incorrect printer information 85
 - MVE does not recognize a printer as a secured printer 86
 - page is loading infinitely 85
 - user has forgotten the password 84

U

- unassigning configurations 53
- understanding action placeholders 68

- understanding printer alerts 70
- understanding printer life cycle states 38
- understanding printer security states 46
- understanding user roles 23
- uninstalling applications from printers 56
- updating printer status 52
- updating the printer firmware 55
- upgrading to the latest version of MVE 19
- user has forgotten the password 84
- user information
 - removing 79
- user roles
 - understanding 23
- user system
 - requirements 12
- user system requirements 12
- users
 - adding 24
 - deleting 24
 - editing 24
 - managing 24

V

- variable settings
 - understanding 62
- viewing logs 75
- viewing the printer Embedded Web Server 52
- viewing the printer information 35
- viewing the printer list 32
- viewing the task status 75
- views
 - copying 36
 - deleting 36
 - editing 36
 - managing 36

W

- web server
 - requirements 12
- web server requirements 12
- Windows firewall
 - adding rules 81