Markvision Enterprise

Version 3.2

Administrator's Guide

July 2018 **www.lexmark.com**

Contents

Change history

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 Markvision Enterprise 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

System requirements

Processor	At least 2GHz dual core processor that uses Hyper-Threading Technology (HTT)
RAM	At least 4GB
Hard disk drive	At least 60GB
Screen resolution	At least 1280 x 768 pixels

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

Supported operating systems

- Windows Server® 2016 Standard Edition
- Windows Server 2012 Standard Edition
- Windows Server 2012 R2
- Windows 10
- Windows Server 2008 R2
- Windows Server 2008 R2 via VMware ESX 3.5 U5
- Windows Server 2008 R2 via VMware vSphere 4 U1
- Windows 7
- Windows 7 on VMware ESX 3.5 Update 5
- Windows 7 on VMware vSphere 4 Update 1

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

Supported web browsers

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

Supported databases

- Firebird® database (built-in)
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008

Supported languages

- Brazilian Portuguese
- English

- French
- German
- Italian
- Simplified Chinese
- Spanish

Supported printer models

- Dell 3330dn, 3333dn, 3335dn
- Dell 5230dn, 5350dn, 5530dn, 5535dn
- Dell B2360dn, B3460dn, B3465dn
- Dell B5460dn, B5465dnf, S5830dn
- Dell S2830dn
- Dell S5840cdn
- Lexmark™ 4600, 6500
- Lexmark B2338*, B2442*, B2546*, B2650*, B2865*
- Lexmark C2132
- Lexmark C2240*, C2325*, C2425*, C2535*
- Lexmark C4150*, C6160*, C9235*
- Lexmark C520, C522, C524, C530, C532, C534, C540†, C543†, C544†, C546†
- Lexmark C734‡, C736‡, C746, C748
- Lexmark C770, C772, C780, C782, C792
- Lexmark C920, C925, C935, C950
- Lexmark CS310, CS410, CS510
- Lexmark CS317, CS417, CS517
- Lexmark CS421*, CS521*, CS622*
- Lexmark CS720*, CS725*
- Lexmark CS727*, CS728*, CX727 *
- Lexmark CS820*, CS827*
- Lexmark CS921*, CS923*, CS927*
- Lexmark CX310, CX410, CX510
- Lexmark CX317, CX417, CX517
- Lexmark CX421*, CX522*, CX622*, CX625*
- Lexmark CX725
- Lexmark CX820*, CX825*, CX827*, CX860*
- Lexmark CX920*, CX921*, CX922*, CX923*, CX924*, CX927*
- Lexmark E250, E260†, E352, E360†, E450, E460†, E462†
- Lexmark Forms Printer 2580§, 2581§, 2590§, 2591§
- Lexmark M1140, M1145, M3150
- Lexmark M1242*, M1246*, M3250*, M5255*, M5265*, M5270*
- Lexmark M5155, M5163, M5170

- Lexmark M5255*, M5265*, M5270*
- Lexmark MB2338*, MB2442*, MB2546*, MB2650*, MB2770*
- Lexmark MC2325*, MC2425*, MC2535*, MC2640*
- Lexmark MS310, MS312, MS315, MS410, MS415, MS510, MS610
- Lexmark MS317, MS417, MS517
- Lexmark MS321*, MS421*, MS521*, MS621*, MS622*
- Lexmark MS617, MS817, MS818
- Lexmark MS710, MS711, MS810, MS811, MS812
- Lexmark MS725*, MS821*, MS822*, MS823*, MS824*, MS825*, MS826*
- Lexmark MS911
- Lexmark MX310, MX410, MX510, MX511, MX610, MX611
- Lexmark MX317, MX417, MX517
- Lexmark MX321*, MX421*, MX521*, MX522*, MX622*
- Lexmark MX617, MX717, MX718
- Lexmark MX6500
- Lexmark MX710, MX711, MX810, MX811, MX812
- Lexmark MX721*, MX722*, MX725*, MX822*, MX824*, MX826*
- Lexmark MX910, MX911, MX912
- Lexmark T640, T642, T644, T650‡, T652‡, T654‡, T656‡
- Lexmark W840, W850‡
- Lexmark X264†, X363†, X364†, X463‡, X464‡, X466‡
- Lexmark X543, X544, X546, X548
- Lexmark X642‡, X644‡, X646‡, X651‡, X652‡, X654‡, X656‡, X658‡
- Lexmark X734‡, X736‡, X738‡, X746, X748, X792
- Lexmark X850‡, X852‡, X854‡, X860‡, X862‡, X864‡
- Lexmark X925, X940, X945, X950, X952, X954
- Lexmark XC2130, XC2132
- Lexmark XC2235*, XC2240*, XC4240*
- Lexmark XC4140*, XC4150*, XC6152*, XC8155*, XC8160*
- Lexmark XC9225*, XC9235*, XC9245*, XC9255*, XC9265*
- Lexmark XM1135, XM1140, XM1145, XM3150
- Lexmark XM1242*, XM1246*, XM3250*
- Lexmark XM5163, XM5170, XM5263, XM5270
- Lexmark XM5365*, XM5370*
- Lexmark XM7155, XM7163, XM7170, XM7263, XM7270
- Lexmark XM7355*, MX7365*, MX7370*
- Lexmark XM9145, XM9155, XM9165
- Pantum CM7105DN
- Pantum CM7000
- Pantum CP2300DN
- Pantum CP2500

- Pantum CP2500DN Plus
- Pantum M7600
- Pantum M7650DN
- Pantum P4000
- Pantum P4200DN
- Pantum P5000
- Pantum P5500DN
- Source Technologies ST9530
- Source Technologies ST9620, ST9630
- Source Technologies ST9712, ST9715, ST9717, ST9720, ST9722, ST9730
- Toshiba e-Studio 305CP
- Toshiba e-Studio 388CP*
- Toshiba e-Studio 305CS, 306CS
- Toshiba e-Studio 338CS*, 388CS*, 389CS*, 479CS*
- Toshiba e-Studio 385P, 470P
- Toshiba e-Studio 385S, 425S
- Toshiba e-Studio 408P*, 478P*
- Toshiba e-Studio 408S*, 448S*, 478S*
- Toshiba e-Studio 520P, 525P
- Toshiba e-Studio 528P*

* SNMPv3 support is required.

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

‡ 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**.

§ 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. 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

Note: The default sizes for the databases are 20MB for FRAMEWORK, and 4.5MB for MONITOR and QUARTZ. The FRAMEWORK table grows at 1KB for each printer record that is added.

- 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 make sure to enable the Microsoft SQL Server and the Windows Authentication mode on the Microsoft SQL Server.

  Notes:

  - 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.
  - 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.

Installing MVE

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.
- You can install MVE as an administrator or as a regular user.

1. Download the executable file into a path that does not contain any spaces.
2. Run the file, and then follow the instructions on the computer screen.

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 16.

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 12.
- 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. On the upper-right corner of the page, click your user name, and then click **Change password**.
2. Change the password.

Maintaining the application

Upgrading to MVE 3.2

Before upgrading to version 3.2, upgrade to version 2.0 first, and then to version 2.4. The policy migration process is performed only when upgrading to MVE 2.0.

Valid upgrade path	**1.6.x** to **2.0** to **2.4** to **3.2** **2.0** to **2.4** to **3.2**
Invalid upgrade path	**1.6.x** to **3.2** **2.1** to **3.2**

1. Back up your database.

   If the upgrade fails, then you can use this backup to revert the application to its previous state.

   Warning—Potential Damage: When you upgrade MVE, the database is changed, and some data may be lost. 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 13.

2. Download the executable file into a temporary location.
3. Run the file, 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 54.
   - After upgrading, make sure to clear the browser cache before accessing the application again.

Backing up and restoring the database

Backing up the database

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 Copy the following files to a safe repository:
- Lexmark\Markvision Enterprise\mve_encryption.jceks
- 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\apps\mve-data-service\WEB-INF\classes\userInit.properties

4 Do either of the following:
- If you are using a Firebird database, then copy the Lexmark\Markvision Enterprise\firebird\data\QUARTZ.FDB, Lexmark\Markvision Enterprise\firebird\data\MONITOR.FDB, and Lexmark\Markvision Enterprise\firebird\data\FRAMEWORK.FDB files to a safe repository. These files must be backed up regularly to avoid data loss.
- If you are using Microsoft SQL Server, then contact your Microsoft SQL Server administrator.

5 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

Warning—Potential Damage: When you upgrade MVE, the database may be changed, and some data may be lost. 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" on page 13.

2 Browse to the folder where Markvision Enterprise is installed.

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

3 Replace the following files with the files that you saved during the backup process:
- Lexmark\Markvision Enterprise\mve_encryption.jceks
- 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\apps\mve-data-service\WEB-INF\classes\userInit.properties

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

4 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 5 of "Backing up the database" on page 13.

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 credentials, such as user name and password.

1 Browse to the folder where Markvision Enterprise is installed.

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

2 Launch the Markvision Enterprise Password Utility in the Lexmark\Markvision Enterprise\ directory.

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

4 Do any of the following:

Change the run-as user settings

a From the MVE Service User Configuration section, select **Specific User**.

b Change the user name and password, and then click **Next**.

Update the Microsoft SQL Server settings

a Select a user type, and then click **Next**.

b From the Microsoft SQL Server Configuration section, update the settings, and then click **Next**.

5 Click **Finish**.

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 17. For more information on using LDAP user accounts, see “Enabling LDAP server authentication” on page 17.

When adding users, roles must be assigned. For more information, see “Understanding user roles” on page 16.

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 17.

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 16.

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 16.

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

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

3 From the Authentication Information section, configure the settings.

- **LDAP server hostname**—The IP address or the host name of the LDAP server where the authentication occurs. If you want to use encrypted communication between the MVE server and the LDAP server, then use the fully qualified domain name (FQDN).
- **Server port**—The port number that the local computer uses to communicate with the LDAP community server. MVE uses the port number to determine what type of encryption to use. The default port number is 389. If the default port number is used, then MVE begins its connection unencrypted. Otherwise, MVE begins its connection using SSL encryption.
- **Root distinguished name**—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 where the user groups that correspond to the MVE roles exist. 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**—The attribute that contains the full name of the group. For example, **`cn`**.
- **Allow nested group search**—The system searches all the nodes under the group search base.

4 From the Binding Information section, select a 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. The follow-up LDAP lookup session uses only unencrypted communication.
- **Simple**—The MVE server produces the specified credentials to the LDAP server to use the LDAP server lookup facility. If the server port is set to 389, then the communication with the LDAP server is unencrypted. If the port is set to any other value, then the communication is encrypted.
  a In the "Bind distinguished name" field, type the bind DN.
  b Type the bind password, and then confirm the password.
- **TLS**—The system uses Start TLS encrypted communication between the MVE server and the LDAP server. The MVE server fully authenticates itself to the LDAP server using the MVE server identity (bind DN) and credentials (bind password). TLS works only when using port 389.
  a In the "Bind distinguished name" field, type the bind DN.
  b Type the bind password, and then confirm the password.
- **Kerberos**—To configure the settings, do the following:
  a Click **Choose File**, and then browse to the krb5.conf file.
  b In the "Encryption method" menu, select whether to use SSL encryption.
  c Select the authentication type.

  If the authentication type is set to **KDC name/password**, then configure the settings.
  1 Type the Key Distribution Center (KDC) name.
  2 Type the KDC password, and then confirm the password.

  Note: If you want clients to log in using Windows Authentication, then use Kerberos authentication. A service principal name (SPN) and a keytab file must be created on the LDAP server. After the authentication method is set up, clients not on the localhost are authorized to use MVE based on their client account. To change the LDAP settings without a valid client account, access MVE from the localhost using a local administrator account. When using Kerberos authentication, the Test LDAP feature does not validate if the SPN or keytab files are properly set up, and the authentication may fail.

Note: For Simple, TLS, and Kerberos binding, MVE must trust the LDAP server certificate. For more information, see "Installing LDAP server certificates" on page 20.

5 From the "LDAP Groups to MVE Role Mapping" section, enter the names of the LDAP groups that correspond to the MVE roles.

Notes:

- For more information, see "Understanding user roles" on page 16.
- You can assign one LDAP group to multiple MVE roles, and you can also type more than one LDAP group in a role field.
- When typing multiple LDAP groups in the role fields, use the vertical bar character (|) to separate multiple LDAP groups. For example, if you want to include the **admin** and the **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.

6 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 17.
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.

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.

5 If necessary, from the Assign Configurations section, associate a configuration to a printer model. For information on creating a configuration, see "Creating a configuration" on page 37.

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

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 21.

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.

Managing printers

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 23.

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.
   - **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 24.
   - **Printer Credentials**—The credentials used in the configuration assigned to the printer.
   - **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.

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 50.

Updating printer status

The Update Status feature lets you update the printer status and supplies information.

1. From the Printers menu, click **Printer Listing**.
2. Select one or more printers.
3. Click **Printer** > **Update status**.

Setting the printer state

For more information on the printer states, see “Understanding printer life cycle states” on page 24.

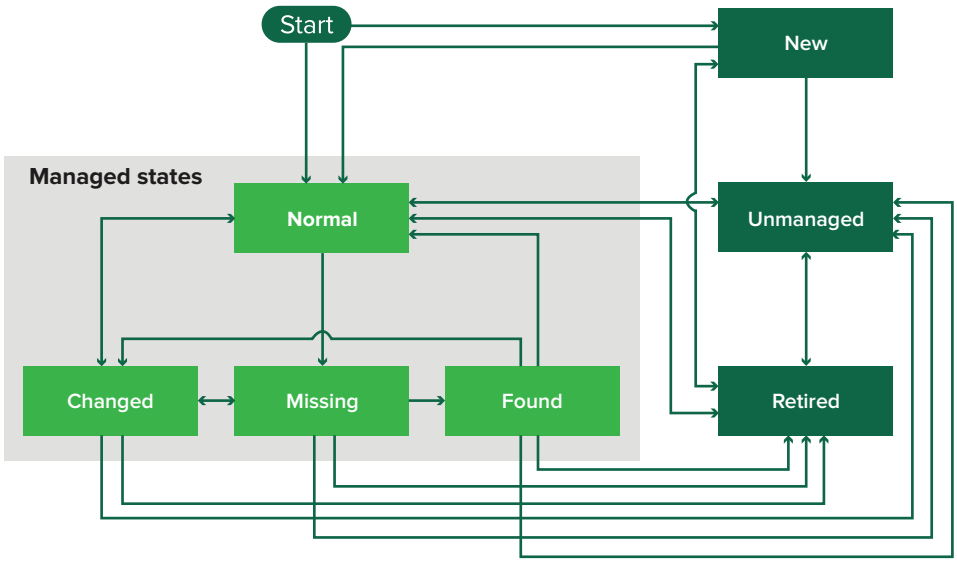
1. From the Printers menu, click **Printer Listing**.
2. Select one or more printers.
3. Click **Printer**, and then select one of the following:
   - **Set state to managed**—The printer is included in all activities that can be performed in the system.
   - **Set state to unmanaged**—The printer is 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.

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
- **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).
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.

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 37.

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.
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 26.

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 27.

Checking the printer conformance with a configuration

During a conformance check, MVE checks the printer settings, and verifies whether or not they match the assigned configuration. MVE does not make any 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 26.

1. From the Printers menu, click **Printer Listing**.
2. Select one or more printers.
3. Click **Configure** > **Check conformance**.

   Note: You can view the results in the task status page.

Deploying files to 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**.

   Note: 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.

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. Click **Choose File**, and then browse to the firmware file.
5. If necessary, to schedule the update, select **Define update window**, and then select the start time and the pause time.

   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**.

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 40.

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 41.

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 35.

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**.

Managing views

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

1. From the Printers menu, click **Views**.
2. Do any of the following:

Create a view

a. Click **Create**.
b. Type a unique name for the view and its description.
c. From the View Columns section, select the identifier column.
d. From the “Possible columns” section, select the information that you want to show as a column, and then click >.
e. Click **Create View**.

Edit a view

a. Select a view.
b. Click **Edit**, and then edit the settings.
c. Click **Save Changes**.

Note: You cannot edit system-generated views.

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.

Note: You cannot delete system-generated views.

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 29.

1. From the Printers menu, click **Printer Listing**.
2. Click **Views**, and then select a view.

Configuring printer certificates

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.

1. Generate the printer certificate signing requests.
   a. From the Printers menu, click **Printer Listing**.
   b. Select one or more printers.
   c. Click **Security** > **Generate printer certificate signing requests**.

   Note: This process lets only one printer certificate signing request to exist on the server at a time. If another request is generated, then the previous request is overwritten. Make sure to download the existing request before generating a new one.
2. Wait for the task to finish, and then download the printer certificate signing requests.
   a. From the Printers menu, click **Printer Listing**.
   b. Click **Security** > **Download printer certificate signing requests**.
3. Use a trusted CA to sign the certificate signing requests.
4. Save the signed certificates in a ZIP file.

   Note: All the signed certificates must be in the root location of the ZIP file. Otherwise, MVE cannot parse the file.
5. From the Printers menu, click **Printer Listing**.
6. Select one or more printers.
7. Click **Configure** > **Deploy file to printers**.
8. Click **Choose File**, and then browse to the ZIP file.
9. In the “File type” menu, select **Printer Certificates**.
10. Click **Deploy File**.

Filtering printers

There are multiple ways to find printers in MVE. From the Printer Listing page, do any of the following:

- Use the search box to search for an IP address, host name, system name, or serial number.
- Use the filters on the left side.
- Run a saved search.

If you are using the search box, then the application searches 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.

Filtering printers using the search bar

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

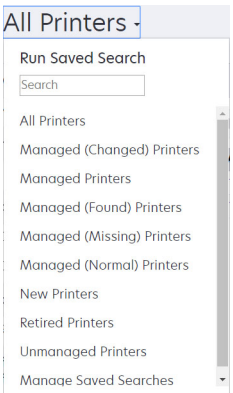
- To search for an IP address, make sure to type the complete IP address or range.

  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.

Running a saved search

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 32.

   ### 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 32.

   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.
Color Capability	The printer prints in color or black and white.
Configuration	The configuration name assigned to the printer.

Parameter	Description
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.
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 Name	The name of any eSF application installed on the printer.
ESF State	The state of any eSF application installed on the printer.
ESF Version	The version of any eSF application installed on the printer.
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.
Firmware:AIO	The AIO firmware version.
Firmware:Base	The base firmware version.
Firmware:Engine	The engine firmware version.
Firmware:Fax	The fax firmware version.
Firmware:Font	The font firmware version.
Firmware:Kernel	The kernel firmware version.
Firmware:Loader	The loader firmware version.
Firmware:Network	The network firmware version.
Firmware:Network Driver	The network driver firmware version.
Firmware:Panel	The panel firmware version.
Firmware:Scanner	The scanner firmware version.
Firmware Version	The printer firmware version.
Hostname	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.

Parameter	Description
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.
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 24.

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 24.

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

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 28.

Securing printer communications

By default, in MVE, communication with printers is unencrypted. In order to set up MVE to use encrypted communication, first set up the security on one printer. Rediscover that printer, create a configuration in MVE from it, and then edit the configuration to make it assignable. Lastly, assign the configuration to your fleet, and then enforce it.

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:
     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 **Remote Management**.
     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:
     a. From the Advanced Security Setup section, create a building block and a security template.
     b. Click **Access Controls**, and then if necessary, expand **Management**.
     c. In the Remote Management menu, select the security template.
     d. Click **Submit**.

Securing printer communications on your fleet

1. Discover a secured printer. For more information, see “Discovering printers” on page 21.

   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 37.
3. Assign the configuration to your fleet. For more information, see “Assigning configurations to printers” on page 26.
4. Enforce the configuration. For more information, see “Enforcing configurations” on page 26. A padlock symbol appears next to the secured printer.

Managing configurations

Creating a configuration

Note: 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 37.

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 Settings 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 38.
   - From the Color Print Permissions tab, configure the settings. For more information, see “Configuring the color print permissions” on page 38.

     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 40.
   - From the Apps tab, select one or more applications to deploy. For more information, see “Creating an applications package” on page 39.

     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 40.
5. Click **Create Configuration**.

Creating a configuration from a printer

1. From the Printers menu, click **Printer Listing**.
2. Select the printer, and then click **Configure** > **Create configuration from printer**.
3. Type a unique name for the configuration and its description, and then click **Create Configuration**.
4. From the Configurations menu, click **All Configurations**.
5. Select the configuration, and then click **Edit**.
6. By default, all settings are included in the configuration. If necessary, edit the settings.
7. From the Advanced Security tab, add the passwords and PINs.
8. Click **Save Changes**.

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 37.

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 from MVE using the Export Data feature.

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

b Select one or more printers, and then click **Printer** > **Export data**.

c In the “Select view for data export” menu, select **Printer List**.

d 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 40.

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**.

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.

Creating an action

An action is either an e-mail notification or a command-line operation. Actions assigned to events are triggered when a printer alert occurs. For a command action, MVE supports running an executable (.exe) file or a command interpreter, such as **`echo`** or **`dir`**.

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 52.

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 e-mail action placeholders" on page 42.
c. Click **Create Action**.

Command

a. In the Type menu, select **Command**.
b. In the Command Path field, type the name of an executable file or a command.
c. To add placeholders to the Command Parameters field, from the placeholders list, select a placeholder.

   Note: You can also add other parameters to be included in the command line.
d. Click **Create Action**.

Sample configuration for a command action

In this sample configuration, the command executes the Windows PowerShell script to log a Windows event for each triggered printer alert.

Command path: **`powershell.exe`**

Command parameters: **`-executionpolicy bypass -File "c:/Program Files/Lexmark/Markvision Enterprise/mve_alert.ps1" -IpAddress "${configurationItem.ipAddress}" -Alert "${alert.name}"`**

Sample Windows PowerShell Script

```
Param(
    [string] $IpAddress,
    [string] $Alert
)
if ([System.Diagnostics.EventLog]::SourceExists("Markvision Enterprise") -eq $False) {
        New-EventLog -LogName Application -Source "Markvision Enterprise"
}
Write-EventLog -LogName Application -Source "Markvision Enterprise" -EntryType Information `
-EventId 1 -Message "Alert for $IpAddress - $Alert"
```

Understanding e-mail 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 49.
- 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 43.

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 41.

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**.

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. Type the command path.
   By default, MVE adds the printer IP address, host name, serial number, status, status severity, and status type parameters to the command.

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 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**.

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 the communication between a server and a client. In MVE, SSL 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.

SSL 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.

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 **mve-*.log** and ***.isf** installation log files in the **%TEMP%** directory.

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 52.

How can I configure MVE to use AES256 or other stronger encryptions?

AES256 or other stronger encryptions require files that are not available in every country. If you have access to the necessary files, then you can enable this feature. To enable the feature, do the following:

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. Go to **www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html**, and then download the **jce_policy.jar** file.

3. Copy the **jce_policy.jar** file to the ***installation_dir*/Lexmark/Markvision Enterprise/jre/lib/security** directory.
4. Create a directory to save the existing **local_policy.jar** and **US_export_policy.jar** files. For example, create a directory named **original**, and then save the files in that directory.
5. Decompress the downloaded **jce_policy.jar** file, and then save the **local_policy.jar** and **US_export_policy.jar** files to the ***installation_dir*/Lexmark/Markvision Enterprise/jre/lib/security** directory, replacing the ones that you copied and saved.
6. 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 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/tomcat8.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.

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.

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 58.

Contact your Lexmark representative

Incorrect printer information

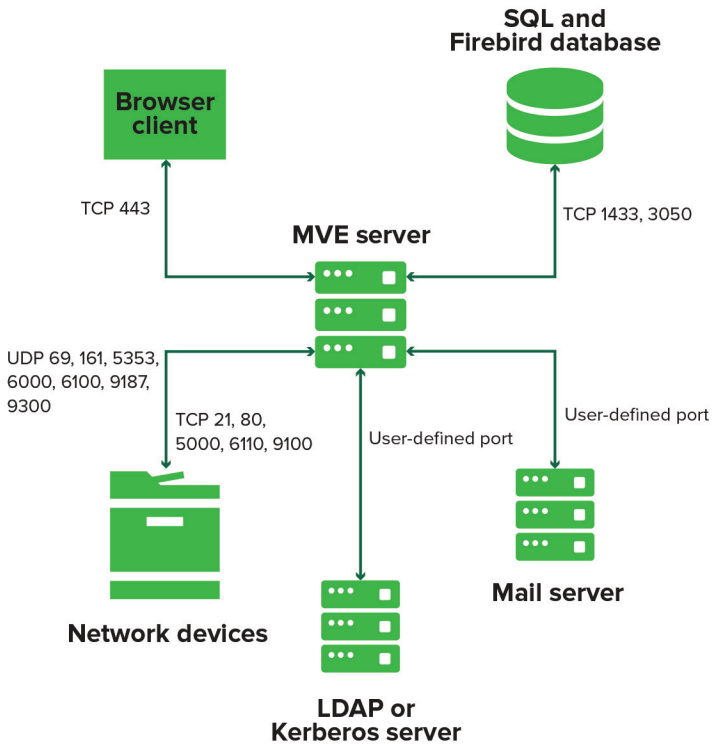
Perform an audit

For more information, see “Auditing printers” on page 23.

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

July 2018

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, visit **http://support.lexmark.com**.

For information on supplies and downloads, visit **www.lexmark.com**.

Trademarks

Lexmark, the Lexmark logo, and Markvision are trademarks or registered trademarks of Lexmark International, Inc. in the United States and/or other countries.

Microsoft, Windows Server, Microsoft Edge, Internet Explorer, SQL Server, and PowerShell are either registered trademarks or trademarks of the Microsoft group of companies in the United States and other countries.

Google Chrome is a trademark of Google Inc.

Safari is a registered trademark of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software

Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

JmDNS License

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

** JmDNS

Licensing notices

All licensing notices associated with this product can be viewed from the program folder.

Glossary

action	An e-mail notification or a command-line operation. Actions assigned to events are triggered when a printer alert occurs.
audit	The task of collecting printer data such as printer status, supplies, and capabilities.
configuration	A collection of settings that can be assigned and enforced to a printer or a group of 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

U

V

W