Markvision Enterprise

User's Guide

January 2016

www.lexmark.com

Contents

Overview

Use *Markvision™ Enterprise* (MVE) to monitor and manage a fleet of printers and print servers. This application is a Web-enabled device management utility designed for IT professionals. MVE works as a client/server application. The server discovers and communicates with devices on the network and provides information about them to the client. The client provides device information and a user interface to manage those devices. Each Markvision server can manage thousands of devices at one time.

Built-in security provisions prevent unauthorized access to the application and allow only authorized users to use the client to access management options.

In *Information Technology Infrastructure Library* (ITIL), printers and print servers are also known as *Configuration Items* (CIs). Within this document, CIs, printers, and print servers are sometimes called devices.

Getting started

Note: For a list of system requirements and of supported database servers, operating systems, and Web browsers, see the *Release Notes*.

Installing Markvision

Preparing the database

You can use either Firebird® or Microsoft® SQL Server® as the back-end database. If you are using Microsoft SQL, then before installing Markvision, do all of the following:

- Enable mixed mode authentication and Auto Run.
- Set the Network Libraries to use a static port and TCP/IP sockets.
- Create a user account that Markvision uses to set up the database schema and any database connections.
- Create the following databases:
  - FRAMEWORK
  - MONITOR
  - QUARTZ

  Note: The account you created must be the owner of these databases or have the privileges to create a schema and perform *Data Manipulation Language* (DML) operations.

Installing the application

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.

Note: Markvision installs and uses its own version of Tomcat regardless of any existing version already installed.

Upgrading to the latest version of Markvision

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.

Valid upgrade path	**1.6.x** to **2.0.x** to **2.1.x** or later **2.0.x** to **2.1.x** or later
Invalid upgrade path	**1.6.x** to **2.1.x** **1.9.x** to **2.2.x**

Note: For MVE versions 1.6.x up to 1.9.x, make sure to upgrade to MVE 2.0 before upgrading to MVE 2.1 or later. Migrating policies to configurations is supported only in MVE 2.0.

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 may be changed. Do not restore a database backup that was created from a previous version.

Notes:

- If you are using a Firebird database, then see "Backing up the Firebird database" on page 7 for more information.
- If you are using Microsoft SQL, then contact your Microsoft SQL administrator.

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 devices 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 devices. 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 47.
- After upgrading, make sure to clear the browser cache and flash cache before accessing the application again.

Backing up and restoring the Firebird database

Backing up the Firebird database

Note: If you are using Microsoft SQL as your database, then contact your Microsoft SQL administrator.

1 Stop the Markvision Enterprise service.

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

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

2 Locate the folder where Markvision Enterprise is installed, and then navigate to **firebird\data**.

   For example, **`C:\Program Files\Lexmark\Markvision Enterprise\firebird\data`**

3 Copy the following databases to a safe repository.

   - FRAMEWORK.FDB
   - MONITOR.FDB
   - QUARTZ.FDB

4 Restart the Markvision Enterprise service.

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

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

Restoring the Firebird database

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.

Note: If you are using Microsoft SQL as your database, then contact your Microsoft SQL administrator.

1. Make sure that you have completed the backup process for the Firebird database.
2. Stop the Markvision Enterprise service.

   For more information, see step 1 of "Backing up the Firebird database" on page 7.
3. Locate the folder where Markvision Enterprise is installed, and then navigate to **firebird\data**.

   For example, **`C:\Program Files\Lexmark\Markvision Enterprise\firebird\data`**
4. Replace the following databases with the databases that you saved during the backup process.
   - FRAMEWORK.FDB
   - MONITOR.FDB
   - QUARTZ.FDB
5. Restart the Markvision Enterprise service.

   For more information, see step 4 of "Backing up the Firebird database" on page 7.

Accessing Markvision

You can access MVE using several login methods such as LDAP, Kerberos, or local accounts, depending on your configuration.

For Kerberos authentication, you can access MVE using a smart card. MVE uses Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO), which provides a mechanism for extending a Kerberos-based single sign-on (SSO) environment to Web applications.

Using Kerberos authentication

Notes:

- Before accessing MVE, make sure that your Web browser supports SPNEGO authentication. For more information, see the online references for your Web browser. For a list of supported Web browsers, see the *Release Notes*.
- To enable Kerberos authentication in MVE, see "Enabling Kerberos authentication" on page 43.

1. From your computer, log in using a smart card.
2. Open a Web browser, and then do either of the following:
   - Type **`http://MVE_SERVER:9788/mve/`**, where ***`MVE_SERVER`*** is the host name or IP address of the server hosting MVE.
   - If SSL is enabled, then type **`https://MVE_SERVER:8443/mve/`**, where ***`MVE_SERVER`*** is the host name or IP address of the server hosting MVE.

   Note: The default port numbers are 9788 and 8443, and they may differ depending on your configuration.
3. If necessary, accept the disclaimer.

Using LDAP or local accounts

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

1. Open a Web browser, and then do either of the following:
   - Type **`http://MVE_SERVER:9788/mve/`**, where ***`MVE_SERVER`*** is the host name or IP address of the server hosting MVE.
   - If SSL is enabled, then type **`https://MVE_SERVER:8443/mve/`**, where ***`MVE_SERVER`*** is the host name or IP address of the server hosting MVE.

   Note: The default port numbers are 9788 and 8443, and they may differ depending on your configuration.
2. If necessary, accept the disclaimer.
3. Type your login credentials.

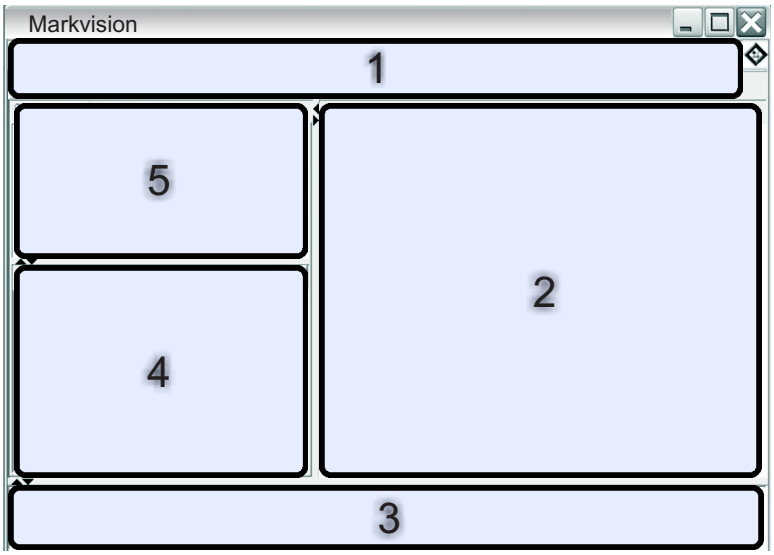
   Note: Use the login credentials that you created during the MVE installation.

Using Markvision

The features and functions of Markvision are divided into four service areas, showing only the features and functions needed for a task. Each service area is accessible from the home screen and corresponds to a service life cycle stage in the ITIL version 3. The ITIL discipline is globally recognized for its compilation of best practices for managing IT resources within an organization.

Use	To
Assets	• Locate, identify, catalog, organize, and track the physical assets that comprise the printer fleet. • Gather and maintain information on the fleet models, capabilities, installed options, and life cycle. **Note:** In ITIL, this area fits into the Service Transition area. If your responsibilities include management of IT assets, then go to "Managing assets" on page 14.
Configurations	• Define and manage configurations such as importing, exporting, or assigning configurations to selected devices. • Run a conformance check or enforce configurations to selected devices. • Deploy eSF apps, including licenses, to the printer fleet. **Note:** In ITIL, this tab fits into the Service Transition area. If your responsibilities include administration and maintenance of configuration management tools, then go to "Managing configurations" on page 25.
Service Desk	• Directly interact with a single device in the printer fleet. • Remotely manage the device, run a conformance check, enforce configurations, and customize configuration settings through the device Embedded Web Server. **Note:** In ITIL, this tab fits into the Service Operation area. If your responsibilities include management or administration of customer IT support service, then go to "Managing the service desk" on page 32.
Event Manager	Create an automated event when a device sends an alert to the network. You can send an e-mail or perform other scripted actions to notify identified personnel. **Note:** In ITIL, this tab fits into the Service Operation area. If your responsibilities include problem management or incident handling, then go to "Managing device events" on page 34.

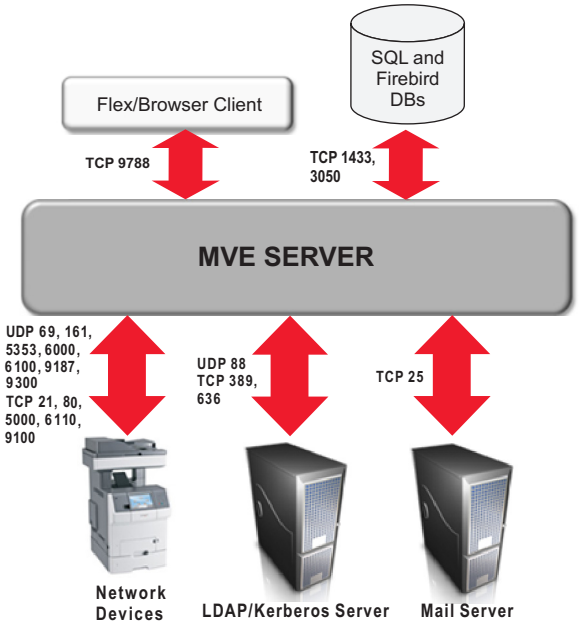
Understanding the home screen



Use this area		To
1	Header	Access the four service area tabs and perform other administrative tasks.
2	Search Results	View the full, paged list of devices matching the currently selected bookmark or search.
3	Task Information	View the status of the most recent activity.
4	Search Results Summary	View a categorized summary of the currently selected bookmark or search.
5	Bookmarks and Advanced Search	Manage and select bookmarks, and refine search queries.

Understanding ports and protocols

MVE uses different ports and protocols for several types of network communication, as shown in the following diagram.



Note: The ports are bidirectional and must be open or active for MVE to function properly. Make sure that all device ports are set to either **Secure and Unsecure** or **Enabled**, depending on the device.

Server-to-device communication

Ports and protocols used during communication from the MVE server to network devices

Protocol	MVE server	Device	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
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 certain Lexmark network printers and determining the security capabilities of devices
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	Downloading generic files

Protocol	MVE server	Device	Used for
Trivial File Transfer Protocol (TFTP)	Ephemeral UDP port	UDP 69	Updating firmware and downloading generic files
Hypertext Transfer Protocol (HTTP)	Ephemeral TCP port	TCP 80	Downloading generic or configuration files
		TCP 443	Downloading generic or configuration files
Hypertext Transfer Protocol over SSL (HTTPS)	Ephemeral TCP port	TCP 161 TCP 443	Downloading generic or configuration files
RAW	Ephemeral TCP port	TCP 9100	Downloading generic or configuration files

Device-to-server communication

Port and protocol used during communication from network devices to the MVE server

Protocol	Device	MVE server	Used for
NPAP	UDP 9300	UDP 9187	Generating and receiving alerts

Serve-to-database communication

Ports used during communication from the MVE server to databases

MVE server	Database	Used for
Ephemeral TCP port	TCP 1433 (SQL Server) The default port and can be configured by the user	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 flex or browser client to the MVE server

Protocol	Flex/Browser Client	MVE server
Action Message Format (AMF)	TCP port	TCP 9788

Messaging and alerts

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	TCP 25 The default port and can be configured by the user	Providing the e-mail functionality used to receive alerts from devices

MVE-server-to-LDAP-server communication

Ports and protocols used during communication involving user groups and authentication functionality

Protocol	MVE server	LDAP server	Used for
Lightweight Directory Access Protocol (LDAP)	Ephemeral TCP port	TCP 389, or the port to which the LDAP server has been configured to listen	Authenticating MVE users using an LDAP server
Secure LDAP (LDAPS)	Ephemeral TCP port	Transport Layer Security (TLS), or the port to which the LDAP server has been configured to listen Used for TLS-encrypted connections	Authenticating MVE users using an LDAP server through a secure channel that uses TLS
Kerberos	Ephemeral UDP port	UDP 88 The default Kerberos Authentication Service port	Authenticating MVE users using Kerberos

Managing assets

Discovering devices

You can search the network for devices and save their identification information in the system. Use bookmarks to show devices in the results area. For more information, see “Searching for devices within the system” on page 20.

To add devices to the system, use a discovery profile or import a CSV file. Discovery profiles let you find devices using network parameters, and automatically assign and enforce configurations to those devices.

Notes:

- By default, discovered devices are set to **New**.
- Before you perform any action on a device, set it to **Managed**. For more information, see “Managing devices” on page 17.

Adding or editing a discovery profile

1. From the Assets tab, click **Discovery Profiles**.
2. Click ✚ or  to add or edit a discovery profile.

   If necessary, type a unique name for the discovery profile.
3. From the Addresses tab, select **Include** or **Exclude**, and then do either of the following:
   - In the text field, type a device IP address, fully qualified DNS host name, subnet with wildcard characters, or IP address range, and then click ✚. To view examples of valid formats, mouse over the text field.

     Notes:

     - You can type only one entry at a time.
     - When typing IP address ranges, do not use wildcard characters.
   - Click  , and then browse to the CSV file.

     The file can contain a list of device IP addresses or host names. To view examples of valid formats, mouse over the text field.
4. From the SNMP tab, select **Version 1,2c** or **Version 3**, and then do either of the following:
   - For **Version 1,2c**, from the Community Names area, set the privacy profile.
   - For **Version 3**, from the Security area, set the security profile.

   Note: For more information on configuring SNMP, contact your administrator.
5. From the General tab, configure the following:
   - **Timeout**—Specify how long the system waits for the devices to respond.
   - **Retries**—Specify how many times the system attempts to communicate with a device before it stops.

- **Include secured printers in the discovery**—Include secured devices when executing the discovery profile. If you do not have a secured device, then do not select this option to avoid performance issues during discovery. For more information on secured devices, see "Understanding secured devices" on page 27.
- **Automatically manage discovered devices**—By default, this option is selected in new discovery profiles. If the discovery profile contains at least one configuration associated with a specified printer model, then this option cannot be modified.

  Note: This feature applies only to newly discovered devices. To manage devices that were already discovered, set each device to a managed state manually, or delete and rediscover them.

6 From the Configurations tab, select a printer model and a configuration, and then click ✚.

Note: During discovery, the configuration is assigned and enforced automatically. Automatic configuration applies only to devices that have no configurations assigned to them.

7 Click **Save**.

Notes:

- Clicking ▶ executes the discovery profile but does not save it.
- A new discovery profile collects basic information to identify a device. To collect the complete information from a device, set it to **Managed**, and then perform an audit.
- To make sure that the device information is current, schedule a regular discovery. For more information, see "Scheduling tasks" on page 44.

Cloning a discovery profile

Note: When you clone a discovery profile, the settings are copied except for the device addresses.

1 From the Assets tab, click **Discovery Profiles**.

2 Click  .

If necessary, type a unique name for the discovery profile.

3 From the Addresses tab, select **Include** or **Exclude**, and then do either of the following:

- In the text field, type a device IP address, fully qualified DNS host name, subnet with wildcard characters, or IP address range, and then click ✚. To view examples of valid formats, mouse over the text field.

  Notes:

  - You can type only one entry at a time.
  - When typing IP address ranges, do not use wildcard characters.

- Click  , and then browse to the CSV file.
  The file can contain a list of device IP addresses or host names. To view examples of valid formats, mouse over the text field.

4 If necessary, modify the SNMP settings, general settings, and configurations.

5 Click **Save**.

Notes:

- Clicking ▶ executes the discovery profile but does not save it.

- A new discovery profile collects basic information to identify a device. To collect the complete information from a device, set it to **Managed**, and then perform an audit.
- To make sure that the device information is current, schedule a regular discovery. For more information, see “Scheduling tasks” on page 44.

Importing devices from a file

Use a comma-separated values (CSV) file to import devices.

Note: In preparation for a deployment, MVE lets you add devices into the system even before these devices are available on the network.

1. From the Assets tab, click **Import**, and then browse to the CSV file.

   Note: Make sure that each line of the CSV file represents a single device.

2. From the Possible Columns section, select the columns to match the values in your CSV file.

3. If you are using SNMP V3 protocol to communicate with the device, then select the following columns:
   - **SNMP V3 Read/Write User**
   - **SNMP V3 Read/Write Password**
   - **SNMP V3 Minimum Authentication Level**
   - **SNMP V3 Authentication Hash**
   - **SNMP V3 Privacy Algorithm**

   Note: In the CSV file, make sure that the following parameters contain one of the values specified below them:
   - Minimum Authentication Level
     - **NO_AUTHENTICATION_NO_PRIVACY**
     - **AUTHENTICATION_NO_PRIVACY**
     - **AUTHENTICATION_PRIVACY**
   - Authentication Hash
     - **MD5**
     - **SHA1**
   - Privacy Algorithm
     - **DES**
     - **AES_128**

   Note: If your CSV file does not contain the exact values specified, then MVE cannot discover the device.

4. Click **Add** to move the selected columns into the CSV File Columns section.
   - If you want the system to ignore a column in your CSV file, then select **Ignore**. Do this step for each column in your CSV file that is not listed in the Possible Columns section.
   - To change the order of the columns you selected to match your CSV file, select a column from the CSV File Columns section. Use the arrows to move the headings up or down.

5. Select whether the first row in your CSV file contains a header.

6. Select whether the imported devices should be automatically set to the **Managed** life cycle state.

7. Click **OK**.

Managing devices

A device can be assigned three different life cycle states:

- **Managed**—This includes the device in all activities that can be performed in the system.
  - **Managed (Normal)**—The device is in its steady state.
  - **Managed (Changed)**—There are changes in the physical property of the device since the last audit. The next time the system communicates with the device and there are no more changes in its physical properties, the device reverts to Managed (Normal) state.
  - **Managed (Missing)**—The system cannot successfully communicate with the device. The next time the system is able to successfully communicate with the device and there is no change in its physical properties, the device reverts to Managed (Found) state.
  - **Managed (Found)**—The device is previously missing, but is able to successfully communicate with the system in its most recent attempt. The next time the system is able to successfully communicate with the device and there are no changes in its physical properties, the device reverts to Managed (Normal) state.
- **Unmanaged**—This excludes the device from all activities performed in the system.
- **Retired**—The device is previously in Managed state, but has now been removed from the network. The system retains the device information, but does not expect to see the device on the network again. If the device appears again in the network, then the system sets its state to New.

Setting the device life cycle state

Before any action can be done on a device, make sure the device is set to **Managed**.

1. From the Assets tab, select **New Printers** from the Bookmarks and Searches drop-down menu.
2. Select the check box beside the IP address of the device.

   Note: You may select multiple or all devices.
3. From the “Set State To” drop-down menu, select **Managed**, and then click **Yes**.

Auditing a device

An audit collects information from any currently Managed device on the network, and then stores the device information in the system. To make sure the information in your system is current, perform an audit regularly.

1. From the Search Results area, select the check box beside the IP address of a device.

   Notes:

   - If you do not know the IP address of the device, then locate the device under the System Name or Hostname column.
   - To audit multiple devices, select the check boxes beside the IP addresses of the devices.
   - To audit all devices, select the check box beside “IP Address.”
2. Click **Audit**.

   The audit status appears in the Task Information area.

3 When the audit is complete, click  in the Header area.

Results of the most recent audit appear in the Log dialog.

After devices are audited, the following instances may prompt the system to set a device to a **Managed (Changed)** state:

- There are changes to any of these device identification values or device capabilities:
  - Property tag
  - Host name
  - Contact name
  - Contact location
  - IP address
  - Memory size
  - Copier option name
  - Duplex
- There are additions to, or removals of, any of these device hardware options:
  - Supplies
  - Input options
  - Output options
  - Ports
- There are additions to, or removals of, any of these device functions or applications:
  - Fonts
  - eSF applications

Note: An audit can be scheduled to occur at a predetermined time or on a regular basis. For more information, see “Scheduling tasks” on page 44.

Viewing device properties

To see the complete list of information on the device, make sure that you have already performed an audit of the device.

1 From the Assets tab, in the Bookmarks and Searches menu, select **Managed Printers**.

2 From the All Printers section, select the IP address of the device.

Note: If you do not know the IP address of the device, then locate the device under the System Name column.

3 From the Asset Properties dialog:

Click	To view
Identification	The device network identification information.
Dates	The list of device events. This list includes the date added to the system, discovery date, and the most recent audit date.
Firmware	The device firmware code levels.
Capabilities	The device features.

Click	To view
Supplies	The device supply levels and details.
Options	Information about the device options, such as the device hard disk and its remaining free space.
Input Options	Settings for the available paper trays and other device inputs.
Output Options	Settings for the available paper bin.
eSF Applications	Information about the installed Embedded Solutions Framework (eSF) applications on the device, such as version number and status.
Device Statistics	Specific values for each of the device properties.
Change Details	Information about the changes in the device. **Note:** This feature applies only to devices that are set in the **Managed (Changed)** state.
Device Credentials	The credentials used in a configuration. **Note:** To manage the security settings, see “Managing security settings” on page 29.

Locating and organizing devices within the system

Searching for devices within the system

A *bookmark* is a saved search. When you run a bookmarked search, the devices that match the search criteria appear in the Search Results area. Use default bookmarks to search for devices based on the device life cycle state. You can also create custom bookmarks using customized search criteria.

The default bookmarks cannot be edited or deleted. To search for devices using default bookmarks, from the Bookmarks and Searches menu, select one of the following:

- **Managed Printers**—Active devices in the system. Devices that appear when selecting this bookmark can be in any of the following states:
  - Managed (Normal)
  - Managed (Changed)
  - Managed (Missing)
  - Managed (Found)
- **Managed (Normal) Printers**—Active devices in the system whose properties have remained the same since the last audit.
- **Managed (Changed) Printers**—Active devices in the system whose properties have changed since the last audit.
- **Managed (Missing) Printers**—Devices that the system was unable to communicate with.
- **Managed (Found) Printers**—Devices that are reported as missing from previous search queries, but have now been found.
- **New Printers**—Devices that are in **New** state.
- **Unmanaged Printers**—Devices that have been marked for exclusion from activities performed in the system.
- **Retired Printers**—Devices that are no longer active in the system.
- **All Printers**—All devices in the system.

Note: To refine the results of your bookmarked search, from the Results Summary section, select a criterion.

To create a bookmark for your refined search, click  .

Using custom bookmarks

1. From the Bookmarks and Searches section, click **Manage bookmarks**.
2. Click ✚ or  to add or edit a custom bookmark.
3. Type a unique name for the bookmark, and then modify the search criteria settings.
   - To add a search criterion, click ✚.
   - To group search criteria together, click [+], and then click ✚ to add individual criteria.

   Note: If you group the search criteria, then the system counts them as one criterion.

4 Specify the parameter, operation, and value for your search criterion.

Note: For more information, see “Understanding search criteria settings” on page 21.

5 Click **Save** to save the bookmark, or **Save And Run** to save the bookmark and begin the search.

Using advanced search

You can use Advanced Search to perform complex searches based on one or multiple parameters.

1 From the Bookmarks and Searches section, click **Advanced Search**.

2 Modify the search criteria settings.

- To add a search criterion, click ✚.
- To group search criteria together, click [+], and then click ✚ to add individual criteria.

Note: If you group the search criteria, then the system counts them as one criterion.

3 Specify the parameter, operation, and value for your search criterion.

Note: For more information, see “Understanding search criteria settings” on page 21.

4 Click **OK** to begin the search.

The located devices appear in the Search Results area.

Understanding search criteria settings

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

Use	To
Asset Tag	Specify the asset tag assigned to the device.
Color Capability	Specify whether the device can print in color.
Communications	Specify the device security or authentication state.
Conformance	Specify the device conformance state.
Contact Location	Specify the device location.
Contact Name	Specify the device contact name.
Copy Capability	Specify whether the device supports copying files.
Disk Encryption	Specify whether the device supports disk encryption.
Disk Wiping	Specify whether the device supports disk wiping.
Duplex Capability	Specify whether the device supports two-sided printing.
eSF Application(Name)	Specify the name of the eSF application installed in the device.
eSF Application(State)	Specify the status of the eSF application installed in the device.
eSF Application(Version)	Specify the version of the eSF application installed in the device.
ESF Capability	Specify whether the device supports managing eSF applications.
Event Name	Specify the event name assigned to the device.
Firmware Version	Specify the device firmware version.

Use	To
Firmware:AIO	Specify the AIO value of the device firmware.
Firmware:Base	Specify the base version of the device firmware.
Firmware:Engine	Specify the engine value of the device firmware.
Firmware:Fax	Specify the fax value of the device firmware
Firmware:Font	Specify the font value of the device firmware.
Firmware:Kernel	Specify the kernel value of the device firmware.
Firmware:Loader	Specify the loader value of the device firmware.
Firmware:Network	Specify the network value of the device firmware.
Firmware:Network Driver	Specify the network driver value of the device firmware.
Firmware:Panel	Specify the panel version of the device firmware.
Firmware:Scanner	Specify the scanner version of the device firmware.
Hostname	Specify the device host name.
IP Address	Specify the device 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.*.*`**, and **`123.*.*.*`**.
Keyword	Specify the assigned keywords, if any.
Lifetime Page Count	Specify the lifetime page count value of the device.
MAC Address	Specify the device MAC address.
Maintenance Counter	Specify the value of the device maintenance counter.
Manufacturer	Specify the device manufacturer name.
Marking Technology	Specify the marking technology that the device supports.
MFP Capability	Specify whether the device is a multifunction product (MFP).
Model	Specify the device model name.
Printer Status	Specify the device status. For example, **`Ready`**, **`Paper Jam`**, **`Tray 1 Missing`**.
Profile Capability	Specify whether the device supports profiles.
Receive Fax Capability	Specify whether the device supports receiving fax.
Scan to E-mail Capability	Specify whether the device supports Scan to E-mail.
Scan to Fax Capability	Specify whether the device supports Scan to Fax.
Scan to Network Capability	Specify whether the device supports Scan to Network.
Serial Number	Specify the device serial number.
State	Specify the current device state in the database.
Supply Status	Specify the device supplies status.
System Name	Specify the device system name.

Use the following operators when searching for devices:

- **Contains**—A parameter contains a specified value.
- **Does not contain**—A parameter does not contain a specified value.
- **Does not equal**—A parameter is not equivalent to a specified value.
- **Ends with**—A parameter ends with a specified value.
- **Equals**—A parameter is equivalent to a specified value.
- **Starts with**—A parameter begins with a specified value.

Using categories and keywords

Keywords let you assign custom tags to devices, providing additional flexibility in locating and organizing devices in the system. Group keywords into categories, and then assign multiple keywords from multiple categories to a device.

Before you can create a keyword, first create a category to which the keyword belongs.

For example, you can create a category called **`Location`**, and then create keywords within that category. Examples of keywords within the Location category might be **`Building 1`**, **`Building 2`**, or something more specific for your business needs.

After creating the categories and keywords, you can then assign the keywords to multiple devices. You can search for devices based on keywords assigned to them, and then bookmark the results of your search for future use.

Adding, editing, or deleting categories

1. If necessary, from the Assets tab, click **Keywords** to show the Keywords section.
2. From the Category pane, click ✚ to add, ✎ to edit, or — to delete a category.

   Note: Deleting a category also deletes its keywords and removes them from the devices to which the keywords are assigned.
3. Follow the instructions on the computer screen.

Adding, editing, or deleting keywords

1. If necessary, from the Assets tab, click **Keywords** to show the Keywords section.
2. From the Keywords pane, do one of the following:
   - To add a keyword:
     a. From the Category pane, select a category where the keyword belongs.
     b. From the Keyword pane, click ✚.
     c. Type the name of the new keyword, and then press **Enter**.
   - To edit a keyword:
     a. Select an existing keyword, and then click ✎.
     b. Edit the name, and then press **Enter**.

- To delete a keyword:
  a Select an existing keyword, and then click —.
  b Click **Yes**.

Note: Deleting a keyword removes it from the devices to which it is assigned.

Assigning keywords to a device

1 If necessary, from the Assets tab, click **Keywords** to show the Keywords section, and then select a keyword.

Note: To select multiple keywords, use **Shift** + **click** or **Ctrl** + **click**.

2 Select the check box beside the IP address of the device where you want the keyword assigned.

Note: You can select multiple or all devices.

3 Click .

4 From the Task Information area, verify that the task is complete.

5 To verify if the keyword is successfully assigned to the device, see the device properties by selecting the IP address of the device.

From the Identification Property section, the new value of the keyword for the device appears.

Removing an assigned keyword from a device

1 From the Assets tab, select the check box beside the IP address of the device from which you want to remove a keyword.

2 If necessary, click **Keywords** to show the Keywords section.

3 Select a keyword, and then click .

4 Select the keyword you want to remove, and then click **OK**.

Note: To select multiple keywords, use **Shift** + **click** or **Ctrl** + **click**.

5 From the Task Information area, verify that the task is complete.

6 To verify if the keyword is successfully removed from the device, do this:
  a Select the IP address of the device.
  b From the Identification Property section, make sure the keyword no longer appears.

Managing configurations

A *configuration* is a collection of settings that can be assigned to a device or a group of devices of the same model. You can perform a conformance check to make sure that a device or a group of devices is compliant with a configuration. If the device does not conform with the configuration, then you can enforce the configuration on the device or group of devices.

Creating a configuration

Note: You can manage security settings only when creating a configuration from a selected device. For more information, see “Creating a configuration from a device” on page 25.

1. From the Configurations tab, click **Configurations** > ➕, and then assign a unique name for the configuration.
2. Select a device, and then click **OK**.
3. From the Device Settings tab, select a configuration type, and then do either of the following:
   - Select one or more settings, and then specify the values.
   - To apply variable settings, do the following:
     a. From the Variable Setting Data File menu, select a file. If necessary, click **Import**, and then browse to the CSV file.

        Note: Changing the file may affect the device settings that are using variables.

     b. Select a setting, and then type the variable in the setting field.
        For example, type **`${Contact_Name}`** in the **Contact Name** field, where **`${Contact_Name}`** is the variable that represents the **`Contact_Name`** token defined in the CSV file. When the configuration is enforced, the variable is replaced with its corresponding value.

        Note: Tokens are case sensitive. For more information, see “Understanding variable settings” on page 26.
4. From the Firmware tab, select a transfer method, and then select a firmware file.

   To import a firmware file, see “Importing files to the library” on page 26.

   Note: If you select HTTPS and your printer only supports HTTP, then the application uses HTTP.
5. From the Solutions tab, select one or more solutions to deploy. For more information, see “Preparing solutions for enforcement” on page 29.
6. Click **Save**.

Creating a configuration from a device

Note: When you create a standalone configuration, you cannot modify its security settings. Creating a configuration from a selected device lets you modify the security settings. For more information, see “Managing security settings” on page 29.

1. From the Configurations tab, select a device.
2. Click **Configurations** >  , and then assign a unique name for the configuration.
3. Click **OK**.

Notes:

- Before enforcing the cloned configuration to other devices, make sure that the host name setting is disabled. You can use variable settings to assign a unique host name to a device. For more information, see “Understanding variable settings” on page 26.
- Configurations that appear in red text and begin with an exclamation point contain one or more invalid settings, and cannot be enforced on a device.

Assigning a configuration

1. From the Configurations tab, click **Configurations**, and then select a configuration.
2. Select one or more devices.
3. Click  .

Editing a configuration

1. From the Configurations tab, click **Configurations**.
2. Select a configuration, and then click  .
3. If necessary, rename the configuration, and then modify the settings.
4. Apply the changes.

Note: Configurations that appear in red text and begin with an exclamation point contain one or more invalid settings, and cannot be enforced on a device.

Importing files to the library

1. From the Configurations tab, click **Library**.
2. Import the file.

   Notes:

   - When importing firmware, use only .fls files.
   - Some solutions require a license. Click **Properties** to view the licenses included in the solutions package.

Understanding variable settings

You can use variable settings in running conformance check or enforcing a configuration to a device. When creating or editing a configuration, you can select a CSV file to be associated with the configuration.

Each row in the CSV file contains a set of tokens that are used as an identifier or a value for the configuration settings.

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, the first column is a “special device identifier” token denoting which device identifier is being used. It should be one of the following and unique in each row:

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

Each subsequent column in the header row is a “replacement” token that is user-defined. This token is replaced with the values in the subsequent rows when the configuration is enforced. Make sure that the tokens do not contain any spaces.

To obtain the correct CSV format, export a CSV file from MVE using Data Export.

1. From the Header area, click  .
2. From the Include Printers menu, select a device group.
3. Create or edit a Data Export template.
4. From the Possible Fields section, in the Identification menu, select a device identifier (such as IP Address).
5. Add the selected device identifier to the Exported Fields section.
6. Click **Generate File** > **Finalize Export**.
7. Save the file, and then open it using a text editor.

   Note: To make sure that the device identifier from the exported file is in the correct CSV format, remove spaces and use capital letters. For example, if the exported data contains **`IP Address`**, then change it to **`IP_ADDRESS`**.
8. Add the variable settings, and then save the file.

You can import the CSV file containing variable settings when creating or editing a configuration. For more information, see “Creating a configuration” on page 25 or “Editing a configuration” on page 26.

Understanding secured devices

There may be various configurations for a secured device. However, MVE only supports devices that are either fully unrestricted or fully restricted.

		Fully unrestricted	Fully restricted
Device settings	Remote Management permission or Remote Management Function Access Control (RM FAC) **Note:** For a list of devices that support security settings, see the *Release Notes*.	No authentication or no security	An authentication method is configured to restrict public access to the Remote Management and Security Menu permissions, or a security template is assigned to RM FAC.
	Significant ports	The following ports are open: • UDP 161 (SNMP) • UDP 9300/9301/9302 (NPAP)	The UDP 161 (SNMP) port is open.
	Security-related ports	The following ports are open: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)	The following ports are open: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)
MVE settings	Discovery profile	The **Include secured printers in the discovery** option is cleared.	The **Include secured printers in the discovery** option is selected.
	Are secure channels used for communication between MVE and the network devices?	No **Note:** In some printer models, secure channels are used even on fully unrestricted devices.	Yes
	How do I determine the security configuration of the devices in my network?	In the main data grid in MVE, an *open* padlock icon appears beside the IP address of a fully unrestricted device.	In the main data grid in MVE, a *closed* padlock icon appears beside the IP address of a fully restricted device. **Note:** If MVE cannot identify the communication credentials of the device, then the closed padlock icon has a red slash through it. To remove the red slash, set the correct communication credentials for the security settings in the configuration before enforcing it to the restricted device.
	How do I search for devices that have this type of configuration?	1 From the “Bookmarks and Advanced Search” area, select **All Printers**. 2 From the Search Results Summary area, scroll down to the Communications category, and then select **Unsecured**.	1 From the “Bookmarks and Advanced Search” area, select **All Printers**. 2 From the Search Results Summary area, scroll down to the Communications category, and then select **Secured**.

Managing security settings

Managing device settings

Note: Before you begin, make sure that the device security settings are configured to let MVE manage the device securely.

1. Obtain the printer IP address. Do either of the following:
   - Locate the IP address on the top or upper-left corner of the printer home screen.
   - View the IP address in the Network Overview section or TCP/IP section of the Network/Ports menu.
2. Open a Web browser, and then type the printer IP address.
3. Depending on your printer model, do either of the following:
   - Click **Settings** > **Security** > **Login Methods**.

     From the Public section, click **Manage Permissions**, and then clear Remote Management and Security Menu. Depending on the authentication method used, navigate to the Remote Management and Security Menu permissions, and then allow secure access to them.
   - Click **Settings** > **Security** > **Security Setup** > **Access Controls**, and then assign a security template to RM FAC.
4. Click **Save** or **Submit**.

Note: For more information on managing permissions or function access controls, see the *Embedded Web Server—Security Administrator's Guide* for your printer.

Managing MVE settings

Notes:

- Make sure that "Include secured devices in the discovery" is enabled when you discover the device. For more information, see "Adding or editing a discovery profile" on page 14.
- Make sure that you have created a configuration from a device. For more information, see "Creating a configuration from a device" on page 25.

1. From the Configurations tab, edit a configuration.
2. From the Security tab, manage the security settings available for your device.

   Note: Some security settings may not be available, depending on your printer model.
3. Click **Save**.

Preparing solutions for enforcement

Creating a solutions package

1. Export the device list from MVE using Data Export.
   a. From the Header area, click  .
   b. From the Include Printers menu, select a device group.

c Select the **Device List** template, and then run Data Export.

Note: When creating a custom template, add only Model and Serial Number to the Exported Fields section.

d Click **Finalize Export**.

2 Access Package Builder.

Note: If you need access to Package Builder, contact your administrator.

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

b Import the device list.

c Type the package description, and then if necessary, type your e-mail address.

d From the Product menu, select a solution or solutions, and then if necessary, add licenses.

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

3 Download the package.

Adding solutions to a configuration

Note: Solutions that are not compatible with a device assigned to a configuration do not appear in the Configurations view.

1 Import the solutions package downloaded from Package Builder. For more information, see "Importing files to the library" on page 26.

2 From the Configurations tab, add or edit a configuration.

3 From the Solutions tab, select one or more solutions to deploy.

Notes:

- For a Solutions bundle, select the components that you want to include.
- Licenses are automatically retrieved from the imported solutions package.
- For new configurations, MVE checks for licenses as you assign the configuration to devices. For configurations that are already assigned to devices, MVE checks for licenses as you select the solutions.

4 From the General Settings section, set the license type and transfer method.

5 Apply the changes.

Checking conformance with a configuration

1 From the Configurations tab, select one or more devices.

2 Assign a configuration, and then click **Conformance**.

3 If a question mark or **x** appears, then click  to view specific details.

Note: A configuration conformance check can be scheduled to occur regularly or at a predetermined time. For more information, see "Scheduling tasks" on page 44.

Enforcing a configuration

1 From the Configurations tab, select one or more devices.

2 Assign a configuration, and then click **Enforce**.

3 Click  to check that the configuration enforcement is complete.

Note: A configuration enforcement task can be scheduled to occur regularly or at a predetermined time. For more information, see “Scheduling tasks” on page 44.

Removing a configuration

1 From the Configurations tab, select one or more devices.

2 Click **Configurations** >  .

Managing the service desk

Working with configuration

Before attempting to resolve a problem on a device, make sure that the device conforms with its assigned configurations.

Checking device conformance with a configuration

1 From the Service Desk tab, select one or more devices.

2 Click **Conformance**.

3 When the task is completed, click  to view the results of the conformance check.

Enforcing configurations

1 From the Service Desk tab, select one or more devices.

2 Click **Enforce**.

3 When the task is completed, click  to make sure that the configuration enforcement is complete.

Working with a device

Checking the status of a device

1 Locate a device using Bookmarks or Advanced Search.

Note: You can use the categories in the Search Results Summary area to narrow down the list of devices found.

2 Select the check box beside the IP address of the device, and then click **Collect current status**.

3 From the Printer Status and Supply Status columns, take note of the icon beside the device.

Icon	Status
	**OK**—The device is ready and supplies are sufficient.
	**Warning**—The device is working, but supplies may be low or may require attention at a later time.
	**Error**—The device or supplies need immediate attention.

4 Click **Work with Device** to view details on the status of the device.

Viewing a device remotely

Note: This feature is available only in devices that support remote viewing.

1. From the Service Desk tab, select the check box beside the IP address of the device.
2. Click **Work with Device**.

   Note: The picture of the device is available only in some printer models.
3. Click **Remote Operator Panel** > **Click here to continue**.
4. From the lower left side, see the keyboard key equivalent for each of the device button commands.

   Note: The location of the keyboard key equivalent may differ depending on the device model.

Viewing the embedded Web page

Note: This feature is available only in devices that support remote viewing of its embedded Web page.

1. From the Service Desk tab, select the check box beside the IP address of the device.
2. Click **Work with Device**.

   Note: The picture of the device is available only in some printer models.
3. Click **Embedded Web Page**.

   Note: From the bottom part of the page, you can also select the language that you want to use.

Managing device events

You can monitor and manage events or alerts in your printer fleet. Set a destination to notify yourself or other specified users when a particular incident occurs. Create an automated event when a device sends an alert to the network.

Note: Events or alerts do not apply to secured devices.

Creating a destination

A destination is a predefined action that executes a set command whenever a specified event occurs across a group of devices. A destination can either be an e-mail notification or a command line prompt for when a custom action is required.

1. If necessary, from the Event Manager tab, click **Destinations** to show the Destinations section.
2. Click ✚, and then type a unique name for the destination.
3. Do one of the following:
   - Select **Command**, and then click **Next**.
     a. Type the name of an executable command into the Command Path box.
     b. Add keyword(s) to the Command Parameters by selecting a keyword from the Place Holders list, and then click ▶.
   - Select **E-mail**, and then click **Next**.
     a. Make sure you have properly configured the e-mail settings in the System Configuration dialog. For more information, see "Configuring e-mail settings" on page 37.
     b. Enter values in the appropriate fields:
        - **From**—Type the e-mail address of the sender.
        - **To**—Type the e-mail address of the recipient.
        - **CC**—Type the e-mail addresses of other recipients who will receive a carbon copy of the e-mail.
        - **Subject**—Type a subject title if you want the e-mail to contain a subject title.
        - **Body**—Type the default e-mail message.

Note: From the Place Holders column, you can use the available *placeholders* as the part of or as the entire subject title. You can also use placeholders as part of an e-mail message. Placeholders represent the variable elements that, when used, will be replaced by the actual value.

4. Click **Finish**.

Editing or deleting a destination

1. If necessary, from the Event Manager tab, click **Destinations** to show the active destinations.
2. Select a destination, and then do one of the following:
   - To edit the destination, click  .
     a. If necessary, edit the destination name, and then click **Next**.
     b. If necessary, edit the name of the executable command in the Command Path box.

c To delete a keyword from the Command Parameters box, double-click the keyword, and then press **Delete**.

d To add more keyword(s) to the Command Parameters box, select a keyword from the Place Holders list, and then click ▶.

- To delete the destination, click —, and then click **Yes**.

  Warning—Potential Damage: When you delete a destination, the events associated with it are also deleted.

3 Click **Finish**.

Creating an event

1 From the Event Manager tab, click **Events**.

2 Click ✚, and then type a unique name for the event and its description.

3 From the Alerts section, select an alert, and then click **Next**.

Note: You can select multiple or all alerts.

4 Select a destination, and then do either of the following:

- To trigger the event when the alert becomes active, select **On Active Only**.
- To trigger the event when the alert becomes active and cleared, select **On Active and Clear**.

5 If you want to allow a delay between the arrival of the first active alert in MVE and the triggering of the device, then select **Enable Grace Period**, and then enter the time in hours and minutes.

Note: The delay applies only to active alerts and is activated when the first alert is received. The delay will not be reset or extended for duplicate alerts.

6 Click **Finish**.

Editing or deleting an event

1 If necessary, from the Event Manager tab, click **Events** to show the active events.

2 Select an event, and then do one of the following:

- To edit the event, click  .
  a If necessary, edit the event name and description.
  b From the Alerts section, add more alerts by selecting them, or remove an alert by clearing the check box beside it.
  c Click **Next**.
  d From the Destinations section, add more destinations by selecting them, or remove a destination by clearing the check box beside it.
  e Select a trigger destination, and then click **Finish**.
- To delete the event, click —, and then click **Yes**.

Assigning an event to a device

1. From the Event Manager tab, select the check box beside the IP address of the device.
2. If necessary, click **Events** to show the active events.
3. Select an event, and then click .

Removing an event from a device

1. From the Event Manager tab, select the check box beside the IP address of the device.
2. If necessary, click **Events** to show the active events.
3. Select an event, and then click .

Displaying event details

1. From the Event Manager tab, locate a device using Bookmarks or Advanced search.

   Note: You can use the categories in the Search Results Summary area to narrow down the list of devices found.
2. From the Search Results area, select the check box beside the IP address of a device.

   Note: If you do not know the IP address of the device, then locate the device under the System Name column.
3. Click **Properties**.

   A dialog appears, showing the current active conditions and event details assigned to the device.

Performing other administrative tasks

Downloading generic files

You can download miscellaneous files from the Markvision Server to one or more devices on a network. This feature allows instant distribution of various file types, including *universal configuration files* (UCF) to any devices that the application manages.

1. From the Header area, click  .
2. From the Include Printers menu, select a device group or an available bookmark.
3. From the Destination menu, select one of the following:
   - **Configuration File (HTTPS)**—Download a configuration file to the printer.
   - **Firmware Update**—Download a firmware update for the devices.
   - **Print (FTP)**—Download a printable file over an FTP network.
   - **Print (raw socket)**—Download a printable file from the computer.
   - **UCF Configuration (HTTP)**—Download a printer UCF.
   - **UCF Configuration (FTP)**—Download a network UCF.

   Note: If you select HTTPS and your printer only supports HTTP, then the application uses HTTP.
4. From the Select the file section, browse to the file that you want to download to the devices.
5. Click **Download**.

Notes:

- The Generic File Download task is not available when the Printer Lockdown option is enabled.
- You can schedule a Generic File Download task to occur regularly or at a predetermined time. For more information, see "Scheduling tasks" on page 44.

Configuring e-mail settings

Notes:

- You need to configure the Simple Mail Transfer Protocol (SMTP) settings so Markvision can send e-mail notifications for alerts and error messages.
- If you enable the SMTP configuration now, and then disable it later, then Markvision will no longer be able to send e-mail notifications for alerts and error messages.

1. From the Header area, click  > **E-mail** tab.
2. Select the **Enable SMTP Configuration** check box, and then enter values in the appropriate fields:
   - **SMTP Mail Server**—Type the mail server information.
   - **Port**—Type the port number of the SMTP mail server.
   - **From**—Type the e-mail address of the sender.

3 If a user needs to log in before sending the e-mail, then select the **Login Required** check box.
   a Type the login information and password.
   b Confirm the password by typing it again.
4 Click **Apply** > **Close**.

Configuring system settings

1 From the Header area, click  > **General** tab.
2 From the Hostname Source section, select the source for the system where you want to acquire the host name for a device, and then click **Apply**.
3 From the Event Manager section, set the interval the system should wait before reregistering with devices for alerts, and then click **Apply**.
4 From the Results Summary section, set the number of results to show, and then click **Apply**.

Adding, editing, or deleting a user in the system

1 From the Header area, click  > **User**.
2 Do one of the following:
   • Click ✚ to add a user.
      a Enter the details.
      b From the Roles section, assign the user to one or more roles, and then click **OK**.
         – **Admin**—The user can access and perform tasks in all tabs. Only users assigned to this role have administrative privileges, such as adding more users to the system or configuring system settings.
         – **Assets**—The user can only access and perform tasks in the Assets tab.
         – **Event Manager**—The user can only access and perform tasks in the Event Manager tab.
         – **Configurations**—The user can only access and perform tasks in the Configurations tab.
         – **Service Desk**—The user can only access and perform tasks in the Service Desk tab.
   • Click  to edit, or — to delete a selected user.
3 Follow the instructions on the computer screen.

Note: Three consecutive failed login attempts disable a user account. Only an administrator can reenable the user account. If the user is the only user in the system with an Admin role, then the account is suspended only temporarily for about 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.

MVE administrators can use the company LDAP server to authenticate user IDs and passwords to avoid maintaining multiple user credentials.

MVE tries to authenticate against the valid user credentials present in the system. If MVE is unable to authenticate the user, then it tries to authenticate against users registered in the LDAP server. If the same user names exist in both the MVE and the LDAP servers, then the MVE password is used.

As a prerequisite, the LDAP server must contain user groups that correspond to the required user roles. For more information, see “Adding, editing, or deleting a user in the system” on page 38.

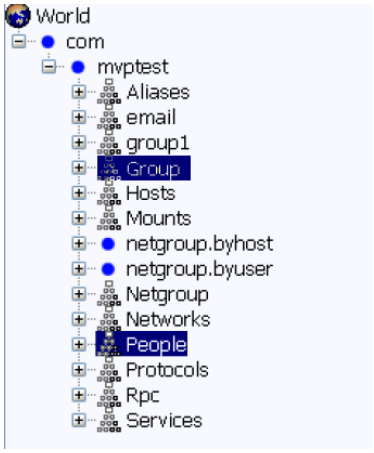
1 From the Header area, click > **LDAP** > **Enable LDAP for Authentication**.

2 From the Connection section, configure the following:

- **Server**—Type 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 do the following:
  a Use the fully qualified domain name (FQDN) of the server host.
  b Access the network host file, and then create an entry to map the server host name to its IP address.

  Notes:

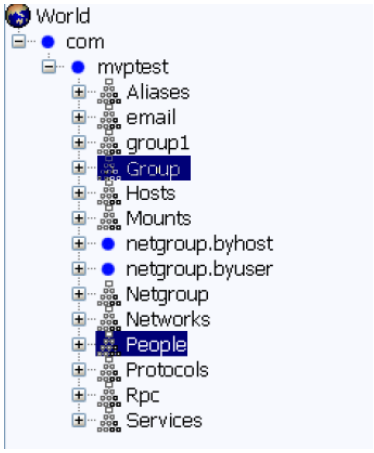
  - In a UNIX or Linux operating system, the network host file is typically found at **`/etc/hosts`**.
  - In a Windows operating system, the network host file is typically found at **`%SystemRoot%\system32\drivers\etc`**.
  - The TLS protocol requires the server host name to match the name of the “Issued To” host specified in the TLS certificate.
- **Port**—Enter the port number that the local computer uses to communicate with the LDAP community server. The default port number is 389.
- **Root DN**—Type the base distinguished name (DN) of the root node. In the LDAP community server hierarchy, this node should be the direct 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 User Search Base and Group Search Base.

3 Configure the search settings.

- **User Search Base**—Type 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**



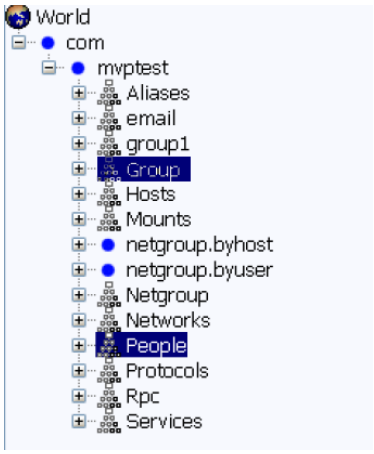
If the users are at multiple-directory hierarchical levels in the LDAP community server, then do the following:

a Calculate any common upstream hierarchy of all the possible locations in the user node.

b Include the configuration in the User Search Base field.

Note: To let MVE search for users starting at the Base or Root DN, select **Enable Nested User Search** and clear the User Search Base field.

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



The User Search Filter function can accommodate multiple conditions and complex expressions.

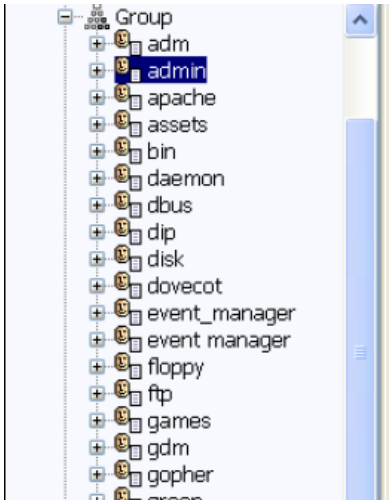
Log in using	In the User Search Filter field, type
Common name	**(CN={0})**
Login name	**(sAMAccountName={0})**
User principal name	**(userPrincipalName={0})**

Log in using	In the User Search Filter field, type
Telephone number	`(telephoneNumber={0})`
Login name or common name	`(|(sAMAccountName={0})(CN={0}))`

Notes:

- These expressions apply only to the Windows Active Directory® LDAP server.
- For User Search Filter, the only valid pattern is **`{0}`**, which means that MVE searches for the MVE user login name.

- **Group Search Base**—Type the node in the LDAP community server where the user groups corresponding to the MVE roles exist. This node is also under the Root DN where all the group nodes are listed. For example, **`ou=group`**



Note: A search base consists of multiple attributes separated by commas, such as cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain).

- **Group Search Filter**—Type the parameter for locating a user within a group that corresponds to a role in MVE.

  Note: You may use the patterns **`{0}`** and **`{1}`**, depending on the configuration of your back-end LDAP community server. If you use **`{0}`**, then MVE searches for the LDAP user DN. The user DN is retrieved internally during the user authentication process. If you use **`{1}`**, then MVE searches for the MVE user login name.

- **Group Role Attribute**—Type the attribute that contains the full name of the group. For example, **`cn`**.

- **Enable Nested Group Search**—Search for nested groups within the LDAP community server.

4 Click **Binding Information**, and then configure the settings.

- **Anonymous Bind**—If there is no LDAP configuration stored in MVE, then 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 Bind**—Uses unencrypted communication between the MVE server and the LDAP server. If you want the MVE server to use the LDAP server lookup facility, then do the following:
  a In the Bind DN field, type the bind DN.
  b Type the Bind Password, and then confirm the password.

  Note: The Bind Password depends on the Bind User settings in the LDAP server. If the Bind User is set as **`Non-Empty`**, then a Bind Password is required. If the Bind User is set as **`Empty`**, then a Bind Password is not required. For more information, contact your LDAP administrator.
- **TLS**—Uses 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). To configure the settings, do the following:

  For self-signed certificates, the TLS fingerprint must be made available to the system-wide Java Virtual Machine (JVM) keystore named **`cacerts`**. This keystore exists in the ***`[mve.home]`*`/jre/lib/security`** folder, where ***`[mve.home]`*** is the installation folder of MVE.
  a In the Bind DN field, type the bind DN.
  b Type the Bind Password, and then confirm the password.

  Note: The Bind Password is required.
- **Kerberos**—Uses encrypted communication between the MVE server and the LDAP server. The Kerberos security protocol is supported only in a Windows Active Directory® that has Generic Security Service Application Program Interface (GSSAPI) implementation. For more information, see the documentation for Kerberos. To configure the settings, do the following:
  a In the Kerberos Config File field, browse to the krb5.conf file.
  Sample configuration:

```
[libdefaults]
    default_realm=ABC.COM

[realms]
    ABC.COM = {
      kdc = abc1.abc.com
    }

[domain_realm]
    .abc.com=ABC.COM
```

  b In the Encryption Method menu, select whether to use SSL encryption.
  c In the KDC Username field, type the Key Distribution Center (KDC) name.
  d Type the KDC password, and then confirm the password.

  Note: If you want to enable Kerberos Authentication, then see "Enabling Kerberos authentication" on page 43.

5 Click **Role Mapping**, and then configure the following:

- **Admin**—Type the existing role in LDAP that has administrative rights in MVE.
- **Assets**—Type the existing role in LDAP that manages the Assets module in MVE.
- **Configurations**—Type the existing role in LDAP that manages the Configurations module in MVE.

- **Service Desk**—Type the existing role in LDAP that manages the Service Desk module in MVE.
- **Event Manager**—Type the existing role in LDAP that manages the Event Manager module in MVE.

Notes:

- MVE automatically maps the specified LDAP group to its corresponding MVE role.
- You can assign one LDAP group to multiple MVE roles, and you may 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 **assets** groups for the Admin role, then type **admin|assets** in the Admin field.
- If you want to use only the Admin role and not the other MVE roles, then leave the fields blank.

6 Click **Apply** > **Close**.

Enabling Kerberos authentication

Before you begin, make sure that:

- Groups and users for MVE are set up in the Active Directory server. For more information, contact your system administrator.
- You have a keytab file that contains the MVE user credentials and an encrypted key. You can use the Ktpass tool to generate a keytab file. For more information, see the online references for Microsoft.

1 From the Header area, click  > **LDAP** > **Enable LDAP for Authentication**.

2 From the Binding Information section, select **Kerberos** > **Enable Kerberos Authentication**.

3 Configure the following:

- **Service Principal Name**—Type the service principal name for the MVE server.
- **Keytab**—Browse to the keytab file.

4 Configure the Role Mapping settings. For more information, see step 5.

Note: Make sure that the specified MVE roles match the existing groups set up in the Active Directory server.

5 Click **Apply** > **Close**.

Adding a login disclaimer

1 From the Header area, click  > **Disclaimer** > **Enable disclaimer prior to login**.

2 In the Disclaimer Text field, type the message that you want to appear before logging in to MVE.

Note: You can type up to 4000 characters.

3 Click **Apply** > **Close**.

Generating reports

1 From the Header area, click  .

2 From the Include Printers menu, select a device group based on your previously bookmarked searches.

3 From the Report Type menu, select the type of data you want to view.

Select	To view
Lifecycle State - Summary	A summarized report of the life cycle states of the devices.
Printer Manufacturer - Summary	A summarized report of device manufacturers.
Printer Model - Summary	A summarized report of device model names and numbers.
Printer Capabilities - Summary	A summarized report of device capabilities.
Printer Capabilities	A spreadsheet listing device capabilities.
Lifecycle State	A spreadsheet listing the life cycle states of devices.
Lifetime Page Count	A spreadsheet listing the lifetime page count of devices.
Maintenance Count	A spreadsheet listing the maintenance count of devices.
Firmware Versions	A spreadsheet listing the firmware versions of devices.
eSF Solutions	A spreadsheet listing the different Embedded Server Framework (eSF) solutions installed on the devices.
Disk Security	A spreadsheet listing the hard disk enabled devices and the state of the disk security.
Statistics:Jobs by Printed Sheets	A spreadsheet listing the number of print jobs performed by the devices.
Statistics:Jobs by Media Sides Count	A spreadsheet listing the number of pick counts for print, fax, and copy jobs performed by the devices.
Statistics:Jobs by Scan Usage	A spreadsheet listing the number of scan jobs performed by the devices.
Statistics:Jobs by Fax Usage	A spreadsheet listing the number of fax jobs performed by the devices.
Statistics:Jobs by Supply Information	A spreadsheet listing important details for each of the supply items in the devices.

4 From the Report Format menu, select **PDF** or **CSV**.

5 If you select PDF, then in the Title field, you can choose to customize the title of the report.

6 If applicable, from the Group menu, select a group.

7 Click **Generate**.

Scheduling tasks

1 From the Header area, click  .

2 From the Add menu, do one of the following:

- Select **Audit**, and then select a device group.
- Select **Discover**, and then select a discovery profile.

- Select **Conformance**, and then select a device group and configuration.
- Select **Enforcement**, and then select a device group and configuration.
- Select **Generic File Download**, and then select a device group, file, and destination. Only users with administrative privileges can use this option.

3 Click **Next**.

4 In the Name field, type the name of the new scheduled event.

5 Adjust the settings.

6 Apply the changes.

Viewing the system log

1 From the Header area, click  .

By default, the last activity in the database is listed first.

2 If you want to view the activities by category, then do the following:

a Click **Filter**.

b From the Time Period section, select the start and end dates.

c In the ID(s) field, type the task ID numbers.

Note: This is an optional field.

d From the Task Name section, clear the check box beside the task that you do not want to include in the log file.

e From the Categories section, clear the check box beside the category that you do not want to include in the log file.

f Click **OK**.

3 Click **Prepare to Export** > **Finalize Export**.

4 From the “Save in” drop-down menu, navigate to the folder where you want to save the log file.

5 In the “File name” field, type the name of the file, and then click **Save**.

6 Navigate to the folder where the log file is saved, and then open the file to view the system log.

Exporting audit data of the device

1 From the Header area, click  .

2 From the Include Printers menu, select a device group.

3 From the Possible Fields section, select the columns you want for your exported file.

4 Select **Add** to move the selected columns into the Export Fields section.

5 Select **Add first row header** to include a header in your CSV file.

6 Click **Generate File** > **Finalize Export**.

7 Select the location and file name on the client system, and then click **Save**.

Notes:

- Only users with administrative privileges and asset roles can use this feature.
- The exported data is generated from the last successful audit of the device.
- You can also create a CSV file for selected printers by selecting them prior to exporting a generic file.

Frequently asked questions

What devices are supported by the application?

For a complete list of supported devices, see the Release Notes.

How do I change my password?

From the Header area, click **Change Password**, and then follow the instructions on the computer screen.

Why can I not choose multiple devices in the Supported Models list when creating a configuration?

Configuration settings and commands differ between printer models. For the configuration to work properly, create the configuration first, and then assign it to multiple devices.

Can other users access my bookmarks?

Yes. Bookmarks can be accessed by any user.

Where can I find the log files?

Navigate to this directory to locate the following installer log files: **%TEMP%**

- *mve-*.log*
- **.isf*

Navigate to this directory to locate the application log files:

<INSTALL_DIR>*\tomcat\logs**, where ***<INSTALL_DIR> is the installation folder of Markvision.

Files in this directory that have the **.log* format are the application log files.

What is the difference between host name and reverse DNS lookup?

A host name is a unique name assigned to a device on a network. Each host name corresponds to an IP address. Reverse DNS lookup is used to determine the designated host name or domain name of a given IP address.

Where can I find reverse DNS lookup in MVE?

From the Header area, click  > **General**.

If you select **Reverse DNS Lookup** in the Hostname Source section, then make sure that the printer IP address is registered in the DNS server. This lets MVE pick up the printer host name from the DNS table by its IP address.

Troubleshooting

User has forgotten the password

To reset the user password, you need to have administrator privileges.

1. From the Header area, click  .
2. From the User tab, select a user, and then click  .
3. Change the password.
4. Click **OK**, and then click **Close**.
5. Ask the user to log in again.

The application is unable to discover a network device

Check the printer connections

- Make sure the power cord is securely plugged into the printer and into a properly grounded electrical outlet.
- Make sure the printer is turned on.
- Make sure other electrical equipment plugged into the outlet are working.
- Make sure the LAN cable is plugged into both the print server and into the LAN.
- Make sure the LAN cable is working properly.
- Restart the printer and the print server.

Make sure the internal print server is properly installed and enabled

- Print a setup page for the printer. The print server should appear in the list of attachments on the setup page.
- Make sure the TCP/IP on the print server is activated. The protocol must be active for the print server and the application to work. From the printer control panel, make sure the protocol is active.
- See your print server documentation.

Make sure the device name in the application is the same as the one set in the print server

1. Check the device name set in the application.

   From the Search Results area, locate the IP address of the printer.

   The name of the device appears beside its IP address. This is the application device name and *not* the print server device name.
2. Check the device name set in the print server. For more information, see the print server documentation.

Make sure the print server is communicating on the network

1. Ping the print server.
2. If the ping works, check the IP address, netmask, and gateway of the print server to make sure they are correct.
3. Turn the printer off, and then ping again to check for duplicate IP addresses.

   If the ping does not work, then print a setup page and check if the IP is enabled.
4. If TCP/IP is enabled, check the IP address, netmask, and gateway to make sure they are correct.
5. Make sure bridges and routers are functioning and configured correctly.
6. Make sure all the physical connections among the print server, the printer, and the network are working.

Device information is incorrect

If the application displays device information that appears to be incorrect, then perform an audit on the device.

Notices

Edition notice

January 2016

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

Firebird is a registered trademark of the Firebird Foundation.

Microsoft, Windows, SQL Server, and Active Directory are either registered trademarks or trademarks of the Microsoft group of companies in the United States and other countries.

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 of Security Terms

Access Controls	Settings that control whether individual device menus, functions, and settings are available, and to whom. Also referred to as Function Access Controls on some devices.
Authentication	A method for securely identifying a user.
Authorization	A method for specifying which functions are available to a user, i.e. what the user is allowed to do.
Group	A collection of users sharing common characteristics.
Security Template	A profile created and stored in the Embedded Web Server, used in conjunction with Access Controls to manage device functions.

Index

V