



# Markvision Enterprise

---

## User's Guide

# Contents

- Overview.....5**
- Getting started.....6**
  - Support statements.....6
    - System requirements.....6
    - Supported database servers .....6
  - Installing Markvision.....6
  - Upgrading to the latest version of Markvision.....7
  - Backing up and restoring the Firebird database.....8
  - Accessing Markvision.....9
  - Migrating from MarkVision Professional to Markvision Enterprise.....9
  - Using Markvision.....10
  - Understanding the home screen.....11
  - Understanding ports and protocols.....12
- Managing assets.....15**
  - Discovering devices.....15
    - Creating a discovery profile .....15
    - Editing or deleting a discovery profile .....16
    - Importing devices from a file .....16
  - Managing devices.....18
    - Setting the device life cycle state .....18
    - Auditing a device .....18
    - Viewing device properties .....19
- Locating and organizing devices within the system.....21**
  - Searching for devices within the system.....21
  - Working with bookmarks.....24
    - Creating bookmarks.....24
    - Accessing bookmarks.....24
    - Editing bookmarks .....24
  - Using categories and keywords.....24
    - Adding, editing, or deleting categories.....25
    - Adding, editing, or deleting keywords .....25
    - Assigning keywords to a device .....25
    - Removing an assigned keyword from a device.....26

---

- Managing configurations.....27**
  - Creating a configuration.....27
  - Creating a configuration from a device.....27
  - Importing files to the library.....28
  - Understanding variable settings.....28
  - Setting color printing permissions.....29
  - Understanding secured devices.....29
  - Understanding security settings.....31
  - Preparing solutions for enforcement.....31
    - Creating a solutions package .....31
    - Adding solutions to a configuration.....32
  - Assigning a configuration.....32
  - Editing a configuration.....32
  - Checking conformance with a configuration.....33
  - Enforcing a configuration.....33
  - Removing a configuration.....33
  
- Managing the Service Desk.....34**
  - Working with configuration.....34
    - Checking device conformance with a configuration .....34
    - Enforcing configurations.....34
  - Working with a device.....34
    - Checking the status of a device .....34
    - Viewing a device remotely.....35
    - Viewing the embedded Web page .....35
  
- Managing device events.....36**
  - Creating a destination.....36
  - Editing or deleting a destination.....36
  - Creating an event.....37
  - Creating events using Microsoft Event Viewer.....37
  - Editing or deleting an event.....38
  - Assigning an event to a device.....38
  - Removing an event from a device.....38
  - Displaying event details.....38
  
- Performing other administrative tasks.....39**
  - Downloading generic files.....39

- Configuring e-mail settings.....39
- Configuring system settings.....40
- Adding, editing, or deleting a user in the system.....40
- Enabling LDAP server authentication.....41
- Generating reports.....46
- Scheduling tasks.....47
- Viewing the system log.....47
- Exporting audit data of the device.....48
  
- Frequently asked questions.....49**
  
- Troubleshooting.....50**
  - User has forgotten the password.....50
  - The application is unable to discover a network device.....50
  - Device information is incorrect.....51
  
- Notices.....52**
  
- Glossary of Security Terms.....54**
  
- Index.....55**

## 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

## Support statements

For a complete list of supported operating systems and Web browsers, see the *Release Notes*.

## System requirements

### RAM

- Required: 1GB
- Recommended: 2GB+

### Processor speed

- Required: 1 physical 2GHz or higher (Hyper-Threaded/Dual Core)
- Recommended: 1+ physical 3+GHz (Hyper-Threaded/Dual Core+)

### Computer hard disk drive space

- At least 60GB available storage space

### Screen resolution

- At least 1024 x 768 pixels (for MVE clients only)

## Supported database servers

- Firebird
- Microsoft SQL Server 2012 (x86 and x64)
- Microsoft SQL Server 2008 x86
- Microsoft SQL Server 2005 x86

### Notes:

- An x86-based system refers to a 32-bit operating system, and an x64-based system refers to a 64-bit operating system.
- The application comes with a preconfigured Firebird database.
- The database server where MVE is installed must have only one *network interface card* (NIC).

## Installing Markvision

With Markvision, you can use either Firebird or Microsoft SQL Server as the back-end database.

Do the following before installing Markvision:

- 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

**Notes:**

- 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.
- If you are using Firebird, then Markvision automatically creates the user account and databases.

- 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:** Upgrading across several versions at once may cause database failures that will make the MVE application unusable. Make sure to upgrade only from the immediately preceding version.

### Example

Valid upgrade path	<b>1.9.x to 1.10.x to 2.0.x to 2.1.x</b>
Invalid upgrade path	<b>1.8.x to 1.10.x to 2.1.x</b>

- 1 Back up your database.

**Notes:**

- If you are using a Firebird database, then see [“Backing up the Firebird database” on page 8](#) for more information.
- If you are using Microsoft SQL Server, then contact your Microsoft SQL administrator.

- 2 Download the executable file into a temporary location.

**Note:** Make sure that the path does not contain any spaces.

- 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 49](#).
- If you are running MVE 1.x, then 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.
- After upgrading, make sure to clear the browser cache and flash cache.

# Backing up and restoring the Firebird database

## Backing up the Firebird database

**Note:** If you are using MS SQL Server as your database, then contact your MS SQL administrator.

- 1 Stop the Markvision Enterprise service.
  - a Click , or click **Start > Settings**.
  - b Select **Control Panel**, and then if necessary, click **System & Security**.
  - c Double-click **Administrative Tools**.
  - d If necessary, double-click **Component Services**.
  - e Double-click **Services**.
  - f From the Services pane, select **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 Repeat steps **1a** through **1e**.
  - b From the Services pane, select **Markvision Enterprise**, and then click **Restart**.

## Restoring the Firebird database

- 1 Make sure 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 8](#).
- 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 you saved when you were completing 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 8](#).



## Accessing Markvision

- 1 Open a Web browser, and then type `http://MVE_SERVER:9788/mve/` in the URL field.

**Note:** Replace *MVE\_SERVER* with the host name or IP address of the machine hosting Markvision.

- 2 Enter your login credentials.

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

If Markvision is idle for more than 30 minutes, then it automatically logs out. Log in again to access Markvision.

## Migrating from MarkVision Professional to Markvision Enterprise

**Note:** Markvision Enterprise (MVE) only supports migration of data from MarkVision Professional (MVP) v11.2.1.

### Exporting data from MVP

#### Using the MVP Server Web page

- 1 Open a Web browser, and then type `http://MVP_SERVER:9180/~MvServer` in the URL field.

**Note:** Replace *MVP\_SERVER* with the IP address or host name of the MVP Server.

- 2 From the MarkVision Server Web page, click **Data Dir**.
- 3 Enter your user name and password if prompted.
- 4 From the Download Data Directory page, click  to download your MVP data as a zip file.
- 5 Save the zip file.

#### Using the file system

- 1 On the system running the MVP Server, navigate to the location where the MVP Server is installed.
- 2 Compress the Data folder into a zip file.

### Importing data into MVE

- 1 Log in to Markvision Enterprise.
- 2 In the “Import data from MarkVision Professional” dialog, click **Yes**, and then click **Browse**.

**Notes:**

- If you click **Yes**, then the dialog does not appear the next time you log in to MVE.
- If you click **No** and you do not want to see the dialog again, then select **Do not show this message again**.

- 3 Navigate to the location where your zip file is stored, and then click **Open**.
- 4 From the “Data to Import” area, select the type of data that you want to import.

Data	Details
<b>Users</b>	<ul style="list-style-type: none"> <li>• In MarkVision Professional, users are given privileges for individual functions.</li> <li>• In Markvision Enterprise, users are assigned roles associated with different functions.</li> <li>• All users imported from MVP are automatically assigned to all roles except <b>ROLE_ADMIN</b>.</li> <li>• If an MVP user's password does not meet the MVE password criteria, then the string <b>Administrator1</b> is appended into the user's current password.</li> </ul>
<b>Devices</b>	<ul style="list-style-type: none"> <li>• MVE only imports basic device information from MVP, including model name, serial number, MAC address, and IP address.</li> <li>• If a printer already exists in MVE, then that printer is ignored during import.</li> <li>• During import, MVE disregards printers connected to External Network Adapters (ENAs), since MVE currently does not support ENAs.</li> <li>• The imported devices are automatically set to the <b>Managed (Normal)</b> life cycle state.</li> <li>• MVP manages printers and print servers. MVE only manages printers. Therefore, two entries in MVP become a single entry in MVE.</li> </ul>
<b>Discovery Profiles</b>	<ul style="list-style-type: none"> <li>• When MVP profiles are imported into the MVE system, only the following details are imported: <ul style="list-style-type: none"> <li>– SNMP Community Name</li> <li>– Retries</li> <li>– Timeout</li> <li>– Exclude Address</li> <li>– Include Address</li> </ul> </li> <li>• In MVP, each Include/Exclude entry contains an SNMP Read/Write Community Name set. A profile that contains multiple Include/Exclude entries may also contain multiple unique Read/Write Community Name sets. In MVE, the Read/Write Community Name set belongs to the profile itself. Each profile can contain only one Read/Write Community Name set. Therefore, one discovery profile in MVP (containing multiple unique Read/Write Community Name sets) is broken into multiple discovery profiles when imported into MVE (each containing one Read/Write Community Name set). The number of profiles in MVE is equal to the number of unique Read/Write Community Name sets in the original MVP profile.</li> <li>• For Timeout, MVE converts the MVP Timeout to milliseconds by multiplying the MVP value (in seconds) by 1000.</li> <li>• The Automatically Manage option is set to <b>False</b> during import.</li> </ul>

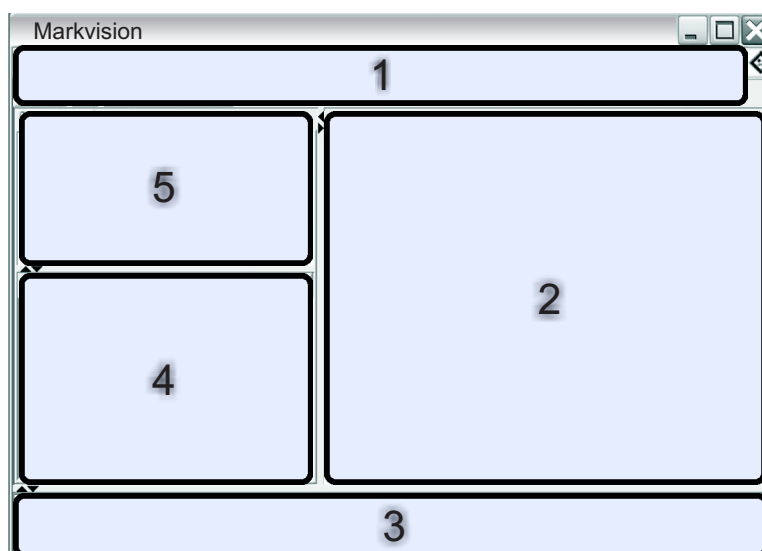
5 Click **Import**.

## 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
<b>Assets</b>	<ul style="list-style-type: none"> <li>• Locate, identify, catalog, organize, and track the physical assets that comprise the printer fleet.</li> <li>• Gather and maintain information on the fleet models, capabilities, installed options, and life cycle.</li> </ul> <p><b>Note:</b> In ITIL, this area fits into the Service Transition area. If your responsibilities include management of IT assets, then go to <a href="#">“Managing assets” on page 15</a>.</p>
<b>Configurations</b>	<ul style="list-style-type: none"> <li>• Define and manage configurations such as importing, exporting, or assigning configurations to selected devices.</li> <li>• Run a conformance check or enforce configurations to selected devices.</li> <li>• Deploy eSF apps, including licenses, to the printer fleet.</li> </ul> <p><b>Note:</b> In ITIL, this tab fits into the Service Transition area. If your responsibilities include administration and maintenance of configuration management tools, then go to <a href="#">“Managing configurations” on page 27</a>.</p>
<b>Service Desk</b>	<ul style="list-style-type: none"> <li>• Directly interact with a single device in the printer fleet.</li> <li>• Remotely manage the device, run a conformance check, enforce configurations, and customize configuration settings through the device Embedded Web Server.</li> </ul> <p><b>Note:</b> 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 <a href="#">“Managing the Service Desk” on page 34</a>.</p>
<b>Event Manager</b>	<p>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.</p> <p><b>Note:</b> In ITIL, this tab fits into the Service Operation area. If your responsibilities include problem management or incident handling, then go to <a href="#">“Managing device events” on page 36</a>.</p>

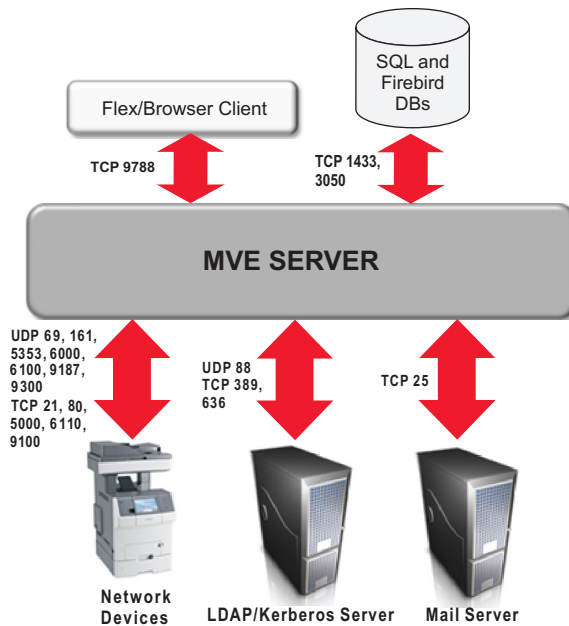
## Understanding the home screen



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

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



**Note:** The ports are bidirectional and must be open or active for Markvision 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 Markvision Server to network devices

Protocol	Markvision Server	Device	Used for
<b>NPAP</b> <i>Network Printer Alliance Protocol</i>	UDP 9187	UDP 9300	Communication with Lexmark network printers
<b>XMLNT</b> <i>XML Network Transport (Object Store)</i>	UDP 9187	UDP 6000	Communication with Lexmark network printers
<b>LST</b> <i>Lexmark Secure Transport</i>	UDP 6100 Ephemeral <i>Transmission Control Protocol (TCP)</i> port (handshaking)	UDP 6100 TCP 6110 (handshaking)	Encrypted communication with Lexmark network printers
<b>mDNS</b> <i>Multicast Domain Name System</i>	Ephemeral <i>User Datagram Protocol (UDP)</i> port	UDP 5353	Discovery of certain Lexmark network printers and determining the security capabilities of devices
<b>SNMP</b> <i>Simple Network Management Protocol</i>	Ephemeral UDP port	UDP 161	Discovery of and communication with Lexmark and third-party network printers
<b>FTP</b> <i>File Transfer Protocol</i>	Ephemeral TCP port	TCP 21 TCP 20	Generic file downloads
<b>TFTP</b> <i>Trivial File Transfer Protocol</i>	Ephemeral UDP port	UDP 69	Firmware updates and generic file downloads
<b>HTTP</b> <i>Hypertext Transfer Protocol</i>	Ephemeral TCP port	TCP 80	Generic or configuration file downloads
		TCP 443	Configuration file downloads
<b>Raw Print Port</b>	Ephemeral TCP port	TCP 9100	Generic or configuration file downloads

## Device to server communication

### Port and protocol used during communication from network devices to the Markvision Server

Protocol	Device	Markvision Server	Used for
<b>NPAP</b>	UDP 9300	UDP 9187	Generating and receiving alerts

## Server to database communication

### Ports used during communication from the Markvision Server to databases

Markvision Server	Database	Used for
Ephemeral TCP port	TCP 1433 (SQL Server) This is the default port and can be configured by the user.	Communication with an SQL Server database
Ephemeral TCP port	TCP 3050	Communication with a Firebird database

## Client to server communication

### Port and protocol used during communication from the flex or browser client to the Markvision Server

Protocol	Flex/Browser Client	Markvision Server
<b>AMF</b> <i>ActionScript Message Format</i>	TCP port	TCP 9788

## Messaging and alerts

### Port and protocol used during communication from the Markvision Server to a mail server

Protocol	Markvision Server	SMTP Server	Used for
<b>SMTP</b> <i>Simple Mail Transfer Protocol</i>	Ephemeral TCP port	TCP 25 This is the default port and can be configured by the user.	Providing the e-mail functionality used to receive alerts from devices

## Markvision Server to LDAP Server communication

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

Protocol	Markvision Server	LDAP Server	Used for
<b>LDAP</b> <i>Lightweight Directory Access Protocol</i>	Ephemeral TCP port	TCP 389, or the port to which the LDAP Server has been configured to listen	Authentication of Markvision Enterprise users using an LDAP Server
<b>LDAPS</b> <i>Secure Lightweight Directory Access Protocol</i>	Ephemeral TCP port	<i>Transport Layer Security (TLS)</i> , or the port to which the LDAP Server has been configured to listen This is for TLS-encrypted connections.	Authentication of Markvision Enterprise users using an LDAP Server through a secure channel that uses TLS
<b>Kerberos</b>	Ephemeral UDP port	UDP 88 This is the default Kerberos Authentication Service port.	Kerberos authentication

# Managing assets

## Discovering devices

The application lets you search the network for devices and save their identification information in the system. Use bookmarks or searches to show devices in the results area.

By default, discovered devices are set to **New**. Before an action is done on a device, set it to **Managed**. For more information, see [“Managing devices” on page 18](#).

To add devices to the system, do either of the following:


- **Using a discovery profile**—Discover devices in the network using customized parameters.
- **Importing devices from a file**—Use a comma-separated values (CSV) file to import devices.

**Note:** Performing both procedures results in duplicate devices.

After adding a device into the system, perform an audit of the device immediately to complete some tasks. For more information, see [“Auditing a device” on page 18](#).

**Note:** For restricted devices, assign a configuration and then enforce it on the restricted devices before performing an audit. When an audit fails, the restricted devices are set to **(Managed) Missing**. For more information, see [“Understanding secured devices” on page 29](#).

## Creating a discovery profile

- 1 If necessary, from the Assets tab, click **Discovery Profiles** to show the Discovery Profiles section.
- 2 Click **+**, and then type the name of the new discovery profile.
- 3 From the Addresses tab, select **Include** or **Exclude**.
- 4 To import a list of items from a file to include or exclude, do the following:
  - a Click .
  - b Navigate to the folder where the file is saved.
  - c Select the file, and then click **Open**.

**Note:** The file can contain any of the patterns that can be entered in the text field above Address/Range. To view examples of a valid pattern, mouse over the text field.

- 5 Beside **+**, type the IP address, fully qualified DNS host name, subnets with wildcard characters, or address ranges you want, and then click **+**.

### Notes:

- You can type only one entry at a time. To view examples of a valid entry, mouse over the text field above Address/Range.
- When typing address ranges, do *not* use wildcard characters.
- To delete an entry, select it, and then click **—**.

**6** Click the **SNMP** tab, and then select **Version 1,2c** or **Version 3**.

**Note:** If you are not sure which version of the SNMP you are using, then contact your system support person.

**7** If you selected **Version 1,2c** in [step 6](#), then from the Community Names area, set the privacy profile.

If you selected **Version 3**, then from the Security area, set the security profile.

**Note:** If you are not sure how to configure your SNMP Version 3 security profile, then contact your system support person.

**8** Click the **General** tab, and then from the Performance area, do the following:

- In the Timeout field, specify the amount of time (in milliseconds) to wait for the devices to respond.
- In the Retries field, specify the number of retries before the system stops attempting to communicate with a device.


**9** Select whether to include secured devices in the discovery.**Notes:**

- If you do not have a secured device, then do *not* select this option. Doing so incurs a performance penalty, which results to a much longer time in discovering devices.
- When a device is secured, one or both of the following conditions apply: (a) communication ports are disabled, and (b) authentication is required to obtain information from the device.

**10** Select whether the discovery profile should automatically manage the discovered devices.



**Note:** If you select this option, then all discovered devices are automatically set to the **Managed** life cycle state.

**11** Click **Save > Close**.**Notes:**

- Clicking  executes the discovery profile and does *not* save it.
- A new discovery profile gathers just enough information to reliably identify a device. To gather the complete information from a device, set the device state to **Managed**, and then perform an audit of the device.
- To make sure that the device information is current, a discovery can be scheduled to occur on a regular basis. For more information, see [“Scheduling tasks” on page 47](#).

## Editing or deleting a discovery profile

**1** If necessary, from the Assets tab, click **Discovery Profiles** to show the Discovery Profiles section.

**2** Select a profile, and then click  to edit or  to delete the discovery profile.

**3** Follow the instructions on the computer screen.

## Importing devices from a file

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



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

**1** From the Assets tab, click **Import**, and then click **Browse**.

**2** Navigate to the folder where the CSV file is stored.

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

**3** Select the CSV file, and then click **Open**.

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

**5** If you are using SNMP V3 protocol to communicate with the device, then you *must* 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 that you selected in [step 3](#), make sure the following parameters contain any 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**
  - **AES\_192**
  - **AES\_256**

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

**6** 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 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, and then use the arrows to move the headings up or down.

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

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

**9** 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 47](#).

## 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, select **Managed Printers** in the Bookmarks and Searches drop-down menu.

**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
<b>Identification</b>	The device network identification information.
<b>Dates</b>	The list of device events. This includes date added to system, discovery date, and the most recent audit date.
<b>Firmware</b>	The device firmware code levels.
<b>Capabilities</b>	The device features.
<b>Ports</b>	The available ports on the device.
<b>Supplies</b>	The device supply levels and details.
<b>Font Cartridges</b>	Information about any installed font cartridges.

Click	To view
<b>Options</b>	Information about the device options, such as the device hard disk and its remaining free space.
<b>Input Options</b>	Settings for the available paper trays and other device inputs.
<b>Output Options</b>	Settings for the available paper exit trays.
<b>eSF Applications</b>	Information about the installed <i>Embedded Solutions Framework</i> (eSF) applications on the device, such as version number and status.
<b>Device Statistics</b>	Specific values for each of the device properties.
<b>Change Details</b>	Information about the changes in the device. <b>Note:</b> This applies <i>only</i> to devices that are set in the <b>Managed (Changed)</b> state.

# Locating and organizing devices within the system

## Searching for devices within the system

### Using default bookmarks

Bookmarks denote a saved device search. When you select a bookmark, the devices that are shown match the criteria of the search.

The default bookmarks are based on the device life cycle state.

- 1 From the Bookmarks and Searches menu, select a bookmark:

Select	To search for
<b>Managed Printers</b>	Active devices in the system <b>Note:</b> Devices that appear when selecting this bookmark can be in any of the following states: <ul style="list-style-type: none"> <li>• Managed (Normal)</li> <li>• Managed (Changed)</li> <li>• Managed (Missing)</li> <li>• Managed (Found)</li> </ul>
<b>Managed (Normal) Printers</b>	Active devices in the system with device properties remaining the same since the last audit
<b>Managed (Changed) Printers</b>	Active devices in the system with device properties that have changed since the last audit
<b>Managed (Missing) Printers</b>	Devices that the system was unable to establish communication with
<b>Managed (Found) Printers</b>	Devices that are reported as missing from previous search queries, but have now been found
<b>New Printers</b>	Devices that are newly added to the system
<b>Unmanaged Printers</b>	Devices that have been marked for exclusion from activities performed in the system
<b>Retired Printers</b>	Devices that are no longer active in the system
<b>All Printers</b>	All devices in the system

- 2 From the Search Results Summary area, select a criterion to quickly and easily refine the results of your bookmarked search.

### Using Advanced Search

The Advanced Search feature lets you quickly perform complex searches based on one or multiple parameters.

- 1 From the Bookmarks and Searches menu, select **Advanced Search**.
- 2 Select whether all or at least one criterion should be met.

### 3 To add a search criterion, click **+**.

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

**Note:** If you group the search criteria, then the system treats all the defined criteria that are grouped together into one criterion.

### 4 From the Parameter menu, select a parameter:

Select	To search for
<b>Asset Tag</b>	Devices that have an assigned asset tag
<b>Color Capability</b>	Devices by their capability to print in color
<b>Contact Location</b>	Devices that have a specified location
<b>Contact Name</b>	Devices that have a specified contact name.
<b>Copy Capability</b>	Devices by their capability to copy files
<b>Disk Encryption</b>	Devices with installed hard disk that supports disk encryption
<b>Disk Wiping</b>	Devices with installed hard disk that supports disk wiping
<b>Duplex Capability</b>	Devices by their capability to perform two-sided printing
<b>eSF Application(Name)</b>	Devices by the specific name of the eSF application currently installed
<b>eSF Application(State)</b>	Devices by the current state of their installed eSF application
<b>eSF Application(Version)</b>	Devices by the version of their installed eSF application
<b>ESF Capability</b>	Devices by their capability to manage an Embedded Solutions Framework (eSF) application
<b>Firmware Version</b>	Devices by their firmware version
<b>Firmware:AIO</b>	Devices by the AIO value of their firmware
<b>Firmware:Base</b>	Devices by the base version of their firmware
<b>Firmware:Engine</b>	Devices by the engine of their firmware
<b>Firmware:Fax</b>	Devices by the fax value of their firmware
<b>Firmware:Font</b>	Devices by the font value of their firmware
<b>Firmware:Kernel</b>	Devices by the kernel value of their firmware
<b>Firmware:Loader</b>	Devices by the loader value of their firmware
<b>Firmware:Network</b>	Devices by the network value of their firmware
<b>Firmware:Network Driver</b>	Devices by the network driver value of their firmware
<b>Firmware:Panel</b>	Devices by the panel version of their firmware
<b>Firmware:Scanner</b>	Devices by the scanner version of their firmware
<b>Hostname</b>	Devices by their host names
<b>IP Address</b>	<p>Devices by their IP addresses</p> <p><b>Note:</b> You may use an asterisk (*) as a wildcard character in the last three octets of the IP address to find all matching IP addresses. If an asterisk is used in an octet, then the remaining octets must also contain asterisks.</p> <ul style="list-style-type: none"> <li>Valid examples are 123.123.123.*, 123.123.*.*, and 123.*.*.*.</li> <li>An <i>invalid example</i> is 123.123.*.123.</li> </ul>

Select	To search for
<b>Keyword</b>	Devices by their assigned keywords, if any
<b>Lifetime Page Count</b>	Devices by their lifetime page count values
<b>MAC Address</b>	Devices by their MAC addresses
<b>Maintenance Counter</b>	Devices by the value of their maintenance counter
<b>Manufacturer</b>	Devices by the name of their manufacturer
<b>Marking Technology</b>	Devices by the value of the marking technology that they support
<b>MFP Capability</b>	Devices by their capability to be a multifunction printer (MFP)
<b>Model</b>	Devices by their model names
<b>Printer Status</b>	Devices by their current status (for example: <b>Ready, Paper Jam, Tray 1 Missing</b> )
<b>Profile Capability</b>	Devices by their supported profile capability
<b>Receive Fax Capability</b>	Devices by their capability to receive incoming fax
<b>Scan to E-mail Capability</b>	Devices by their capability to perform a Scan to E-mail task
<b>Scan to Fax Capability</b>	Devices by their capability to perform a Scan to Fax task
<b>Scan to Network Capability</b>	Devices by their capability to perform a Scan to Network task
<b>Serial Number</b>	Devices by their serial number
<b>State</b>	Devices by their current state in the database
<b>Supply Status</b>	Devices by the current status of their supplies
<b>System Name</b>	Devices by their system names

5 From the Operation menu, select an operator:

Select	To search for
<b>Contains</b>	Devices with a parameter that contains a specific value
<b>Does not contain</b>	Devices with a parameter that does not contain a specific value
<b>Does not equal</b>	Devices with a parameter that is not equivalent to an exact value
<b>Ends with</b>	Devices with a parameter that ends with a specific value
<b>Equals</b>	Devices with a parameter that is equivalent to an exact value
<b>Starts with</b>	Devices with a parameter that begins with a specific value

6 From the Value field or drop-down menu, enter the value of the parameter.

**Note:** If you want to delete the criterion, then click **X**.

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

The located devices appear in the Search Results area.


8 From the Search Results Summary area, select a criterion to quickly and easily refine the results of your bookmarked search.

## Working with bookmarks

Bookmarks denote a saved search.

When a device enters the system and meets the criteria specified for a bookmark, the device is included in the search results whenever the bookmark is selected.

### Creating bookmarks


- 1 From the Bookmarks and Searches drop-down menu, select the bookmark that represents the group of devices from which you would like to begin your search.  
To refine the search, click **Advanced Search**.
- 2 If necessary, under Search Results Summary, click the available subcategories to further refine the search.
- 3 When the device or group of devices that you want appears in the search window, click  .
- 4 Enter a name for the bookmark, and then click **OK**.

### Accessing bookmarks

- 1 From the Bookmarks and Searches drop-down menu, select the bookmark you want to view.
- 2 If necessary, under Search Results Summary, click the available subcategories to further refine the search.

### Editing bookmarks

**Note:** Default bookmarks cannot be edited or deleted.

- 1 From the Bookmarks and Searches menu, select **Manage bookmarks**.
- 2 Select the bookmark, and then click  .
- 3 If necessary, rename the bookmark, and then adjust the search criteria settings.
- 4 Apply the changes.

## 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. Make sure that a device or group of devices matches a configuration by running a conformance check. 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

- 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 Customize the settings for the configuration.
  - a From the Device Settings tab, do the following:
    - 1 Select a configuration type.
    - 2 Select **Setting Name**, and then set the value for each setting that you want to include when running a conformance check and enforcing configurations.


### Notes:

- You can use variables as the value for a setting. 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.
  - Tokens are case-sensitive.
- b From the Security tab, configure the security settings. For more information, see [“Understanding secured devices” on page 29](#) and [“Understanding security settings” on page 31](#).
  - c From the Firmware tab, select a transfer method, and then if necessary, select a firmware file.

**Note:** You can import a firmware file from the MVE Resource Library. For more information, see [“Importing files to the library” on page 28](#).
  - d From the Solutions tab, select one or more solutions to deploy. For more information, see [“Preparing solutions for enforcement” on page 31](#).
- 4 Apply the changes.

## Creating a configuration from a device

**Note:** When you create a standalone configuration, security settings cannot be cloned from a device and cannot be used in the existing configuration. To use security settings, make sure to create a configuration from a device.

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

**Notes:**

- When cloning a device, make sure that the host name setting is disabled before enforcing the cloned configuration to other devices. You can use variable settings to assign a unique host name to a device. For more information, see [“Understanding variable settings” on page 28](#).
- 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.
- To edit the configuration, see [“Editing a configuration” on page 32](#).

## 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

Markvision also uses variable settings for 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 defined by the user. 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, 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 spreadsheet application.

**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 27](#) or [“Editing a configuration” on page 32](#).

## Setting color printing permissions

Monitor color printing and save resources by restricting color printing to specific users.

- 1 Create or edit a configuration.
- 2 From the Device Settings section, select a color print permission.
  - **Hosts Table**—Restrict color printing permissions for each specified host computer.
  - **Users Table**—Restrict color printing permissions for each specified user ID.
- 3 Click **View**.
- 4 Add or edit host computers or user IDs, and then set the permissions you want to use.

**Note:** Settings in Hosts Table override user-level permissions.
- 5 Apply the changes.

## Understanding secured devices

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

		Fully unrestricted	Fully restricted
Device settings	<p><i>Remote Management Function Access Control (RM FAC) or advanced password</i></p> <p><b>Note:</b> For a list of devices that support the RM FAC, see the <i>Release Notes</i> for the application.</p>	No security or no password	RM FAC is set using a security template, or a password is configured
	Significant ports	The following ports are open: <ul style="list-style-type: none"> <li>• UDP 161 (SNMP)</li> <li>• UDP 9300/9301/9302 (NPAP)</li> </ul>	Closed
	Security-related ports	The following ports are open: <ul style="list-style-type: none"> <li>• UDP 5353 (mDNS)</li> <li>• TCP 6110</li> <li>• TCP/UDP 6100 (LST)</li> </ul>	The following ports are open: <ul style="list-style-type: none"> <li>• UDP 5353 (mDNS)</li> <li>• TCP 6110</li> <li>• TCP/UDP 6100 (LST)</li> </ul>
Markvision settings	Discovery profile	Make sure that the <b>Include secured printers in the discovery</b> option is cleared.	Make sure that the <b>Include secured printers in the discovery</b> option is selected.
	Are secure channels used for communication between Markvision and the network devices?	No <b>Note:</b> This type of configuration is recommended, unless there are settings that require secure channels.	Yes
	How do I determine the security configuration of the devices in my network?	In the main data grid in Markvision, an <i>open</i> padlock icon appears beside the IP address of a fully unrestricted device.	In the main data grid in Markvision, a <i>closed</i> padlock icon appears beside the IP address of a fully restricted device. <b>Note:</b> If Markvision cannot identify the communication credentials of the device, then the closed padlock icon has a red slash through it. The red slash means that Markvision cannot currently communicate, beyond this minimal discovery, with the device. To remove the red slash, make sure to enforce a configuration with the correct communication credentials before enforcing it to the restricted device.
	How do I search for devices that have this type of configuration?	<ol style="list-style-type: none"> <li>1 From the “Bookmarks and Advanced Search” area, select <b>All Printers</b>.</li> <li>2 From the Search Results Summary area, scroll down to the Communications category, and then select <b>Unsecured</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1 From the “Bookmarks and Advanced Search” area, select <b>All Printers</b>.</li> <li>2 From the Search Results Summary area, scroll down to the Communications category, and then select <b>Secured</b>.</li> </ol>

**Notes:**

- If the device or discovery profile is not fully unrestricted or fully restricted, then an unexpected or undefined behavior may occur.
- Before discovering a device, make sure that it is ready and the discovery profile is configured correctly. If you change the state or the configuration after executing the discovery profile, then delete the device and run the discovery again.

## Understanding security settings

Make sure that the security settings adhere to the following parameters:

- From the General Settings section of the security setting, set the following port access to **Enabled** or **Secure and Unsecure**:
  - Port Access: TCP/UDP (6110/6100)
  - Port Access: mDNS (UDP 5353)

To enable mDNS from the Embedded Web Server, navigate to either of the following:

- **Settings > Network/Ports > TCP/IP > Enable mDNS > Submit**
- **Configuration > Network/Ports > TCP/IP > mDNS > Submit**
- Depending on your printer model, from the Access Controls section, set the NPA Network Adapter Setting Changes and Firmware Updates settings to **No Security**.
- The following sections are read-only and cannot be edited:
  - Access Controls
  - Security Templates

**Note:** Provide the credentials for building blocks under the Authentication Setup column.


  - Miscellaneous Settings

**Note:** The Access Controls, Security Templates, and Miscellaneous Settings sections are available only in some printer models. For more information, see the *Embedded Web Server — Security Administrator's Guide* for your printer.

## 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 28](#).
- 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.

## 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.




## 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 47](#).

## 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 47](#).

## 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
	<b>OK</b> —The device is ready and supplies are sufficient.
	<b>Warning</b> —The device is working, but supplies may be low or may require attention at a later time.
	<b>Error</b> —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 only available for 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**.

A dialog appears, showing the device details and a picture of the device.

**3** Click **Remote Operator Panel** > **Click here to continue**.

Another dialog appears, remotely showing a dynamic display of the device control panel in its current state.

**4** From the lower left side, refer to 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 only available for 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**.

A dialog appears, showing the device details and a picture of the device.

**3** Click **Embedded Web Page**.

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

# Managing device events

Event Manager lets you proactively monitor and manage 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.

## 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 39](#).
    - 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**.

## Creating events using Microsoft Event Viewer



- 1 Run the command prompt with administrative privileges.
- 2 Go to the root directory where Event Viewer is installed.
- 3 In the command prompt, type `eventcreate /l application /t error /id 1 /so mve /d "$ {ConfigurationItem.ipAddress} ${alert.name}"` where
  - `/l` specifies the event location.
  - `/t` specifies the type of event.
  - `/id` specifies the event ID.
  - `/so` specifies the event source.
  - `/d` specifies the event description.

### Notes:


- You need to configure the destination path in MVE. Set the **Command Path (Required)** as `C:\Windows\system32\event.exe` and the **Command Parameters (Optional)** with your created event. For more information on creating a destination, see [“Creating a destination” on page 36](#).

- For more information on Event Viewer, visit [www.microsoft.com](http://www.microsoft.com).


## 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

The application lets you download miscellaneous files from the Markvision Server to one or more devices on a network. This allows for the 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 Click **Browse**, and then navigate to the folder where the file is saved.
- 4 Select the file you want to download, and then click **Open**.
- 5 From the Destination menu, select one of the following:
  - **Configuration File (HTTPS)**—This downloads a configuration file to the printer.
  - **Firmware Update**—This downloads a firmware update for the devices.
  - **Print (FTP)**—This downloads a printable file over an FTP network.
  - **Print (raw socket)**—This downloads a printable file from the computer.
  - **UCF Configuration (HTTP)**—This downloads a printer UCF.
  - **UCF Configuration (FTP)**—This downloads a network UCF.
- 6 Click **Download**.


### Notes:

- The Generic File Download task will not be available when the Printer Lockdown option is enabled.
- A Generic File Download task can be scheduled to occur at a predetermined time or on a regular basis. For more information, see [“Scheduling tasks” on page 47](#).

## 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


Lightweight Directory Access Protocol (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*.

Markvision administrators can use the company LDAP server to authenticate user IDs and passwords, eliminating the need to maintain multiple user credentials.

Markvision attempts to authenticate against the valid user credentials present in the system. If Markvision is unable to authenticate the user on the first attempt, then it attempts to authenticate against users registered in the LDAP server. If the same user names exist in both the Markvision and LDAP servers, then use the Markvision password.

As a prerequisite, the LDAP server must contain user groups that correspond to roles defined in [“Adding, editing, or deleting a user in the system” on page 40](#).

### Step 1. Configure the authentication settings

1 From the Header area, click  > **LDAP** tab.

2 Select **Enable LDAP for Authentication**.

3 From the Authentication Information section, type the values in the appropriate fields.

- **Server**—Type the IP address or the host name of the LDAP Directory server where the authentication occurs.

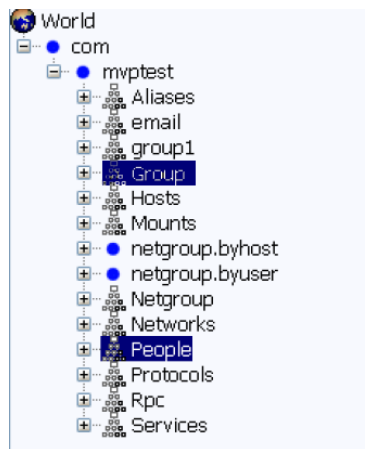
If you want to use encrypted communication between the MVE server and the LDAP Directory server, then do the following:

- 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/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 Transport Layer Security (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 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`

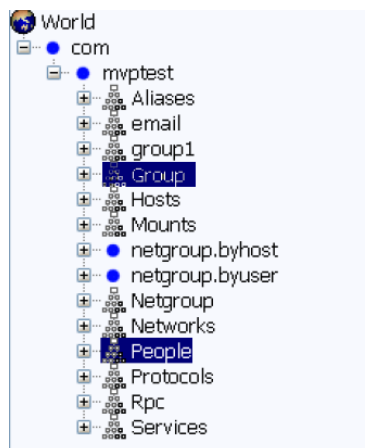


**Note:** When specifying the Root DN, make sure that only `dc` and `o` are part of the Root DN expression. If `ou` or `cn` stands as the common ancestor of the user and group nodes, then use `ou` or `cn` in the User Search Base and Group Search Base expressions.

- 4 If you want Markvision to search for nested users within the LDAP Community server, then select **Enable Nested User Search**.

To refine the search query, type the values in the appropriate fields.

- **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`

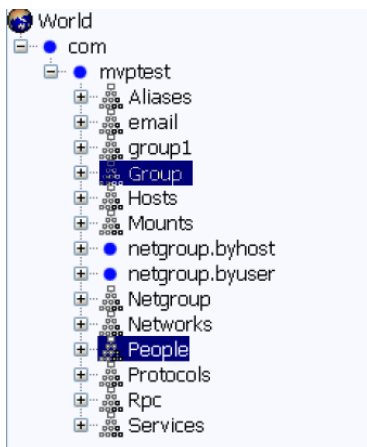


If the users are at multiple directory hierarchical levels in the LDAP Community server, then do the following:

- a Calculate any common upstream hierarchy of all the possible locations of the User node.
- b Include the configuration in the User Search Base field.

**Note:** If you want Markvision to search for users starting at the Base/Root DN, then 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})
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.

**5** If you want Markvision to search for nested *groups* within the LDAP Community server, then select **Enable Nested Group Search**.

To refine the search query, type the values in the appropriate fields.

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

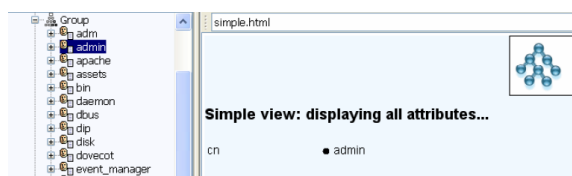


**Note:** A Search Base consists of multiple attributes separated by commas, such as cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain).

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

**Note:** You may use the patterns `{0}` and `{1}`, depending on the schema configuration of your back-end LDAP Community server. If you use `{0}`, then MVE searches for the LDAP User DN (Distinguished Name). 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 (role). For example, `cn`



**Note:** Select **Enable Nested User Search** and **Enable Nested Group Search** to specify the depth of the LDAP Community server. Use Nested Search (SubTree) to search all nested levels under and including the specified User Search Base and Group Search Base.

## Step 2. Configure the binding settings

This section determines the protocol that the MVE server uses to communicate with the external LDAP Directory server.

### 1 Click **Binding Information**.

**Notes:**

- If there is no LDAP configuration stored in Markvision, then Anonymous LDAP Bind is selected by default. The MVE server does not produce its identity or credential to the LDAP server for using the LDAP server lookup facility. The follow-up LDAP lookup session is unencrypted communication only.

- The Windows Active Directory LDAP does not support the Anonymous Bind option.

**2** If you want the MVE server to use the LDAP server lookup facility, then configure the Simple Bind option.

- a** Select **Simple Bind**.
- b** In the Bind DN field, type the bind-distinguished name.
- c** Type the binding password, and then confirm the password.

**Notes:**

- The Bind Password is dependent on the Bind User settings in the LDAP Directory 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.
- The Simple Bind option uses unencrypted communication between MVE and LDAP.

**3** If you want to use encrypted communication between the MVE server and the LDAP Directory server, then select **TLS** or **Kerberos V5 (Windows Active Directory)**.

If you selected **TLS**, then the MVE server fully authenticates itself to the LDAP Directory server using the MVE server identity (Bind DN) and credentials (Bind Password).

- a** In the Bind DN field, type the bind-distinguished name.
- b** Type the binding password, and then confirm the password by typing it again.

**Note:** The Bind Password is required.

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 Markvision.

If you selected **Kerberos V5 (Windows Active Directory)**, then do the following:

- a** In the KDC Username field, type the Key Distribution Center (KDC) name.
- b** Type the KDC password, and then confirm the password.
- c** Click **Browse**, and then navigate to the folder where the `krb5.conf` file is stored.

**Notes:**

- For more information on the Kerberos configuration file, see the documentation for your Kerberos security protocol.
- The Kerberos security protocol is supported only in a Windows Active Directory that has GSS-API support endorsement.

- d** Select the file, and then click **Open**.

### Step 3. Configure the Role Mapping settings

**1** Click **Role Mapping**.

**2** Type the values in the appropriate fields.

- **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 (role) 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 an MVE 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.

**3** To validate your configuration, click **Test**.


**4** Type your LDAP user name and password, and then click **Test Login**.

If there are errors, then do the following:

- Review the information in the dialog to determine the cause of the errors.
- Update the entries you made in the Authentication Information, Binding Information, and Role Mapping tabs.
- Repeat [step 3](#) through [step 4](#) until there are no more errors from the Test LDAP Configuration Results dialog.

**5** 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
<b>Lifecycle State - Summary</b>	A summarized report of the life cycle states of the devices.
<b>Printer Manufacturer - Summary</b>	A summarized report of device manufacturers.
<b>Printer Model - Summary</b>	A summarized report of device model names and numbers.
<b>Printer Capabilities - Summary</b>	A summarized report of device capabilities.
<b>Printer Capabilities</b>	A spreadsheet listing device capabilities.
<b>Lifecycle State</b>	A spreadsheet listing the life cycle states of devices.
<b>Lifetime Page Count</b>	A spreadsheet listing the lifetime page count of devices.
<b>Maintenance Count</b>	A spreadsheet listing the maintenance count of devices.
<b>Firmware Versions</b>	A spreadsheet listing the firmware versions of devices.
<b>eSF Solutions</b>	A spreadsheet listing the different Embedded Server Framework (eSF) solutions installed on the devices.
<b>Disk Security</b>	A spreadsheet listing the hard disk enabled devices and the state of the disk security.
<b>Statistics:Jobs by Printed Sheets</b>	A spreadsheet listing the number of print jobs performed by the devices.
<b>Statistics:Jobs by Media Sides Count</b>	A spreadsheet listing the number of pick counts for print, fax, and copy jobs performed by the devices.


Select	To view
<b>Statistics:Jobs by Scan Usage</b>	A spreadsheet listing the number of scan jobs performed by the devices.
<b>Statistics:Jobs by Fax Usage</b>	A spreadsheet listing the number of fax jobs performed by the devices.
<b>Statistics:Jobs by Supply Information</b>	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

October 2014

**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](http://www.lexmark.com).

© 2014 Lexmark International, Inc.

All rights reserved.

## Trademarks

Lexmark, Lexmark with diamond design, and MarkVision are trademarks of Lexmark International, Inc., registered in the United States and/or 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 227.7202-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

## JmDNS License

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

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

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

Arthur van Hoff

avh@strangeberry.com

Rick Blair

rickblair@mac.com

\*\* JmDNS

## Licensing notices

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

# Glossary of Security Terms

<b>Access Controls</b>	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.
<b>Authentication</b>	A method for securely identifying a user.
<b>Authorization</b>	A method for specifying which functions are available to a user, i.e. what the user is allowed to do.
<b>Group</b>	A collection of users sharing common characteristics.
<b>Security Template</b>	A profile created and stored in the Embedded Web Server, used in conjunction with Access Controls to manage device functions.

# Index

## A

- adding a user 40
- adding solutions to a configuration 32
- advanced search, using 21
- application log files
  - locating 49
- assets tab
  - using 10
- assigning a configuration 32
- assigning an event to a device 38
- assigning keywords to a device 25
- audit data
  - exporting 48
- auditing a device 18

## B

- backing up Firebird database 8
- bookmarks
  - accessing 24
  - creating 24
  - editing 24
- Bookmarks and Advanced Searches area 11

## C

- categories
  - adding 25
  - deleting 25
  - editing 25
  - using 24
- changing passwords 49
- checking conformance with a configuration 33
- checking device conformance with a configuration 34
- checking device status 34
- color print permissions
  - setting 29
- computer RAM 6
- configuration
  - assigning 32
  - checking conformance 33
  - checking device conformance 34
  - creating 27
  - creating from a device 27
  - editing 32

- enforcing 33, 34
  - removing 33
- configurations
  - managing 27
  - using 10
- configuring e-mail settings 39
- configuring system settings 40
- creating
  - event 37
- creating a configuration 27
- creating a configuration from a device 27
- creating a discovery profile 15
- creating a solutions package 31
- creating an event 37
  - Event Viewer 37
- creating bookmarks 24
- CSV
  - variable settings 28

## D

- database servers
  - supported 6
- default bookmarks, using 21
- deleting a destination 36
- deleting a discovery profile 16
- deleting a user 40
- deleting an event 38
- destination
  - creating 36
  - deleting 36
  - editing 36
- device
  - assigning an event 38
  - assigning keywords 25
  - auditing 18
  - checking status 34
  - displaying event details 38
  - importing from a file 16
  - removing an assigned keyword 26
  - removing an event 38
  - viewing properties 19
  - viewing remotely 35
- device life cycle state
  - Managed 18
  - Managed (Changed) 18
  - Managed (Found) 18
  - Managed (Missing) 18

- Managed (Normal) 18
- Retired 18
- setting 18
- Unmanaged 18
- device status
  - checking 34
- device, alerts
  - receiving 40
- device, host name
  - acquiring 40
- devices
  - discovering 15
  - searching for 21
- discovering devices 15
- discovery profile
  - creating 15
  - deleting 16
  - editing 16
- displaying event details 38
- downloading generic files 39

## E

- editing a configuration 32
- editing a destination 36
- editing a discovery profile 16
- editing a user 40
- editing an event 38
- editing bookmarks 24
- embedded Web page
  - viewing 35
- enabling LDAP server authentication 41
- enforcing a configuration 33
- enforcing configuration 34
- event
  - creating 37
  - deleting 38
  - displaying details 38
  - editing 38
  - removing from a device 38
- event manager tab
  - using 10
- Event Viewer
  - creating an event 37
- exporting audit data
  - device 48
- exporting CSV
  - variable settings 28

e-mail  
configuring settings 39

## F

files  
downloading 39  
importing to the library 28  
Firebird database  
backing up 8  
restoring 8  
forgotten user password 50

## G

General tab  
using 40  
generating reports 46  
getting started  
home screen 11

## H

Header area 11  
home screen  
understanding 11  
host name  
printer 49  
host name and reverse DNS lookup  
difference 49  
host name lookup  
reverse lookup 49

## I

importing CSV  
variable settings 28  
importing devices from a file 16  
importing files  
to the library 28  
importing files to the library 28  
incorrect device information 51  
installer log files  
locating 49  
installing Markvision 6  
IP address  
printer 49

## K

keywords  
adding 25  
assigning to a device 25  
deleting 25  
editing 25

removing from a device 26  
using 24

## L

LDAP server  
enabling authentication 41  
library  
importing files to 28  
log files  
locating 49

## M

managing configurations 27  
Markvision  
accessing 9  
installing 6  
using 10  
Markvision Enterprise  
upgrading to latest version 7  
MarkVision Professional  
migrating to Markvision  
Enterprise 9  
migrating from MarkVision  
Professional to Markvision  
Enterprise 9  
MVE  
migrating to 9  
MVP  
importing to Markvision  
Enterprise 9  
migrating to Markvision  
Enterprise 9

## N

notices 52

## O

overview 5

## P

password, user  
resetting 50  
passwords  
changing 49  
placeholders 36  
ports  
understanding 12  
Printer Status 34  
processor speed 6

properties, device  
viewing 19  
protocols  
understanding 12

## R

receiving alerts from devices 40  
removing a configuration 33  
removing an assigned keyword  
from a device 26  
removing an event from a  
device 38  
reports  
generating 46  
resetting user password 50  
restoring Firebird database 8  
reverse DNS lookup  
in MVE 49

## S

scheduling tasks 47  
Search Results area 11  
Search Results Summary area 11  
searching for devices 21  
secured devices  
understanding 29  
security settings  
understanding 31  
service desk tab  
using 10  
settings  
security 31  
solutions  
adding to a configuration 32  
solutions package  
creating 31  
Supply Status 34  
supported database servers 6  
supported devices 49  
supported models list 49  
system log  
viewing 47  
system names  
verifying 50  
system requirements  
computer hard disk drive space 6  
processor speed 6  
RAM 6  
screen resolution 6  
system settings  
configuring 40



**T**

Task Information area 11

tasks

- scheduling 47

troubleshooting

- incorrect device information 51

- resetting user password 50

- unable to discover a network device 50

**U**

unable to discover a network device 50

understanding ports 12

understanding protocols 12

understanding secured devices 29

understanding the home screen 11

upgrading to the latest version of Markvision 7

user

- adding, editing, or deleting 40

using categories 24

using keywords 24

**V**

variable settings

- understanding 28

viewing a device remotely 35

viewing device properties 19

viewing the embedded Web page 35

viewing the system log 47