Lexmark™

Markvision Enterprise

User's Guide

July 2016

www.lexmark.com

Contents

Overview.. 5

Definition of terms.. 5

Getting started..7

Installing MVE..7

Upgrading to the latest version of MVE..7

Backing up and restoring the Firebird database..8

Understanding ports and protocols..9

Accessing MVE.. 12

Understanding the home screen.. 13

Setting up user access..14

Managing users..14

Enabling LDAP server authentication.. 14

Enabling Kerberos authentication..19

Managing assets..20

Discovering devices.. 20

Managing devices.. 23

Locating and organizing devices within the system..26

Searching for devices within the system.. 26

Understanding search criteria settings..27

Using categories and keywords..29

Managing configurations.. 31

Creating a configuration.. 31

Creating a configuration from a device.. 31

Assigning a configuration..32

Editing a configuration.. 32

Exporting or importing a configuration..33

Importing files to the library..33

Understanding variable settings.. 33

Understanding secured devices.. 34

Managing security settings..35

Preparing solutions for enforcement 36

Checking conformance with a configuration 37

Enforcing a configuration 37

Performing service desk tasks 39

Checking device conformance with a configuration 39

Enforcing configurations 39

Checking the status of a device 39

Working with a device 39

Rebooting devices 40

Managing device events 41

Creating a destination 41

Editing or deleting a destination 42

Creating an event 42

Editing or deleting an event 43

Assigning an event to a device 43

Removing an event from a device 43

Displaying event details 44

Performing other administrative tasks 45

Deploying generic files 45

Configuring e‑mail settings 45

Configuring system settings 46

Adding a login disclaimer 46

Enabling data sharing 46

Generating reports 46

Scheduling tasks 47

Viewing the system log 49

Exporting audit data of the device 49

Frequently asked questions 51

Troubleshooting 52

User has forgotten the password 52

Cannot discover a network device 52

Incorrect device information 53

Notices.. 54

Index...56

Overview

Markvision^{TM} Enterprise (MVE) is a web-based device management utility designed for IT professionals. It lets you find, organize, and configure a large fleet of devices in an enterprise environment. The application provides a set of features and tasks that helps you manage those devices efficiently.

The MVE application is divided into four key areas:

- **Assets**—Find, organize, and track a fleet of devices. You can audit a device to collect device data such as status, settings, and supplies. You can view these data in the asset properties for each device.
- **Configurations**—Define and manage configurations such as importing, exporting, or assigning configurations to devices. In a configuration, you can modify the printer settings and deploy Embedded Solutions Framework (eSF) applications, including licenses to the devices. You can also deploy firmware and certificate authority (CA) certificates to the devices. To apply the configuration settings to a device, run a conformance check, and then enforce the configuration to the device.
- **Service Desk**—Access the printer control panel remotely or modify the printer configuration settings using the Embedded Web Server.

  Note: Remote access to the control panel is available only in some printer models.
- **Event Manager**—Create an event that sends alerts to the network automatically, depending on the printer occurrences that are set to trigger the alerts. An event may include supply level warnings, paper jam errors, and other occurrences. You can send the alerts using a script or e-mail.

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.

Definition of terms

- **Audit**—The task of collecting device data such as printer status, supplies, and settings.
- **Bookmark**—A saved search that filters the device list based on the default or user-defined criteria.
- **Clone**—The task of copying discovery profile settings into a new discovery profile. For configurations, cloning does not copy the settings of another configuration but only creates a configuration based on a device.
- **Configuration**—A collection of settings that can be assigned and enforced to a device or a group of devices of the same model. Within a configuration, you can modify printer settings and deploy applications, licenses, firmware, and CA certificates to the devices.
- **Destination**—A predefined action that can be either an e-mail notification or a command-line operation. The action is triggered when a device event occurs.
- **Device state**—The status of a device in the system that determines whether the device has been changed, removed, or in its steady state.
- **Discovery profile**—A profile that contains a set of parameters used to find devices on a network. It may also contain predefined configurations that can be assigned and enforced to devices automatically during the discovery.
- **Event**—An automated alert that e-mails notifications or executes a command, depending on the device occurrences that are set to trigger the alerts. Each event must be associated with one or more destinations.
- **Function access control**—A feature in the printer that lets you limit user access to functions, applications, and printer management.

- **Keyword**—A custom text assigned to devices that you can use to search for those devices within the system. When you filter a search using a keyword, only devices that are tagged with the keyword are shown.
- **Report**—A summary of information that provides statistical data on the status or activities of devices that are managed in the system.
- **Secured device**—A printer that is configured to communicate through an encrypted channel and requires authentication to access its functions or applications.
- **Token**—An identifier that represents device data values for variable settings in a configuration.
- **Variable settings**—A set of device settings containing dynamic values that can be integrated into a configuration.

Getting started

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

Installing MVE

Preparing the database

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

- Enable mixed mode authentication and Auto Run.
- Set the Network Libraries to use a static port and TCP/IP sockets.
- Create a user account that MVE 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 operations.
  - Passwords are not saved. Make sure that you remember your passwords, or store them in a secure location.

Installing the application

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

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

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

Upgrading to the latest version of MVE

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

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

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

1 Back up your database.

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

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

Notes:

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

2. Download the executable file into a temporary location.
3. Run the file, and then follow the instructions on the computer screen.

Notes:

- When you upgrade to MVE 2.0, policies that are assigned to devices are migrated into a single configuration for each printer model. For example, if Fax, Copy, Paper, and Print policies are assigned to an X792 printer, then those policies are consolidated into an X792 configuration. This process does not apply to policies that are not assigned to devices. MVE generates a log file confirming that the policies are migrated to a configuration successfully. For more information, see “Where can I find the log files?” on page 51.
- After upgrading, make sure to clear the browser cache and flash cache before accessing the application again.

Backing up and restoring the Firebird database

Backing up the Firebird database

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

1. Stop the Markvision Enterprise service.
   - **a** Open the Windows® Run dialog box, and then type `services.msc`.
   - **b** Right-click **Markvision Enterprise**, and then click **Stop**.
2. Locate the folder where Markvision Enterprise is installed, and then navigate to **firebird\data**.

   For example, `C:\Program Files\Lexmark\Markvision Enterprise\firebird\data`
3. Copy the following databases to a safe repository.
   - FRAMEWORK.FDB
   - MONITOR.FDB
   - QUARTZ.FDB
4. Restart the Markvision Enterprise service.
   - **a** Open the Windows Run dialog box, and then type `services.msc`.
   - **b** Right-click **Markvision Enterprise**, and then click **Restart**.

Restoring the Firebird database

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

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

1 Make sure that you have backed up 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 that you saved during the backup process.

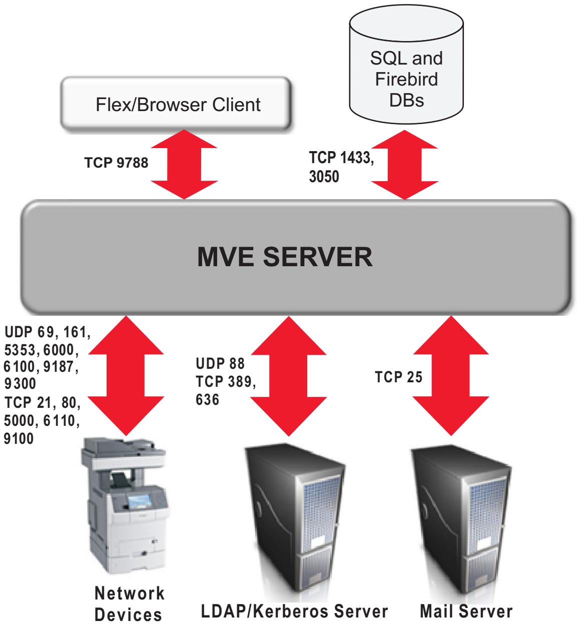
   - FRAMEWORK.FDB
   - MONITOR.FDB
   - QUARTZ.FDB

5 Restart the Markvision Enterprise service.

   For more information, see step 4 of "Backing up the Firebird database" on page 8.

Understanding ports and protocols

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



Notes:

- The ports are bidirectional and must be open or active for MVE to function properly. Depending on the printer model, make sure that all the device ports are enabled or set to **Secure and Unsecure**.
- Some communications require an ephemeral port, which is an allocated range of available ports on the server. When a client requests for a temporary communication session, the server assigns a dynamic port to the client. The port is valid only for a short duration and can become available for reuse when the previous session expires.

Server-to-device communication

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

Protocol	MVE server	Device	Used for
Network Printing Alliance Protocol (NPAP)	UDP 9187	UDP 9300	Communicating with Lexmark network printers
XML Network Transport (XMLNT)	UDP 9187	UDP 6000	Communicating with some Lexmark network printers
Lexmark Secure Transport (LST)	UDP 6100 Ephemeral Transmission Control Protocol (TCP) port (handshaking)	UDP 6100 TCP 6110 (handshaking)	Communicating securely with some Lexmark network printers
Multicast Domain Name System (mDNS)	Ephemeral User Datagram Protocol (UDP) port	UDP 5353	Discovering certain Lexmark network printers and determining the security capabilities of devices
Simple Network Management Protocol (SNMP)	Ephemeral UDP port	UDP 161	Discovering and communicating with Lexmark and third-party network printers
File Transfer Protocol (FTP)	Ephemeral TCP port	TCP 21 TCP 20	Deploying generic files
Trivial File Transfer Protocol (TFTP)	Ephemeral UDP port	UDP 69	Updating firmware and deploying generic files
Hypertext Transfer Protocol (HTTP)	Ephemeral TCP port	TCP 80	Deploying generic or configuration files
		TCP 443	Deploying generic or configuration files
Hypertext Transfer Protocol over SSL (HTTPS)	Ephemeral TCP port	TCP 161 TCP 443	Deploying generic or configuration files
RAW	Ephemeral TCP port	TCP 9100	Deploying generic or configuration files

Device-to-server communication

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

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

Server-to-database communication

Ports used during communication from the MVE server to databases

MVE server	Database	Used for
Ephemeral TCP port	TCP 1433 (SQL Server) Users can configure the default port	Communicating with an SQL Server database
Ephemeral TCP port	TCP 3050	Communicating with a Firebird database

Client-to-server communication

Port and protocol used during communication from the flex or browser client to the MVE server

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

Messaging and alerts

Port and protocol used during communication from the MVE server to a mail server

Protocol	MVE server	SMTP server	Used for
Simple Mail Transfer Protocol (SMTP)	Ephemeral TCP port	TCP 25 Users can configure the default port	Providing the e-mail functionality used to receive alerts from devices

MVE-server-to-LDAP-server communication

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

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

Accessing MVE

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

For Kerberos authentication, you can access MVE using a smart card. MVE uses Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO), which provides a mechanism for extending a Kerberos-based single sign-on environment to web applications. To enable Kerberos authentication in MVE, see "Enabling Kerberos authentication" on page 19.

Kerberos authentication

Note: Before accessing MVE, make sure that your web browser supports SPNEGO authentication. For more information, see the online references for your web browser. For a list of supported web browsers, see the *Release Notes*.

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

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

LDAP or local accounts

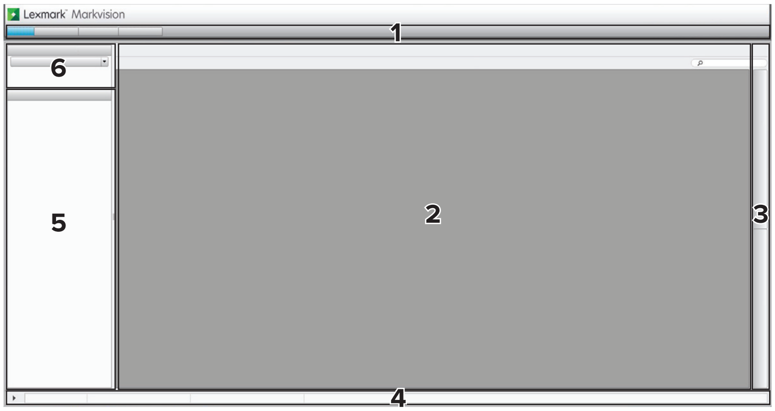
Note: If MVE is idle for more than 30 minutes, then the user is logged out automatically.

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

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

   Note: For initial setup, use the login credentials that you created during the MVE installation.

Understanding the home screen



Use this area		To
1	Header	Access the four key area tabs and perform other administrative tasks.
2	Search Results	View the list of printers matching the currently selected bookmark or search.
3	Toolbar	Access the tools for performing tasks such as creating discovery profiles, configurations, and events, depending on the selected area tab.
4	Task Information	View the status of the most recent activity.
5	Search Results Summary	View a categorized summary of the currently selected bookmark or search.
6	Bookmarks and Advanced Search	Manage and select bookmarks, and refine search queries.

Setting up user access

Managing users

1. From the Header area, click 🔧 > **User**.
2. Do either of the following:
   - To add a user, click ✚, and then enter the user credentials.
   - To edit a user, click ✎, and then if necessary, modify the user credentials.
3. From the Roles section, assign the user to one or more roles.
   - **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.
4. Click **OK**.

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

Enabling LDAP server authentication

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

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

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

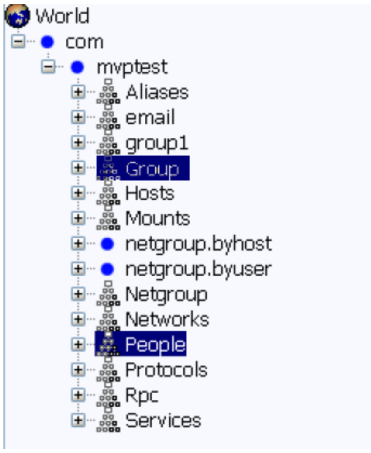
As a prerequisite, the LDAP server must contain user groups that correspond to the required user roles. For more information, see “Managing users” on page 14.

1. From the Header area, click 🔧 > **LDAP** > **Enable LDAP for Authentication**.
2. From the Connection section, configure the following:
   - **Server**—Type the IP address or the host name of the LDAP server where the authentication occurs. If you want to use encrypted communication between the MVE server and the LDAP server, then do the following:
     a. Use the fully qualified domain name (FQDN) of the server host.
     b. Access the network host file, and then create an entry to map the server host name to its IP address.

Notes:

- In a UNIX or Linux operating system, the network host file is typically found at **`/etc/hosts`**.
- In a Windows operating system, the network host file is typically found at **`%SystemRoot%\system32\drivers\etc`**.
- The TLS protocol requires the server host name to match the name of the “Issued To” host specified in the TLS certificate.

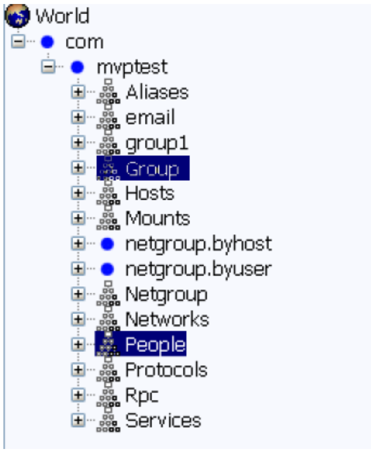
- **Port**—Enter the port number that the local computer uses to communicate with the LDAP community server. The default port number is 389.
- **Root DN**—Type the base distinguished name (DN) of the root node. In the LDAP community server hierarchy, this node should be the direct ancestor of the user node and group node. For example, **`dc=mvptest,dc=com`**.



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

3 Configure the search settings.

- **User Search Base**—Type the node in the LDAP community server where the user object exists. This node is under the Root DN where all the user nodes are listed. For example, **`ou=people`**.



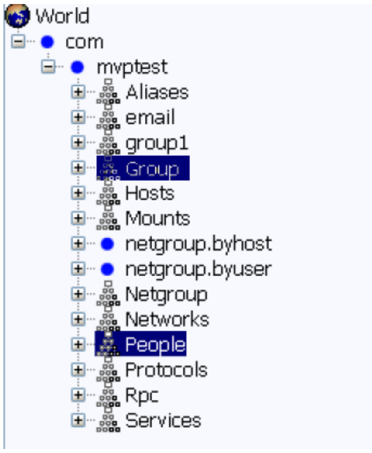
If the users are at multiple-directory hierarchical levels in the LDAP community server, then do the following:

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

b Include the configuration in the User Search Base field.

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

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



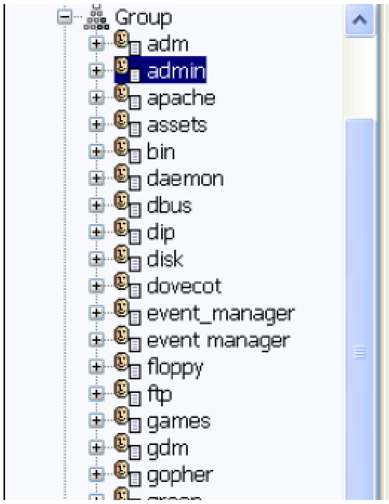
The User Search Filter function can accommodate multiple conditions and complex expressions.

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

Notes:

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

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

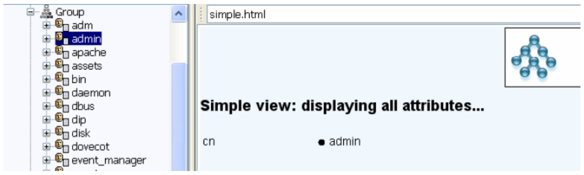


  Note: A search base consists of multiple attributes separated by commas, such as cn (common name), ou (organizational unit), o (organization), c (country), and dc (domain).

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

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

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



Simple view: displaying all attributes...

cn ● admin

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

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

- **Anonymous Bind**—If there is no LDAP configuration stored in MVE, then this option is selected by default. The MVE server does not produce its identity or credentials to the LDAP server to use the LDAP server lookup facility. The follow-up LDAP lookup session uses only unencrypted communication.
- **Simple Bind**—Uses unencrypted communication between the MVE server and the LDAP server. If you want the MVE server to use the LDAP server lookup facility, then do the following:
  - **a** In the Bind DN field, type the bind DN.
  - **b** Type the Bind Password, and then confirm the password.

    Note: The Bind Password depends on the Bind User settings in the LDAP server. If the Bind User is set as **Non-Empty**, then a Bind Password is required. If the Bind User is set as **Empty**, then a Bind Password is not required. For more information, contact your LDAP administrator.

- **TLS**—Uses encrypted communication between the MVE server and the LDAP server. The MVE server fully authenticates itself to the LDAP server using the MVE server identity (Bind DN) and credentials (Bind Password).

  For self-signed certificates, the TLS fingerprint must be made available to the system-wide Java Virtual Machine keystore named **`cacerts`**. This keystore exists in the ***`[mve.home]`*****`/jre/lib/security`** folder, where ***`[mve.home]`*** is the installation folder of MVE. To configure the settings, do the following:

  a In the Bind DN field, type the bind DN.

  b Type the Bind Password, and then confirm the password.

  Note: The Bind Password is required.

- **Kerberos**—Uses encrypted communication between the MVE server and the LDAP server. The Kerberos security protocol is supported only in an Active Directory that has GSSAPI implementation. For more information, see the documentation for Kerberos. To configure the settings, do the following:

  a In the Kerberos Config File field, browse to the krb5.conf file.
  Sample configuration:

  ```
  [libdefaults]
      default_realm=ABC.COM

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

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

  b In the Encryption Method menu, select whether to use SSL encryption.

  c In the KDC Username field, type the Key Distribution Center (KDC) name.

  d Type the KDC password, and then confirm the password.

  Note: If you want to enable Kerberos Authentication, then see “Enabling Kerberos authentication” on page 19.

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

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

Notes:

- MVE automatically maps the specified LDAP group to its corresponding MVE role.
- You can assign one LDAP group to multiple MVE roles, and you may also type more than one LDAP group in a role field.
- When typing multiple LDAP groups in the role fields, use the vertical bar character (**|**) to separate multiple LDAP groups. For example, if you want to include the **`admin`** and **`assets`** groups for the Admin role, then type **`admin|assets`** in the Admin field.
- If you want to use only the Admin role and not the other MVE roles, then leave the fields blank.

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

Enabling Kerberos authentication

Before you begin, make sure that:

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

1. From the Header area, click 🔧 > **LDAP** > **Enable LDAP for Authentication**.
2. From the Binding Information section, select **Kerberos** > **Enable Kerberos Authentication**.
3. Configure the following:
   - **Service Principal Name**—Type the service principal name for the MVE server.
   - **Keytab**—Browse to the keytab file.
4. Configure the Role Mapping settings. For more information, see step 5 of “Enabling LDAP server authentication” on page 14.

   Note: Make sure that the specified MVE roles match the existing groups set up in the Active Directory server.
5. Click **Apply** > **Close**.

Managing assets

Discovering devices

To add devices to the system, you can either use a discovery profile or import a list of devices using a comma-separated values (CSV) file.

A discovery profile lets you find devices using network parameters and add them to the system. In a discovery profile, you can do the following:

- Include or exclude a list or range of IP addresses during discovery. If you have a list of IP addresses from an external system, then you can import them directly to the system using a CSV file.
- Configure the SNMP settings for communicating to the devices during discovery. Make sure that SNMP is enabled in the devices.
- Adjust the connection settings based on your network performance.
- Include secured devices during the discovery.
- Assign and enforce a configuration automatically to a compatible printer model found during discovery.

Adding or editing a discovery profile

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

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

     Notes:

     – You can type only one entry at a time.
     – When typing IP address ranges, do not use wildcard characters.
   - Click ➡, and then browse to the CSV file.
     The file can contain a list of device IP addresses or host names. To view examples of valid formats, mouse over the text field.
4. From the SNMP tab, select **Version 1,2c** or **Version 3**, and then set the access permissions.

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

- **Include secured printers in the discovery**—Include secured devices when executing the discovery profile. If you do not have a secured device, then do not select this option to avoid performance issues during discovery. For more information on secured devices, see “Understanding secured devices” on page 34.
- **Automatically manage discovered devices**—Set newly discovered devices to a Managed state automatically during discovery. By default, this option is selected in new discovery profiles. If auto-configuration is set, then this option cannot be modified. If this option is not selected, then the discovered devices are set to a New state.

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

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

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

7 Click **Save**.

Notes:

- Clicking ▶ executes the discovery profile but does not save it.
- A new discovery profile collects basic information to identify a device. To collect the complete information from a device, set it to **Managed**, and then perform an audit. For more information, see “Managing devices” on page 23.
- To make sure that the device information is current, schedule a regular discovery. For more information, see “Scheduling tasks” on page 47.

Cloning a discovery profile

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

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

2 Click ⧉.

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

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

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

  Notes:

  – You can type only one entry at a time.

  – When typing IP address ranges, do not use wildcard characters.

- Click ⇥, and then browse to the CSV file.

  The file can contain a list of device IP addresses or host names. To view examples of valid formats, mouse over the text field.

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

5 Click **Save**.

Notes:

- Clicking ▶ executes the discovery profile but does not save it.
- A new discovery profile collects basic information to identify a device. To collect the complete information from a device, set it to **Managed**, and then perform an audit. For more information, see “Managing devices” on page 23.
- To make sure that the device information is current, schedule a regular discovery. For more information, see “Scheduling tasks” on page 47.

Importing devices from a file

Use a CSV file to import devices.

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

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

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

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

3. If you are using SNMP V3 protocol to communicate with the device, then select the following columns:

   - **SNMP V3 Read/Write User**
   - **SNMP V3 Read/Write Password**
   - **SNMP V3 Minimum Authentication Level**
   - **SNMP V3 Authentication Hash**
   - **SNMP V3 Privacy Algorithm**

   Note: In the CSV file, make sure that the following parameters contain one of the following values:

   - Minimum Authentication Level
     - `NO_AUTHENTICATION_NO_PRIVACY`
     - `AUTHENTICATION_NO_PRIVACY`
     - `AUTHENTICATION_PRIVACY`
   - Authentication Hash
     - `MD5`
     - `SHA1`
   - Privacy Algorithm
     - `DES`
     - `AES_128`

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

4. Click **Add** to move the selected columns into the CSV File Columns section.

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

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

6. Select whether the imported devices should be automatically set to **Managed**. For more information, see “Managing devices” on page 23.
7. Click **OK**.

Managing devices

You can assign a device to the following life cycle states:

- **Managed**—Includes the device in all activities that can be performed in the system.
  - **Managed (Normal)**—The device is in its steady state.
  - **Managed (Changed)**—The physical properties of the device have been changed since the last audit. If the system communicates with the device and its physical properties are unchanged, then the device reverts to a Managed (Normal) state.
  - **Managed (Missing)**—The system cannot communicate with the device. If the system communicates with the device successfully in the next attempt, then the device changes to a Managed (Found) state.
  - **Managed (Found)**—The device is previously missing, but is able to communicate with the system successfully in its recent attempt. If the system communicates with the device successfully in the next attempt, then the device reverts to a Managed (Normal) state.
- **Unmanaged**—Excludes the device from all activities performed in the system.
- **Retired**—The device is previously in a 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

Note: Before performing any tasks on a device, make sure that the device is set to **Managed**.

1. From the Assets tab, in the Bookmarks and Searches menu, select **New Printers**.
2. Select one or more devices.
3. From the Set State To 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, in the Bookmarks and Searches menu, select **Managed Printers**.
2. From the All Printers section, select the IP address of the device.

   Note: If you do not know the IP address of the device, then locate the device under the System Name column.
3. From the Asset Properties dialog box, view the following:
   - **Identification**—Device network identification information.
   - **Dates**—List of device events. This list includes the date added to the system, discovery date, and the most recent audit date.
   - **Firmware**—Device firmware code levels.
   - **Capabilities**—Device features.
   - **Supplies**—Device supply capacity and other details.
   - **Options**—Information about the device options, such as the device hard disk and its remaining free space.

- **Input Options**—Settings for the available paper trays and other device inputs.
- **Output Options**—Settings for the available paper bin.
- **eSF Applications**—Information about the installed eSF applications on the device, such as version number and status.
- **Device Statistics**—Specific values for each of the device properties.
- **Change Details**—Information about the changes in the device.

  Note: This feature applies only to devices that are in a Managed (Changed) state.
- **Device Credentials**—Credentials used in a configuration.

  Note: To manage the security settings, see “Managing security settings” on page 35.

Locating and organizing devices within the system

Searching for devices within the system

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

Default bookmarks

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

- **All Printers**—All devices in the system.
- **Managed Printers**—Active devices in the system. Devices that appear when selecting this bookmark can be in any of the following states:
  - Managed (Normal)
  - Managed (Changed)
  - Managed (Missing)
  - Managed (Found)
- **Managed (Changed) Printers**—Active devices in the system whose properties have changed since the last audit.
- **Managed (Found) Printers**—Devices that are reported as missing from previous search queries, but have now been found.
- **Managed (Missing) Printers**—Devices that the system was unable to communicate with.
- **Managed (Normal) Printers**—Active devices in the system whose properties have remained the same since the last audit.
- **New Printers**—Devices that were newly discovered and were not set to a Managed state automatically.
- **Retired Printers**—Devices that are no longer active in the system.
- **Unmanaged Printers**—Devices that have been marked for exclusion from activities performed in the system.

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

To create a bookmark for your refined search, click 🔖.

Custom bookmarks

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

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

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

Note: For more information, see "Understanding search criteria settings" on page 27.

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

Advanced search

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

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

2 Modify the search criteria settings.

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

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

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

Note: For more information, see "Understanding search criteria settings" on page 27.

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

The located devices appear in the Search Results area.

Understanding search criteria settings

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

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

Use	To
Firmware Version	Specify the device firmware version.
Firmware:AIO	Specify the AIO value of the device firmware.
Firmware:Base	Specify the base version of the device firmware.
Firmware:Engine	Specify the engine value of the device firmware.
Firmware:Fax	Specify the fax value of the device firmware
Firmware:Font	Specify the font value of the device firmware.
Firmware:Kernel	Specify the kernel value of the device firmware.
Firmware:Loader	Specify the loader value of the device firmware.
Firmware:Network	Specify the network value of the device firmware.
Firmware:Network Driver	Specify the network driver value of the device firmware.
Firmware:Panel	Specify the panel version of the device firmware.
Firmware:Scanner	Specify the scanner version of the device firmware.
Hostname	Specify the device host name.
IP Address	Specify the device IP address. **Note:** You can use an asterisk in the last three octets to search for multiple entries. For example, `123.123.123.*`, `123.123.*.*`, and `123.*.*.*`.
Keyword	Specify the assigned keywords, if any.
Lifetime Page Count	Specify the lifetime page count value of the device.
MAC Address	Specify the device MAC address.
Maintenance Counter	Specify the value of the device maintenance counter.
Manufacturer	Specify the device manufacturer name.
Marking Technology	Specify the marking technology that the device supports.
MFP Capability	Specify whether the device is a multifunction product (MFP).
Model	Specify the device model name.
Printer Status	Specify the device status. For example, `Ready`, `Paper Jam`, `Tray 1 Missing`.
Profile Capability	Specify whether the device supports profiles.
Receive Fax Capability	Specify whether the device supports receiving fax.
Scan to E-mail Capability	Specify whether the device supports Scan to E-mail.
Scan to Fax Capability	Specify whether the device supports Scan to Fax.
Scan to Network Capability	Specify whether the device supports Scan to Network.
Serial Number	Specify the device serial number.
State	Specify the current device state in the database.
Supply Status	Specify the device supplies status.
System Name	Specify the device system name.

Use the following operators when searching for devices:

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

Using categories and keywords

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

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

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

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

Adding, editing, or deleting categories

1. From the Assets tab, click **Keywords**.
2. From the Category pane, do one of the following:

   ### Add a category

   a. Click ✚.
   b. Type a name for the category.
   c. Press **Enter**.

   ### Edit a category

   a. Select the category, and then click ✎.
   b. Modify the name of the category.
   c. Press **Enter**.

   ### Delete a category

   a. Select the category, and then click —.
   b. Click **Yes**.

Note: Deleting a category also deletes and removes the keywords from the devices to which they are assigned.

Adding, editing, or deleting keywords

1 From the Assets tab, click **Keywords**.

2 From the Keywords pane, do one of the following:

Add a keyword

a From the Category pane, select a category where the keyword belongs.

b From the Keyword pane, click ✚.

c Type a name for the keyword.

d Press **Enter**.

Edit a keyword

a Select the keyword, and then click ✎.

b Edit the name.

c Press **Enter**.

Delete a keyword

a Select the 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 From the Assets tab, click **Keywords**, and then select a keyword.

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

2 Select one or more devices where you want to assign the keyword.

3 Click +📌.

Notes:

- When the task is complete, a confirmation appears in the Task Information area.
- To check the keywords assigned to the device, view the device properties.

Removing assigned keywords from a device

1 From the Assets tab, select the device from which you want to remove keywords.

2 Click **Keywords** > −📌, and then select the keyword that you want to remove.

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

3 Click **OK**.

Managing configurations

Creating a configuration

Note: You can manage the security settings only when creating a configuration from a selected device. For more information, see "Creating a configuration from a device" on page 31.

1. From the Configurations tab, click **Configurations** > ✚, and then type a unique name for the configuration.
2. Select a printer model, and then click **OK**.
3. From the Device Settings tab, to filter the settings, do either of the following:
   - In the Type menu, select a setting category.
   - In the Filter field, type the setting name.
4. Select one or more settings, and then specify the values.

   In some settings, you can use variables to specify the values. To apply variable settings, do the following:

   a. From the Variable Setting Data File menu, select a file. If there are no existing files, then click **Import**, and then browse to the CSV file.

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

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

      Note: Tokens are case sensitive. For more information, see "Understanding variable settings" on page 33.

5. From the Firmware tab, select a transfer method, and then select a firmware file.

   To import a firmware file, see "Importing files to the library" on page 33.

   Note: If you select HTTPS and your printer supports only HTTP, then the application uses HTTP.

6. From the Solutions tab, select one or more solutions to deploy. For more information, see "Preparing solutions for enforcement" on page 36.
7. From the CA certificates tab, select one or more certificates to deploy.

   To import a certificate file, see "Importing files to the library" on page 33.

8. Click **Save**.

Creating a configuration from a device

Note: When you create a standalone configuration, you cannot modify its security settings. Creating a configuration from a selected device lets you modify the security settings. For more information, see "Managing security settings" on page 35.

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

3. Click **OK**.
4. Select the configuration, and then click ✎.
5. From the Device Settings tab, modify the settings or apply variable settings. For more information, see step 4 of “Creating a configuration” on page 31.

   Note: When you clone a configuration, all the settings are selected by default. MVE evaluates each selected setting and enforces them to the devices. To avoid performance issues, we recommend selecting only the settings that are necessary. You can use filters to find the settings that you want to modify.
6. From the Security tab, manage the security settings available for your device.

   Note: Some security settings may not be available, depending on your printer model.
7. If necessary, modify the firmware, solution, and CA certificate deployment settings.
8. Click **Save**.

Notes:

- Before enforcing the cloned configuration to other devices, make sure that the host name setting is disabled. You can use variable settings to assign a unique host name to a device. For more information, see “Understanding variable settings” on page 33.
- Configurations that appear in red text and begin with an exclamation point contain one or more invalid settings, and cannot be enforced on a device.

Assigning a configuration

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

   Note: To remove an assigned configuration from a device, 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.

Exporting or importing a configuration

1. From the Configurations tab, click **Configurations**.
2. Do either of the following:
   - To export a configuration file, select a configuration, click ⇨, and then click **Download**.
   - To import a configuration file, click ⇨, browse to the configuration file, and then click **Send**.

   Note: Only one of the passwords in a configuration is exported, and the password is encrypted. When you import the configuration, the password is not included. You can add the password manually in the configuration settings after importing.

Importing files to the library

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

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

   Notes:

   - Only .fls, .zip, and .pem files can be imported. An engine code file is not supported.
   - To view certificates and licenses, click **Properties**.

Understanding variable settings

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

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

Sample CSV format:

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

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

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

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

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

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

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

You can import the CSV file containing variable settings when creating or editing a configuration. For more information, see “Creating a configuration” on page 31 or “Editing a configuration” on page 32.

Understanding secured devices

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

		Fully unrestricted	Fully restricted
Device settings	Remote Management permission or Remote Management Function Access Control (RM FAC) **Note:** For a list of devices that support security settings, see the *Release Notes*.	No authentication or no security	An authentication method is configured to restrict public access to the Remote Management and Security Menu permissions, or a security template is assigned to RM FAC.
	Significant ports	The following ports are open: • UDP 161 (SNMP) • UDP 9300/9301/9302 (NPAP)	The UDP 161 (SNMP) port is open.
	Security-related ports	The following ports are open: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)	The following ports are open: • UDP 5353 (mDNS) • TCP 6110 • TCP/UDP 6100 (LST)

		Fully unrestricted	Fully restricted
MVE settings	Discovery profile	The **Include secured printers in the discovery** option is cleared.	The **Include secured printers in the discovery** option is selected.
	Are secure channels used for communication between MVE and the network devices?	No **Note:** In some printer models, secure channels are used even on fully unrestricted devices.	Yes
	How do I determine the security configuration of the devices in my network?	In the main data grid in MVE, an *open* padlock icon appears beside the IP address of a fully unrestricted device.	In the main data grid in MVE, a *closed* padlock icon appears beside the IP address of a fully restricted device. **Note:** If MVE cannot identify the communication credentials of the device, then the closed padlock icon has a red slash through it. To remove the red slash, set the correct communication credentials for the security settings in the configuration before enforcing it to the restricted device.
	How do I search for devices that have this type of configuration?	1 From the “Bookmarks and Advanced Search” area, select **All Printers**. 2 From the Search Results Summary area, scroll down to the Communications category, and then select **Unsecured**.	1 From the “Bookmarks and Advanced Search” area, select **All Printers**. 2 From the Search Results Summary area, scroll down to the Communications category, and then select **Secured**.

Managing security settings

Device settings

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

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

     ### Restrict public access

     a. From the Public section, click **Manage Permissions**.
     b. Expand **Administrative Menus** and **Device Management**, and then clear **Security Menu** and **Remote Management**.

c Click **Save**.

Allow authenticated access

a From the Local Accounts, Network Accounts, or Additional Login Methods section, click **Manage Group/Permissions** or **Manage Permissions** for the authentication method.

b Expand **Administrative Menus** and **Device Management**, and then select **Security Menu** and **Remote Management**.

c Click **Save**.

- Click **Security** > **Security Setup** > **Access Controls** > **Management**, assign a security template to Remote Management, and then click **Submit**.
- Click **Security** > **Edit Security Setups** > **Access Controls**, assign a security template to Remote Management, and then click **Submit**.

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

MVE settings

Notes:

- Make sure that "Include secured devices in the discovery" is enabled when you discover the device. For more information, see "Adding or editing a discovery profile" on page 20.
- Make sure that you have created a configuration from a device. For more information, see "Creating a configuration from a device" on page 31.

1 From the Configurations tab, edit a configuration.

2 From the Security tab, manage the security settings available for your device.

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

3 Click **Save**.

Preparing solutions for enforcement

Creating a solutions package

1 Export the device list from MVE using Data Export.

a From the Header area, click .

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

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

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

d Click **Finalize Export**.

2 Access Package Builder.

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

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

b Import the device list.

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

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

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

3 Download the package.

Adding solutions to a configuration

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

1 Import the solution package downloaded from Package Builder. For more information, see "Importing files to the library" on page 33.

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 solution bundle, select the components that you want to include.
- Licenses are automatically retrieved from the imported solution 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, select the license type.

5 Apply the changes.

Checking conformance with a configuration

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

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

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

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

Performing service desk tasks

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.

Checking the status of a device

1. From the Service Desk tab, select one or more devices.
2. Click **Collect current status**.
3. From the Printer Status and Supply Status columns, note the icon beside the device.

Icon	Status
✓	**OK**—The device is ready and supplies are sufficient.
⚠	**Warning**—The device is working, but supplies are low or may require attention later.
✖	**Error**—The device or supplies need immediate attention.

Note: A current status collection task can be scheduled to occur regularly or at a predetermined time. For more information, see “Scheduling tasks” on page 47.

Working with a device

Viewing a device remotely

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

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

   Note: The picture of the device is available only in some printer models.

3. Click **Remote Operator Panel** > **Click here to continue**.
4. From the lower left side, see the keyboard key equivalent for each of the device button commands.

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

Viewing the embedded Web page

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

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

   Note: The picture of the device is available only in some printer models.

3. Click **Embedded Web Page**.

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

Rebooting devices

Note: You can reboot only one device at a time. In some printer models, a reboot failure report may appear in the task log even when the device is rebooted successfully.

1. From the Service Desk tab, select a device.
2. Click **Reboot Device**.

Managing device events

Use Event Manager to monitor and manage events or alerts in your printer fleet. Create an automated event and set a destination to notify yourself or other specified users when a particular incident occurs.

Note: Events or alerts are not supported on secured devices.

Creating a destination

A destination is a predefined action that can be either an e-mail notification or a command-line operation. The action is triggered when a device event occurs. For a command destination, MVE supports running an executable (.exe) file or a command interpreter (such as `echo` or `dir`).

1. From the Event Manager tab, click **Destinations** > ➕, and then type a unique name for the destination.
2. Select a destination type.

Command destination

a. Select **Command**, and then click **Next**.

b. In the Command Path (Required) field, type the name of an executable file or a command.

c. To add placeholders to the Command Parameters field, from the Place Holders list, select a placeholder, and then click ▶.

Note: You can add other parameters to be included in the command line.

d. Click **Finish**.

E-mail destination

Note: Make sure that the e-mail settings are configured. For more information, see “Configuring e-mail settings” on page 45.

a. Select **E-mail**, and then click **Next**.

b. Type the appropriate values in the 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 receiving a carbon copy of the e-mail.
- **Subject**—Type a subject title.
- **Body**—Type the default e-mail message.

Note: You can use the available placeholders as part of or as the entire subject title, or as part of an e-mail message. Placeholders represent the variable elements that are replaced with the actual values when used.

c. Click **Finish**.

Sample configuration for a command destination

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

Command path: **powershell.exe**

Command parameters: **-executionpolicy bypass -File “c:/Program Files (x86)/Lexmark/Markvision Enterprise/mve_alert.ps1” -IpAddress “${configurationItem.ipAddress}” -Alert “${alert.name}”**

Sample Windows PowerShell Script

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

Editing or deleting a destination

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

2 Do either of the following:

Edit a destination

a Select a destination, and then click ✎.

b If necessary, change the name, and then click **Next**.

c Modify the command parameters.

d Click **Finish**.

Delete a destination

a Select a destination, and then click —.

b Click **Yes**.

Creating an event

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

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

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

Note: You can select multiple or all alerts.

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

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

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

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

6 Click **Finish**.

Editing or deleting an event

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

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

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

Assigning an event to a device

1 From the Event Manager tab, select the check box beside the IP address of the device.

2 If necessary, click **Events** to show the active events.

3 Select an event, and then click +📌.

Removing an event from a device

1 From the Event Manager tab, select the check box beside the IP address of the device.

2 If necessary, click **Events** to show the active events.

3 Select an event, and then click −📌.

Displaying event details

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

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

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

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

3. Click **Properties**.

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

Performing other administrative tasks

Deploying generic files

Use Generic File Download to deploy configuration files or other solutions that are not included in a solution package to one or more devices. This feature allows instant distribution of various file types, such as universal configuration (UCF) files and firmware (.fls) files, to any devices that the application manages.

Note: Make sure that the printer security settings are configured to allow communication with the MVE server. For more information, see “Managing security settings” on page 35.

1 From the Header area, click ⬇.

2 From the Include Printers menu, select an available bookmark.

3 From the Destination menu, select one of the following:

- **CA Certificate**—Deploy CA certificates to the printer.
- **Configuration File (HTTPS)**—Deploy a configuration file to the printer through HTTPS.
- **Firmware Update**—Deploy a firmware file to the printer.
- **Print (FTP)**—Send a printable file through an FTP network.
- **Print (raw socket)**—Send a printable file from the computer.
- **UCF Configuration (HTTP)**—Deploy a printer UCF configuration file through HTTP.
- **UCF Configuration (FTP)**—Deploy a network UCF configuration file through FTP. This feature works only in unsecured devices.

4 From the “Select the file” section, browse to the file that you want to deploy, and then click **Send**.

5 Click **Download**.

Note: A generic file download task can be scheduled to occur regularly or at a predetermined time. For more information, see “Scheduling tasks” on page 47.

Configuring e-mail settings

Note: Enable the SMTP configuration to let MVE send data export files and event notifications through e-mail.

1 From the Header area, click 🔧 > **E-mail**.

2 Select **Enable SMTP Configuration**, and then enter the values in the following 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 e-mailing, then select **Login Required**, and then type the user credentials.

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 a login disclaimer

1. From the Header area, click 🔧 > **Disclaimer** > **Enable disclaimer prior to login**.
2. In the Disclaimer Text field, type the message that you want to appear before logging in to MVE.

   Note: You can type up to 4000 characters.
3. Click **Apply** > **Close**.

Enabling data sharing

Data sharing allows sending of anonymous supplies and page usage information to Lexmark. The shared data are handled in compliance with the Lexmark Privacy Statement. We recommend using this feature to help improve Lexmark products and services. For more information, contact your Lexmark representative.

1. From the Header area, click 🔧 > **Data Sharing**.
2. Enter the enrollment code, and then click **Verify**.

   Note: To get the enrollment code, contact your Lexmark representative.
3. Follow the instructions on the screen.

Generating reports

1. From the Header area, click 📊.
2. From the Include Printers menu, select a device group based on your previously bookmarked searches.
3. From the Report Type menu, select the type of data you want to view.

Select	To view
Lifecycle State - Summary	A summarized report of the life cycle states of the devices.
Printer Manufacturer - Summary	A summarized report of device manufacturers.
Printer Model - Summary	A summarized report of device model names and numbers.
Printer Capabilities - Summary	A summarized report of device capabilities.

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

4. From the Report Format menu, select **PDF** or **CSV**.
5. If you select PDF, then in the Title field, you can choose to customize the title of the report.
6. If applicable, from the Group menu, select a group.
7. Click **Generate**.

Scheduling tasks

1. From the Header area, click 🕒.
2. Add a scheduled event.

Audit

a. From the Add menu, select **Audit**.
b. Select a bookmark, and then click **Next**.
c. Type a name for the scheduled event, and then specify the schedule information.
d. Click **Finish**.

Conformance

a. From the Add menu, select **Conformance**.
b. Select a bookmark, and then click **Next**.
c. Type a name for the scheduled event, and then specify the schedule information.
d. Click **Finish**.

Current Status

a From the Add menu, select **Current Status**.

b Select a bookmark, and then type a command path.

By default, MVE adds the printer IP address, host name, serial number, status, status severity, and status type parameters to the command. For example, a command path contains the following line:

`echo %* >><dir>\PrinterStatus.txt`, where ***`<dir>`*** is the location of the specified file.

When the command executes, the PrinterStatus.txt file is created or updated with the following sample parameters:

`10.195.1.255 MyPrinter 123ABC456DEF "*** Tray 3 Low ***" Warning Printer`.

Notes:

- The command is triggered only when a printer is not in a ready state.
- Make sure that you have the appropriate permissions to access the file.
- You can also log the event in Windows Event Viewer. For more information, go to the Microsoft website.

c Click **Next**.

d Type a name for the scheduled event, and then specify the schedule information.

e Click **Finish**.

Data Export

Note: Make sure that the e-mail settings are configured. For more information, see "Configuring e-mail settings" on page 45.

a From the Add menu, select **Data Export**.

b Select a bookmark, and then from the Data Export Template menu, select a template.

c In the E-mail Distribution List field, type the e-mail address where you want to send the exported file.

d Click **Next**.

e Type a name for the scheduled event, and then specify the schedule information.

f Click **Finish**.

Discover

a From the Add menu, select **Discover**.

b Select a discovery profile, and then click **Next**.

c Type a name for the scheduled event, and then specify the schedule information.

d Click **Finish**.

Enforcement

a From the Add menu, select **Enforcement**.

b Select a bookmark, and then click **Next**.

c Type a name for the scheduled event, and then specify the schedule information.

d Click **Finish**.

Generic File Download

a. From the Add menu, select **Generic File Download**.
b. Select a bookmark, and then from the Destination menu, select the deployment option.
c. From the “Select a file” section, browse to the file that you want to deploy, and then click **Send**.
d. Click **Next**.
e. Type a name for the scheduled event, and then specify the schedule information.
f. Click **Finish**.

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

Use Data Export to create a CSV file that contains data for managed devices. The exported data is generated from the last successful audit of the device.

Note: Only Admin and Asset users can use this feature.

1. From the Header area, click 🛢.
2. From the Include Printers menu, select a bookmark.
3. From the Possible Fields section, select the columns that you want for your exported file.
4. To move the selected columns into the Export Fields section, select **Add**.
5. To include a header in your CSV file, select **Add first row header**.

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

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

Note: A data export task can be scheduled to occur regularly or at a predetermined time. For more information, see “Scheduling tasks” on page 47.

Frequently asked questions

What devices does the application support?

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.

Can other users access my bookmarks?

Yes. Any user can access bookmarks.

Where can I find the log files?

You can find the installation log files that have the following formats in the **%TEMP%** directory:

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

You can find the application log files that have the ***.log** format in the following directory:

`<INSTALL_DIR>\tomcat\logs`, where `<INSTALL_DIR>` is the installation folder of MVE.

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

A host name is a unique name assigned to a 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. MVE picks up the printer host name from the DNS table by its IP address.

Troubleshooting

User has forgotten the password

Reset the user password

You need administrative privileges to reset the password.

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.

Cannot discover a network device

Try one or more of the following:

Make sure that the printer is turned on

Make sure that the power cord is securely plugged into the printer and into a properly grounded electrical outlet

Make sure that the print server is connected to the network

Restart the printer and the print server

Print a setup page for the printer and make sure that the print server appears on the list of attachments

Make sure that TCP/IP is activated on the print server

For more information, see your print server documentation.

Make sure that the device name on the application matches the device name set on the print server

1. From the Search Results area, locate the IP address of the printer.
2. Note the application device name that appears beside its IP address.
3. Check the device name set in the print server.

Incorrect device information

Perform an audit on the device

For more information, see "Auditing a device" on page 23.

Notices

Edition notice

July 2016

The following paragraph does not apply to any country where such provisions are inconsistent with local law: LEXMARK INTERNATIONAL, INC., PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in later editions. Improvements or changes in the products or the programs described may be made at any time.

References in this publication to products, programs, or services do not imply that the manufacturer intends to make these available in all countries in which it operates. Any reference to a product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any existing intellectual property right may be used instead. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by the manufacturer, are the user’s responsibility.

For Lexmark technical support, visit **http://support.lexmark.com**.

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

Trademarks

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

Firebird is a registered trademark of the Firebird Foundation.

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

All other trademarks are the property of their respective owners.

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

JmDNS License

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.

Index

A

adding a discovery profile 20
adding a login disclaimer 46
adding solutions to a configuration 37
adding users 14
advanced search 26
application log files
  locating 51
assigning a configuration 32
assigning an event to a device 43
assigning keywords to a device 30
audit data
  exporting 49
auditing a device 23

B

backing up Firebird database 8
bookmark search criteria 27
Bookmarks and Advanced Searches area 13

C

cannot discover a network device 52
categories
  adding 29
  deleting 29
  editing 29
  using 29
changing passwords 51
checking conformance with a configuration 37
checking device conformance with a configuration 39
checking device status 39
cloning a configuration 31
cloning a discovery profile 21
command destination 41
configuration
  assigning 32
  checking conformance 37
  checking device
    conformance 39
  creating 31
  creating from a device 31
  editing 32
  enforcing 37, 39
  exporting or importing 33
configuring e-mail settings 45
configuring system settings 46
creating a configuration 31
creating a configuration from a device 31
creating a solutions package 36
creating an event 42
CSV
  variable settings 33
custom bookmarks 26

D

data sharing
  enabling 46
default bookmarks 26
definition of terms 5
deleting a destination 42
deleting an event 43
deploying generic files 45
destination
  creating 41
  deleting 42
  editing 42
device
  assigning an event 43
  assigning keywords 30
  auditing 23
  checking status 39
  displaying event details 44
  importing from a file 22
  removing an event 43
  removing assigned
    keywords 30
  viewing properties 24
  viewing remotely 39
device life cycle state
  Managed 23
  Managed (Changed) 23
  Managed (Found) 23
  Managed (Missing) 23
  Managed (Normal) 23
  Retired 23
  setting 23
  Unmanaged 23
device state
  setting 23
device status
  checking 39
device, alerts
  receiving 46
device, host name
  acquiring 46
devices
  discovering 20
  rebooting 40
  searching for 26
disclaimer
  enabling 46
discovering devices 20
discovery profile
  adding or editing 20
  cloning 21
displaying event details 44

E

editing a configuration 32
editing a destination 42
editing a discovery profile 20
editing an event 43
editing users 14
embedded Web page
  viewing 40
enabling data sharing 46
enabling Kerberos authentication 19
enabling LDAP server authentication 14
enforcing a configuration 37
enforcing configuration 39
event
  creating 42
  deleting 43
  displaying details 44
  editing 43
  removing from a device 43
exporting a configuration 33
exporting audit data
  device 49
exporting CSV
  variable settings 33
exporting or importing a configuration 33

e-mail
  configuring settings 45
e-mail destination 41

F
files
  deploying 45
  importing to the library 33
Firebird database
  backing up 8
  restoring 8
forgotten user password 52

G
General tab
  using 46
generating reports 46
getting started
  home screen 13

H
Header area 13
home screen
  understanding 13
host name lookup
  reverse lookup 51

I
importing a configuration 33
importing CSV
  variable settings 33
importing devices from a file 22
importing files to the library 33
incorrect device information 53
installer log files
  locating 51
installing MVE 7

K
Kerberos authentication 19
keywords
  adding 30
  assigning to a device 30
  deleting 30
  editing 30
  removing from a device 30
  using 29

L
LDAP server
  enabling authentication 14
library
  importing files to 33
log files
  locating 51

M
managing security settings 35
managing users 14
MVE
  accessing 12
  installing 7
  upgrading to latest version 7

O
overview 5

P
password
  resetting 52
passwords
  changing 51
placeholders 41
ports
  understanding 9
Printer Status 39
properties of the device
  viewing 24
protocols
  understanding 9

R
rebooting devices 40
receiving alerts from devices 46
removing an event from a device 43
removing assigned keywords from a device 30
removing configuration from a device 32
reports
  generating 46
resetting user password 52
restoring Firebird database 8
reverse DNS lookup 51

S
scheduled event
  adding 47
scheduling tasks 47
search criteria 27
search criteria settings
  understanding 27
Search Results area 13
Search Results Summary area 13
searching for devices 26
secured devices
  understanding 34
security settings
  managing 35
solutions
  adding to a configuration 37
solutions package
  creating 36
Supply Status 39
supported devices 51
supported models list 51
system log
  viewing 49
system settings
  configuring 46

T
Task Information area 13
tasks
  scheduling 47
Toolbar area 13
troubleshooting
  cannot discover a network device 52
  incorrect device information 53
  user has forgotten the password 52

U
understanding secured devices 34
understanding the home screen 13
upgrading to the latest version of MVE 7
users
  adding 14
  assigning roles 14
  editing 14
  managing 14
using categories 29

using keywords 29

V

variable settings
  understanding 33
viewing a device remotely 39
viewing device properties 24
viewing the embedded Web page 40
viewing the system log 49