



**MarkVision Professional 11.2.1**

**Release Notes**

October 2009

# CONTENTS

Overview.....	1
<b>OPERATING SYSTEM INFORMATION.....</b>	<b>1</b>
Supported Operating Systems.....	1
Supported Web Browsers.....	2
Java Virtual Machine Recommendations.....	2
Supported Database Management Systems.....	3
<b>SUPPORTED DEVICES.....</b>	<b>3</b>
<b>UPGRADING.....</b>	<b>7</b>
<b>NEW FEATURES.....</b>	<b>7</b>
<b>ISSUES ADDRESSED WITH MVP 11.2.1.....</b>	<b>9</b>
Incorporation of Plug-Ins.....	9
Correction of Previous Issues.....	11
<b>SETTINGS CHANGES AND CLARIFICATIONS.....</b>	<b>12</b>
<b>SUGGESTIONS AND RECOMMENDATIONS.....</b>	<b>14</b>
<b>KNOWN ISSUES.....</b>	<b>15</b>
Device Specific Issues.....	24
<b>UNSUPPORTED SETTINGS.....</b>	<b>29</b>
Displayed Settings Differences.....	32

This MarkVision™ Professional (MVP) 11.2.1 software release contains feature enhancements and functional improvements. This document describes these enhancements as well as current issues and their workarounds.

## OVERVIEW

This release of MVP provides support for the 2009 line of Lexmark printers. These devices provide significant new capabilities and MVP 11.2.1 incorporates corresponding management support for them. In addition, this release of MVP contains updated support for operating platforms, addresses previous issues, and rolls in plug-ins for previous versions. MVP 11.2.1 also provides a few new features.

## OPERATING SYSTEM INFORMATION

---

### SUPPORTED OPERATING SYSTEMS

MarkVision Professional 11.2.1, including all current functions except where otherwise specified, fully supports the following operating system environments and the associated hardware platforms.

Operating System	Platform
Windows 2008 Server (Enterprise Edition)	Intel (IA32)
Windows Vista Business	Intel (IA32)
Windows Vista Enterprise	Intel (IA32)
Windows 2003 Server R2 Service Pack 2 (SP2), 32-bit only	Intel (IA32)
Windows 2003 Server Service Pack 2 (SP2), 32-bit only	Intel (IA32)
Windows XP Service Pack 3 (SP3)	Intel (IA32)
Windows 2000 Service Pack 4 (SP4)	Intel (IA32)
Mac OS X 10.4x – 10.5x	Intel and PowerPC
IBM AIX 5.3	POWER and PowerPC
HP-UX 11i 11.11	PA-RISC 2.0
Red Hat Enterprise Linux (RHEL) ES 4	Intel (IA32)
Red Hat Enterprise Linux (RHEL) Client 5	Intel (IA32)
SUSE Linux Enterprise 10	Intel (IA32)
SUSE Linux Enterprise 11	Intel (IA32)
Sun Solaris 9	Sun SPARC and Ultra SPARC
Sun Solaris 10	Sun SPARC and Ultra SPARC

## SUPPORTED WEB BROWSERS

MarkVision Professional 11.2.1 supports the following Web browsers.

Operating System	Browser
Windows	Windows Internet Explorer 6.x or later and IE 7 (XP, 2003, and Vista), IE 8 (XP, 2003, and Vista)
IBM AIX	Mozilla 1.7
HP-UX 11i	Mozilla 1.7
Red Hat Enterprise Linux ES	Firefox 2.0 and above
SUSE Enterprise Linux	Firefox 2.0 and above
Sun Solaris Unix	Mozilla 1.7

In order to run the MarkVision Web client, users must first enable their Web browser to support Sun's Java Runtime Environment (JRE) by installing the Java plug-in. In Windows environments, the plug-in is provided, and the user is automatically prompted to install it the first time they run the Web client.

*\*Note – The standalone MarkVision client program does not require installation of the browser plug-in.*

## JAVA VIRTUAL MACHINE RECOMMENDATIONS

The following JVM levels are recommended for running MarkVision Professional 11.2.1.

Operating System	JVM Level
Windows	1.6.0_14-b08
Mac OS X	1.5.0_09
IBM AIX	5.0.0.250
HP-UX	1.6.0.04
Linux	1.6.0_14
Sun Solaris SPARC	1.6.0_14

*\*Note – Java 5 is currently used for AIX and Mac.*

## SUPPORTED DATABASE MANAGEMENT SYSTEMS

MarkVision Professional 11.2.1 supports the following database management systems. This applies only to tasks such as *Printer Inventory* and *Job Statistics* that supported export to external relational databases in previous versions of MVP.

### Windows

- Oracle (10g)
- Microsoft SQL Server (2005)
- Microsoft Access (2002, 2003)
- Comma-separated variable (CSV)

### UNIX

- Oracle (10g)
- Comma-separated variable (CSV)

*\*Note – The ‘Oracle’ database option is available only after the Oracle JDBC Driver plug-in has been installed.*

## SUPPORTED DEVICES

---

MarkVision Professional 11.2.1 supports the following devices.

*\*Note – The devices listed below have been tested with MarkVision Professional but are only a subset of the thousands of networked print devices MarkVision can discover and manage by means of the standard SNMP Printer Management Information Block. Note that actual support varies by device. Some devices expose more data than others and some report data fields in nonstandard locations.*

Supported Print Servers (Network Interface)	
Dell Wireless Printer Adapter 3300	MarkNet N2004fl-ST
Lexmark C750 Ethernet	MarkNet N2501e
Lexmark C910 Ethernet	MarkNet N4050e
Lexmark T520 Ethernet	MarkNet N7000e
Lexmark T520 SBE Ethernet	MarkNet N7002e
Lexmark T522 Ethernet	MarkNet N7020e
Lexmark T620 Ethernet	MarkNet N8020
Lexmark T622 Ethernet	MarkNet N8050
Lexmark W820 Ethernet	MarkNet Pro1
Lexmark X820 Ethernet	MarkNet Pro3
MarkNet N2000t	MarkNet S
MarkNet N2001e	MarkNet X2011
MarkNet N2002e	MarkNet X2030
MarkNet N2003fx-MTRJ	MarkNet X2031
MarkNet N2003fx-SC	MarkNet XI
MarkNet N2003fx-ST	MarkNet Xle
MarkNet N2004fl-MTRJ	MarkNet XL
MarkNet N2004fl-SC	

Supported Lexmark Devices	
Lexmark 4079 plus	Lexmark Optra SC
Lexmark 4600 MFP	Lexmark Optra Se
Lexmark C500n**	Lexmark Optra Se plus
Lexmark C510	Lexmark Optra T
Lexmark C520	Lexmark Optra W810
Lexmark C522	Lexmark T420
Lexmark C524	Lexmark T430
Lexmark C530	Lexmark T520
Lexmark C532	Lexmark T520 SBE
Lexmark C534	Lexmark T522
Lexmark C540	Lexmark T620
Lexmark C543	Lexmark T622
Lexmark C544	Lexmark T630
Lexmark C546	Lexmark T632
Lexmark C734	Lexmark T634
Lexmark C736	Lexmark T640
Lexmark C750	Lexmark T642
Lexmark C752	Lexmark T644
Lexmark C760	Lexmark T650
Lexmark C762	Lexmark T652
Lexmark C770	Lexmark T654
Lexmark C772	Lexmark T656
Lexmark C780n	Lexmark W812
Lexmark C782n	Lexmark W820
Lexmark C910	Lexmark W840
Lexmark C912	Lexmark W850
Lexmark C920	Lexmark X203n
Lexmark C935	Lexmark X204n
Lexmark E120	Lexmark X264dn
Lexmark E120n	Lexmark X340
Lexmark E230	Lexmark X340n
Lexmark E232	Lexmark X342n**
Lexmark E234	Lexmark X363dn
Lexmark E234n	Lexmark X364dn
Lexmark E238	Lexmark X364dw
Lexmark E240	Lexmark X422
Lexmark E240n	Lexmark X463de
Lexmark E250d**	Lexmark X464de
Lexmark E250dn**	Lexmark X466de
Lexmark E260d, dn	Lexmark X466dte
Lexmark E320	Lexmark X466dtwe
Lexmark E321	Lexmark X500 Series**
Lexmark E322	Lexmark X502
Lexmark E323	Lexmark X543
Lexmark E330	Lexmark X544
Lexmark E332n	Lexmark X546
Lexmark E340	Lexmark X560n
Lexmark E342n	Lexmark X642e
Lexmark E350d	Lexmark X644e
Lexmark E352dn	Lexmark X646e -- v1.1
Lexmark E360d, dn	Lexmark X646ef Lexmark 4600 MFP = T64x+4600

Lexmark E450dn	Lexmark X651de
Lexmark E460dn, dw	Lexmark X652de
Lexmark E462dtn	Lexmark X654de
Lexmark Forms Printer 2580	Lexmark X656de
Lexmark Forms Printer 2581	Lexmark X658de
Lexmark Forms Printer 2590	Lexmark X734de
Lexmark Forms Printer 2591	Lexmark X736de
Lexmark Optra	Lexmark X738de
Lexmark Optra C	Lexmark X772e Lexmark C772 + 4600
Lexmark Optra C710	Lexmark X830e
Lexmark Optra Color 40	Lexmark X832e
Lexmark Optra Color 45	Lexmark X850e
Lexmark Optra Color 1200	Lexmark X852e
Lexmark Optra E	Lexmark X854e -- v1.1
Lexmark Optra Ep	Lexmark X860de
Lexmark Optra K 1220	Lexmark X862de
Lexmark Optra M	Lexmark X864de
Lexmark Optra N	Lexmark X940e
Lexmark Optra Plus	Lexmark X945e
Lexmark Optra S	

*\*\*The Lexmark C500n, E250d, E250dn, X342n, and X500 devices provide very limited configuration and management information to host management software such as MarkVision. As a result, MarkVision support for these devices is extremely limited, consisting of the display of only a few pieces of information such as serial number and model name.*

<b>Supported (Other Manufacturer) Devices</b>	
Brother HL-1470N Series	Kyocera FS-3830N
Brother HL-1650 / 1670N Series	Kyocera FS-7000
Brother HL-1870N Series	Kyocera FS-9000
Brother HL-2460 Series	Kyocera FS-9100DN
Brother HL-5070N	Lenovo C8300N
Brother HL-6050D	Lenovo C8700DN
Brother MFC-8820DN	Lenovo LJ3900D
Canon GP 200D	Lenovo MC8300DN
Canon ImageCLASS C2100	Minolta Color PageWorks
Canon ImageRunner 330	Minolta PageWorks 20
Canon ImageRunner 400	Minolta Magicolor 7300
Canon ImageRunner 500	Minolta-QMS Magicolor 2200
Canon ImageRunner 600	Minolta-QMS Magicolor 3100
Canon ImageRunner 2800	NEC SuperScript 1800
Canon ImageRunner 5000i	Oki C5300
Dell Color Laser Printer 3100cn	Okidata C7350n
Dell Laser Printer 1700	QMS Magicolor 2
Dell Laser Printer 1700n	QMS Magicolor 6100
HP 2000 C	Ricoh Aficio 180
HP 2500 C	Ricoh Aficio 270
HP 4345 MFP	Ricoh Aficio 350/355
HP 8550 MFP	Ricoh Aficio 450/455
HP 8550GN	Ricoh Aficio 550
HP Business InkJet 2250TN	Ricoh Aficio 650
HP Color LaserJet 2840 AIO	Ricoh Aficio 750
HP Color LaserJet 3000 DN	Ricoh Aficio 850

HP Color LaserJet 3550N	Ricoh Aficio 1045
HP Color LaserJet 3600N	Ricoh Aficio CL3000
HP Color LaserJet 3700 DTN	Ricoh Aficio CL7000CMF
HP Color LaserJet 3800N	Ricoh AP3800C Series
HP Color LaserJet 4500	Samsung ML-2152W
HP Color LaserJet 4550 Series	Tektronix Phaser 350
HP Color LaserJet 4650 DTN	Tektronix Phaser 550
HP Color LaserJet 4700 DN	Tektronix Phaser 560
HP Color LaserJet 4730 MFP	Tektronix Phaser 740/750
HP Color LaserJet 5550 DTN	Tektronix Phaser 750DX
HP Color LaserJet 8500	Tektronix Phaser 780GN
HP Color LaserJet 9500	Tektronix Phaser 850
HP Color LaserJet 9500n	Xerox DocuColor 4CP
HP LaserJet 1320 NW	Xerox DocuColor 2006
HP LaserJet 2100 Series	Xerox Document Centre 220/230
HP LaserJet 2200	Xerox Document Centre 240 ST
HP LaserJet 2420 DN	Xerox Document Centre 265 ST
HP LaserJet 2430 TN	Xerox Document Centre 332
HP LaserJet 3300 MFP Series	Xerox Document Centre 340
HP LaserJet 4000 Series	Xerox Document Centre 440
HP LaserJet 4050 Series	Xerox DocuPrint 4512
HP LaserJet 4100 MFP Series	Xerox DocuPrint C55/C55mp
HP LaserJet 4250 DTN	Xerox DocuPrint N17
HP LaserJet 4350 DTN	Xerox DocuPrint N24
HP LaserJet 5000 Series	Xerox DocuPrint N32
HP LaserJet 5/5M	Xerox DocuPrint N40
HP LaserJet 5si	Xerox DocuPrint N2025
HP LaserJet 8000 Series	Xerox DocuPrint N2125
HP LaserJet 8100 Series	Xerox DocuPrint N2825
HP LaserJet 8150 Series	Xerox DocuPrint N3225
HP LaserJet 9000 Series	Xerox DocuPrint N4025
HP LaserJet 9050N	Xerox DocuPrint N4525DX
HP Mopier 320	Xerox DocuPrint NC60
IBM InfoPrint 20	Xerox Phaser 790
IBM InfoPrint 21	Xerox Phaser 860
IBM InfoPrint 1145 MFP	Xerox Phaser 1235
IBM InfoPrint 1145L MFP	Xerox Phaser 2135DT
IBM InfoPrint Color 8	Xerox Phaser 3400
IBM LaserPrinter 4039	Xerox Phaser 3450
IBM Network Printer 12	Xerox Phaser 3500
IBM Network Printer 17	Xerox Phaser 4500DX
Konica KL-3015	Xerox Phaser 5400
Kyocera FS-C50 16N	Xerox Phaser 6200
Kyocera FS-1700	Xerox Phaser 6250
Kyocera FS-1750	Xerox Phaser 7700DN
Kyocera FS-1800	Xerox Phaser 8200
Kyocera FS-3750	Xerox Phaser 8400DP
Kyocera FS-3800	Xerox WorkCentre Pro 32C
Kyocera FS-3820N	

*\*Note – The level of support in MarkVision for networked print devices varies widely depending on the settings exposed on the device via SNMP and/or other network management protocols. On some devices, vendors use non-standard locations for management information. As a result, MarkVision is not always able to report the information.*

## UPGRADING

---

The recommended process for upgrading from previous versions of MarkVision Professional is as follows.

For MarkVision 10.0 forward, install the new version directly over the old version. MarkVision will migrate any existing settings/configurations to the new version the next time it runs. Be aware, however, of back-version plug-ins that may not be supported in the new version, such as special product requests that are not part of the new release. To avoid data loss during the upgrade process, refer to [this](#) section of the Release Notes.

Before upgrading from a previous version, list any plug-ins installed on your system and compare them with the list of plug-ins folded into this release and the list of back-level plug-ins supported by this release. Contact your SE or technical support if you have plug-ins installed that are not included in this release.

## NEW FEATURES

---

The following new features and functionality enhancements have been added in MVP 11.2.1.

### **MVP Web Server Pages Available through HTTPS Connection**

MVP Web server pages (Messenger, server parameters, etc.) are now available on HTTPS port 8443 in addition to HTTP ports 9180 and 80. Users can now launch the HTTPS version while entering user credentials for Messenger or Web server pages.

Notes:

- When the user is entering credentials, the connection will not automatically switch to HTTPS. The user must manually type the HTTPS URL (<https://8443>) into the browser. This ensures that the entire session is encrypted rather than only the user credentials page. The HTTPS certificate currently being used is a self-signed certificate.
- Only browser-to-server connections are encrypted by HTTPS. MarkVision Web client runs in its normal un-encrypted mode even if it is launched from the HTTPS page. This is because MarkVision Web Client uses a separate means of communication (involving random ports) between client and server JVMs.
- For LDAP or Kerberos user accounts in MVP, the credentials forwarded by the MarkVision server to the LDAP or Kerberos server are not encrypted. Only the browser-to-server communication is encrypted. Users should use LDAP/SSL to ensure complete end-to-end security.

This feature is not available in AIX 5L. An SSL-secured connection to the MVP Web server requires the Sun JSSE package, which is not supported by the IBM-supplied JRE for AIX systems.

### **Disk Encryption**

The following disk encryption features have been added.

- Filter on devices with disk encryption enabled or disabled
- Report disk encryption (enabled/disabled) in custom tables

### **Additional Page Count Options**

*Color A3 Page Count* and *Mono A3 Page Count* options have been added for supported devices in the following areas.

- *View → Custom Tables*
- *View → Page Counts*
- *Features → Overview → Printers → Page Counts*

### **Collecting and Sending Page Counts in MVP Messenger**

Color and mono A4 and A3 page counts can now be collected and sent in MVP Messenger.

### **Device Policies Task Enhancements**

The *Device Policies* task can now override any current device fax shortcut numbers, regardless of how they were configured. Previously, sending MVP Device Policies with fax shortcut numbers only overrode a device's current fax shortcut numbers if the original device fax shortcut numbers were created using *Device Policies*. If the original device shortcut numbers were created using the operator panel and/or Web page, MVP Device Policies would not override them.

The *Device Policies-Conformance* task can now check for installed solutions and profile destinations. In addition, *MVP Custom Tables* can now import data on installed solutions and profile destinations.

## ISSUES ADDRESSED WITH MVP 11.2.1

### INCORPORATION OF PLUG-INS

The following plug-ins have been merged into MVP 11.2.1.

Plug-Ins Merged into MVP 11.2.1	
Plug-In Name	Description
Access_Controls_Fix	Enables the “Disabled” and “No Security” values to be edited and applied properly for <i>Access Control</i> in printer server policy.
Access_Controls_Fix_for_Device_Policy	Enables supported access controls to be applied successfully from both settings and device policy (printer server).
BuildingBlockGroupSupportInDevicePolicy v1.0	Adds LDAP Building Block Group Support in Device Policy.
DBConnection_Cleanup v1.1.mvp	Does the following: 1) Removes all earlier and stale connection instances. 2) Closes the pool and connection appropriately by clearing all warnings. 3) Performs new implementation with respect to connection validity checks.
DevicePolicy_AdvancedSecurity_OneStep_Fix v1.0	Resolves the issue for applying Advanced Security in three steps – i.e. first creating building blocks, then creating a security template, then using Access Control from device policy (print server). This fix also enables the “Disabled” and “No Security” values to be edited and applied properly for <i>Access Control</i> in printer server policy.
DevicePolicyConformance v1.1.mvp	Fixes conformance issues for certain settings such as embedded solutions and e-mail alert.
DevicePolicy_CopyContent_Fix v1.0.mvp	Fixes the issue that occurred in device policy when the Copy Content photo option was applied. MVP applied the “Printed Image” setting instead of displaying an “unsupported” error.
DevicePolicy_enableECM_Fix v1.0	Added send.enableECM in LexMarkNet0x0100Os2.
DevicePolicy_ImportExport_Fix v1.0	Fixes the issue in which device policies built out of composite settings such as tables would not import after being exported.
DisplayNameDuplicateEntryFix v1.0	Fixes the issue in which the display name appeared twice in the basic LDAP settings in print server device policy.
EmbeddedSolutions_LicenseUpdate_Fix v1.0	Fixes the license update issue.
ESF_Scheduling_Status_Fix	Fixes the issue in which the warning message for failing eSF schedules was not displayed in the message window.
HostnameDiscoveryStrategy_Correction v1.0.mvp	Built for an AIX system running Java 5 and MVP 11.2.
JobStatistics_RemoteMgmt_Issue_Fix v1.0.mvp	Fixes the issue in which a printer would go offline if Job Statistics was run using Schedule. File changed: ResourceManagement.java.
LST_Negotiate_Failure_Fix v1.0	Introduces renegotiation capability.
Macon_FunctionaccessFix	Correctly builds the FunctionAccess authentication method into MarkVision for the X620e, X632e, X752e, X762e, X820e, X830e, X832e, and X912e devices.
Misc_Security_Remote_Login_Timeout_Fix	Fixes the issue in which fetching the print server device policy for E460dn devices failed.
MissingAccessControlsFix v1.0.mvp	Enhances available access control settings.
Missing_LDAP_Settings	Fixes the issue in which the Displayed Name setting was missing under LDAP Setup.
OEMVersion_Picturesupport_fix v1.0.mvp	Fixes the issue in the OEM version of MVP in which pictures of several printers were not displayed.

Oppanel_access_translations_fix v1.0	Enables MarkVision to display the Operator Panel Access settings as reported by the printer Web page for MarkNets.
PageCount_Missing_Fix	Removes disableSecurity.
Plugin_URL_FQDN	Adds Wins with DNS in the "Hostname Discovery Strategy" in <i>Administrative Settings</i> . When it is selected, MVP 11.2.1 can discover a device with a Fully Qualified Domain Name.
Refinement_Correction_E352dn	Corrects refinement for the E352dn device when mDNS must be disabled.
RefinementCorrection v1.3	Verifies that MVP-supported Lexmark devices are discovered properly for all supported security levels in MVP 11.2.1.
ScheduleDevicePolicyFix	Fixes the issue involving reapplying device policies during scheduled conformance.
Scheduler_Table_Performance_Fix	Fixes the inconsistent display of scheduled items in the scheduling window.
SecuritySettings_Conformance_Fix	Fixes the security settings conformance issue.
SNFImportFix v1.0	Fixes the SNF solution import issue: if a password was set for any device, the profiles were not imported but a success message was displayed.
SupplyStatus_Filter_Fix v1.0	Provides Supply Status Folder Creation and Folder refreshes based on a device's supply status.
T65x_Picture_Fix v1.0	Provides a picture fix for T650, T652, T654, and T656 devices using the MVP Web client.
TCPIP_Port_Access_Fix_Boeing_11_2 v1.0	Enables multiple changes to be applied successfully in TCP/IP Port Access from print server policy (based on "For Any Print Server").
TCP_IP_Port_Access_Missing_Fields	Includes "Thin Print" and "Web Services" in the TCP/IP Port Access settings page and \n displays the ports in ascending order of port number.
Toner_Cartridge_SerialNumber v1.0	Removes the Toner and Cartridge serial number column and adds Toner/Cartridge serial number.
TunnelDeviceFix v1.0	Fixes the issue in which MVP could not discover a certain combination of pre-2008 devices but could discover the print server.
VNCOppanel_fix	Adds a label in the <i>Operator Panel</i> task to guide the user in fetching the descriptor for "Remote Operator Panel" from the <i>Embedded Solutions</i> → <i>Solution Management</i> task and enabling it from <i>Configure</i> . This launches the <i>Operator Panel</i> VNC applet. After the "Remote Operator Panel" descriptor is fetched and enabled, the label is no longer displayed in the <i>Operator Panel</i> task.

## CORRECTION OF PREVIOUS ISSUES

The following issues have been corrected in MVP 11.2.1.

### **Device Policy Changes with X940e and X945e Ports**

For the HBN1, HBN3, TCP 6100, and UDP 6110 ports, MVP can now make the following changes through device policy.

1. *Secure and Unsecure to Disable*
2. *Unsecure only to Disable*
3. *Secure and Unsecure to Unsecure only*

This issue is resolved in the PE release of the Lexmark X940e and X945e firmware (level LC.BR.P080) and in level NC.NPS.N131 network firmware. The issue is still present in firmware level LC.BR.P079 (network level NC.NPS.N130) and earlier releases.

### **Default Value of “services.persistence.elementPersist” Increased to Prevent Data Loss**

The default value of the “services.persistence.elementPersist” server Web page parameter has been increased from 5 seconds to 600 seconds (10 minutes). This resolves some of the data loss issues (with scheduling, actions, alerts, policies, folders, etc.) that occurred during server restarts and sudden power shutdowns.

As a result of this change, if the MVP services are restarted or stopped at any point in time:

- Only the changes made (from MVP) more than 10 minutes before the stop/restart will be saved. Changes made within 10 minutes or less of the stop/restart will not be saved. For example, with LDAP/SSL User Accounts, the user is explicitly asked to restart the server after importing the SSL certificate. The user should wait 10 minutes before restarting the server to avoid possible data loss.
- After changing the value of an MVP server Web page parameter, users should wait at least 10 minutes before restarting the MVP services.
- To prevent data loss while upgrading from previous versions of MVP, change the value of the “services.persistence.elementPersist” key on the MarkVision Server Web page to 600 before upgrading.

### **Maintenance Kit Support**

Support has been added for 100k and 600k maintenance kits on the *Supplies* menu for the following devices.

- C930dn, C935dn
- X940e, X945e

### **Low Security Printer Lockdown**

The Printer Lockdown in Low Security Level issue has been resolved (implemented in “ON” security level in MVP 11.2.1 for the design change of Modify Security Levels).

## SETTINGS CHANGES AND CLARIFICATIONS

---

### **MVP Behavior When Incorrect PIN is Entered**

If a user enters an incorrect PIN/password three times, they will be locked out of that particular menu for the amount of time specified for the *Lockout* setting under *Miscellaneous Security*. Once the user is locked out, even a correct PIN/password entry will not be accepted until the *Lockout* time has passed.

The user will be locked out if they enter an incorrect PIN three times within the *Failure time frame* (under *Miscellaneous Security*), even if the login failures occurred inconsecutively.

The number of allowed login failures can be changed using the *Login restriction* functionality under *Miscellaneous Security*.

### **Device Policy Options May Not Be Supported All Devices**

All of the options listed in device policy (*Enable, Disable, Secure and Unsecure, and Unsecure only*) may not be supported on all devices under *Settings* → *Security* → *Device Security* → *TCP/IP Port Access*. For example, some devices support only *Enable* and *Disable*, while other devices support *Disable, Secure and Unsecure, and Unsecure only*. Regardless of whether they are supported on a particular device, all options are always listed in device policy.

### **Shifted Menus**

The previous location for the *Settings* → *MFP* → *Manage Function Access* menus has changed to *Settings* → *Security* → *Basic Security* → *Manage Function Access*.

The previous location for the *Settings* → *Security* menu has changed to *Settings* → *Security* → *Device Security*.

### **Two Settings with the Same Function**

There is a slight variance between two settings labels (*Enable Receive Log* and *Enable Call Log*) that serve the same purpose. You can find the two settings in the following locations.

- *Enable Receive Log* is located under the *Fax Log Settings* heading under *Settings* → *Fax* → *Print Server* in MVP.
- *Enable Call Log* is located under *Fax Log Settings* on a device's embedded Web page.

### **NTP Settings Locations**

Network Time Protocol (NTP) settings for some devices are distributed between two separate nodes: *Printer Device Policies* and *Print Server Policies*. These tasks handle Network Time Protocol settings on different classes of devices. Most 2008 and later devices are supported by the (Printer) version.

#### Printer Device Policies

Automatically Observe DST  
DST End  
DST Offset  
DST Start  
Enable NTP  
NTP Authentication  
UTC Offset

#### Print Server Policies

Allow NTP Broadcast  
Date & Time  
Daylight Savings Time  
DST Mode  
Time Server IP Address  
Time Server Name  
Time Source  
Time Zone

### **X500 vs. X560n Clarification**

In Basic Filters, when the *Model* (Printer/Print Server) filter is selected, the user can select a list of model names. One of these is the Lexmark X500 Series. Directly below it in the list is the Lexmark X560n. A common assumption might be that the first selection would automatically include the second. In reality, it does not. Selecting the Lexmark X500 Series includes all devices marketed as Lexmark X500 and Lexmark X502, but not any others.

### **“Analog Fax” and “Fax Server” Settings May Switch Locations**

If the *Analog Fax* and *Fax Server* settings have both been configured on a device, the settings may appear in one location and not the other when a policy is generated from the device. Ensure that settings are configured only for the fax mode that the device will be using.

### **“AppleTalk” Settings Duplicated Under “Ports”**

Some of the settings that appear under *Settings* → *Network* → *AppleTalk* also appear under *Settings* → *Network* → *Ports*. Changing the value of a setting in one of these locations changes the setting in the other location.

### **“Job Timeout” Setting Appears in Two Tasks**

The *Job Timeout* setting appears in two different tasks:

- *Settings* → *Network* → *General Settings*
- *Settings* → *Network* → *Job Timeout (Print Server)*

### **TCP/IP “Enabled” Setting is a Read-Only Field**

In the *Settings* → *Network* → *TCP/IP* task, the *Enabled* setting is a read-only field. However, it can be set to “Yes” or “No” in the Printer Server Policy. If a user disables TCP/IP by changing this setting to “No,” MVP will no longer be able to discover the device. If this occurs, go to the device’s embedded Web page or operator panel and re-enable the TCP/IP setting.

### **Acceptable Early Warning Level Values**

The *Early Warning Cartridge Percent* level only accepts values greater than the *Toner Low* value.

## **SUGGESTIONS AND RECOMMENDATIONS**

---

### **Tasks Requiring Additional Memory**

The default amount of memory MVP has when installed may not be sufficient when there are several folders monitoring the status of many (>1000) devices while a device discovery is taking place. These two tasks require a fair amount of memory to perform and may require a change to the memory configuration with respect to the number of devices and number of status folders.

For such an operation, the user should increase MVP's memory (both server and client) to suit the configuration.

### **Preventing Data Loss During Migration from MVP 11.2**

To prevent data loss while migrating from MVP 11.2 to MVP 11.2.1, users should change the value of the "services.persistence.elementPersist" server parameter to 600 seconds before starting the migration.

### **Network Speed Setting**

Users should not change the value of the *Network Speed* setting in MVP. This setting is very sensitive to a device's performance. If its value is changed and an error occurs, the device may drop off the network.

If this occurs, users must change the *Network Speed* setting on the actual device back to its default value.

### **Nested Folders and Memory**

If folders are nested at three or more levels deep, it is recommended that you configure the MarkVision Server's Java Virtual Machine (JVM) to use 1GB of memory or more to avoid generating "out of memory" errors in the system log.

See the MVP 11.2.1 User's Guide for instructions on increasing the amount of memory allocated to the JVM.

## KNOWN ISSUES

---

The following issues may be addressed in a future release.

### **Groups Cannot Be Defined for Internal Account Building Block**

Due to device restrictions, the Groups option is not available in the Print Server Device Policy for the Internal Accounts building block in MVP. This setting can be configured using the *Settings* page for the Internal Accounts task.

### **Deleting Internal User Accounts that Belong to a Group**

If a group containing internal account blocks has been selected in the Authorization Setup and is in use inside a security template, users should not be allowed to delete the internal accounts associated with the user group. However, currently a user can delete all user accounts from a group (except for the last account) even if the group is in use inside a security template.

### **Password Protected Devices Remain Accessible in MVP**

After a user applies a password to a device using device policy, the user can no longer access the device's settings from the embedded Web page. However, MVP does not display the device in red (indicating it is password protected), and the user is allowed to access the device's settings in MVP as if there is no password on the device. MVP does not acknowledge that the device is password protected.

### **MVP Cannot Create a Security Template Containing "Groups" Credentials**

If a user selects multiple devices and creates an LDAP block containing groups on the selected devices, then tries to add a security template on the selected devices, an "Authentication Error" message is displayed and the template cannot be added. This issue occurs in Print Server Device Policy and Internal Accounts, mainly for blocks that support groups.

### **Remote Operator Panel Cannot Be Secured by a PIN**

If a user configures a remote operator panel under *Settings* → *Embedded Solutions* → *Solution Management*, then creates a PIN block to secure remote management, the PIN cannot be used to secure VNC. When the user launches the VNC applet and enters the PIN in the VNC window, the authentication fails even though the PIN was entered correctly.

This issue also occurs if NTLM is used to secure VNC.

### **"Selected Printers" List Not Available After Server Restart**

For "Printer Inventory" and "Job Statistics Trend Analysis" functionalities, the list of devices in the "Selected Printers" list may not be available or may not match after an MVP server restart or after migration from a previous version of MVP.

### **Viewing Device Policy Conformance Details May Shut Down MVP Client**

If a user views the "Details" window of a device policy conformance several times, the MVP client may abruptly shut down without warning. This is due to a client heap space limitation.

To work around this issue, increase the client heap space to **-ms64M -mx256M**.

### **"Find Result" Window Freezes if MVP Client is Connected Using "Retry" Button**

If a user discovers a device in MVP using the quick find option, then restarts the MVP service, selects the device from the "Find Results" window, and selects any task, a pop-up message appears prompting the user to re-establish the connection. When the user clicks the *Retry* button, the "Find Results" window freezes.

To work around this issue, close and re-launch the MVP client.

### **Scheduled Events Cannot be Created for an Offline Device**

If a user tries to create a scheduled event and selects an offline device, the schedule cannot be created. In addition, if the user tries to create a scheduled event for several devices and one of the devices is offline, the scheduled event cannot be created.

### **Conformance Check Fails with “Row-Mismatch” Error**

For a device policy containing settings as rows organized in tabular form (for example, the “LDAP Configuration” settings under *Advanced Security* → *Building Blocks* or *Email Destinations* under *MFP* → *Destinations in Print Server Policy*), a conformance check on a device may fail with a “row-mismatch” error if the number of rows on the device differs from the number of rows on the policy.

For example, a policy may have two LDAP building blocks: LDAP1 and LDAP2, while the device only has LDAP1. Even though the LDAP1 block matches, a conformance check will fail because the number of blocks on the device is different than the number of blocks on the policy.

### **Conformance Check Fails when Run with Policy Containing Security Templates**

A device policy conformance check run with a policy containing security templates always returns a “Failed” message, even when the device settings are in conformance with the policy.

To avoid this message, remove any security templates from the policy (*Print Server Policy* → *Security* → *Security Template* → *Edit*) before running the conformance.

### **Settings Mismatch Message Not Displayed Correctly**

For all newer devices that support eSF:

During a “Check Device Conformance” operation on a printer policy (*Actions* → *Device Policies* → *Check Device Conformance*), the solution name in the policy is always compared to the last solution name listed in “Installed Solutions” (*Embedded Solutions* → *Installed Solutions*). If these two solution names do not match, a message should be displayed indicating the mismatch. MVP currently does not display the message correctly.

This issue also occurs with Profile name checks through Server Policy.

### **Invalid Values Saved in E-mail Alert Setup**

Under *Settings* → *Printer* → *E-mail Alert Setup*, if a user enters invalid values (for example, %, @, #, and \$) in the “E-mail List Edit” field, the invalid values are saved.

### **“Memory Limit Exceeded” Message on Mac OS X**

On Mac OS X systems, if a user discovers around 200-400 devices, then selects all of the devices and selects *View* → *Picture of Printer*, a “MarkVision has exceeded its memory limit” message may appear. This issue may also occur with “Status Overview” and with device policy fetching.

### **NTLM Configuration Settings Not Available in MVP**

MVP does not provide the capability to set or edit NTLM configuration settings that are required for a device to register itself with an NTLM domain controller. These settings include “Domain Name,” “Domain PDC Name,” “User ID” and “Password.” To access these settings, users must open the device Web page using HTTPS instead of the normal HTTP connection.

For newer devices, these settings are available on the embedded Web page under *Links & Index* → *Security* → *Edit Security Steps* → *NTLM* → *Register Domain*. The equivalent task in MVP (available under the *All Tasks* list) is *Security* → *NTLM (Advanced)*. This task contains only one field (“Default User Domain”).

For older devices, these settings are available on the embedded Web page under *Links & Index* → *Security* → *NTLM Authentication Setup*. The equivalent task in MVP is *Security – NTLM (Basic)*. It also contains only one field (“Default User Domain”).

#### **Deleted Custom Views/Custom Tables on Mac OS X**

If a user deletes a custom view (*View* → *Custom Views* → *Create/Manage*), then selects a device and selects *View* → *Custom Views*, the deleted view’s icon is still listed on the menu. If the user selects the icon, an “Error” message is displayed. In addition, each time a custom view is deleted, a new grayed-out “None” entry is added under *View* → *Custom Views*.

This issue occurs only with Mac OS X operating systems and also occurs with deleted Custom Tables (*View* → *Custom Tables*).

To work around this issue, restart the MVP client.

#### **MVP and File Send Success with FTP/TFTP**

MVP uses various methods such as FTP and TFTP to send files for Generic File Download, Firmware Download, and Resource Management. MVP declares the action a success or failure based on the success/failure of these methods (FTP, TFTP). In some instances, FTP/TFTP may have been successful, but the results may not be visible on the device due to internal device issues. However, because the FTP/TFTP was successful, MVP declares the action successful.

#### **Folder Refreshes**

MVP does not automatically refresh folders on the server.

#### **All MVP Main Window Options Disabled After Power Failure**

If a power failure occurs while the MarkVision Server is writing its settings to cache, the cache can become corrupted and all menu items on the MVP client become disabled (grayed out). When this occurs, all server settings are lost, including policies, discovery profiles, etc.

If this issue occurs:

1. Close the MVP client.
2. Stop the MarkVision Server.
3. Delete the contents of the `data` folder.
4. Copy the contents of the `lastSavedData` folder (which is created in the same hierarchy as the `data` folder) into the `data` folder.
5. Restart the MarkVision Server.
6. Re-launch the MVP client.

You can choose how frequently the data is backed up in the `lastSavedData` folder by using the `services.dataBackup.interval` parameter on the MarkVision Server Web page.

#### **MarkVision Server Service Temporarily Disappears if “Services” Window is Open During Upgrade**

For Windows installations, keeping the *Services* window open during an upgrade from MVP 11.2 to MVP 11.2.1 may cause the MarkVision Server service to briefly disappear from Windows service management utilities. This results in a failed installation. To avoid this problem, close the *Services* window before starting the installation.

#### **SSL Encrypted Connections Not Supported on a MVP Client Running on AIX**

The *Communications Security* option under *Administrative Settings* is not supported for AIX. The *Server to Client Security* check box must NOT be checked because the IBM JVM does not support SSL. If the check box is checked, you will be unable to log in again and will have to reinstall MVP 11.2.1.

### **Instance Settings Not Retrieved Correctly**

When a user manages embedded solutions using the *Configure* task under *Settings* → *Embedded Solutions* → *Solutions Management*, solutions with instance settings do not always retrieve the instance settings correctly. Instance settings are groups of similar settings, like arrays, used in eSF solutions to provide groups of similarly classified values.

### **MVP Continues to Discover Disconnected Devices**

In some environments, the number of discovered devices may appear to increase even though no discovery is running. This can occur when a device that MVP has already discovered is turned off/disconnected and its IP address is assigned to another device. When MVP periodically checks its devices, it discovers the disconnected device as a new device, even though it is no longer communicating. This can occur, for example, in a DHCP environment when a printer is turned off and its IP address lease expires.

To work around this issue, remove the device that is no longer communicating from MVP's list of managed devices.

### **Discovered Devices May Not Match the Specified Community Name**

When discovering Lexmark devices, MarkVision does not consider SNMP community names specified in discovery profiles or in the default SNMP community name that is configurable in *Administrative Settings*. As a result, devices may be discovered that do not match the specified community name.

To work around this issue, set the following MarkVision Server parameter to TRUE: `device.mdnsQuery.snmpCommunityName` (to configure the MarkVision Server operating parameters, enter the URL `http://[IP address or hostname]:9180/~MyServer/index.jsp` in a compatible Web browser, substituting the IP address or hostname of the computer running MarkVision Server).

**WARNING:** This workaround may cause a failure to discover devices when a discovery profile contains consecutive devices with the same IP address but different community names. In this case, a further workaround is to group devices by community name in different discovery profiles.

### **Cannot Launch MVP Web Client Locally or Remotely in Safari Browser**

If MVP is installed on a local machine or on a remote machine (not necessarily a MAC OS X, but any MVP supported operating system) and a user tries to launch the MVP Web client in the Safari Web browser, the Web client does not launch. To work around this issue, complete the following steps.

1. Copy (not move) the `log4j.properties` file from:  
`/usr/local/lexmark/mv_pro/mvWeb/mvp-tomcat/common/classes`  
to:  
`/usr/local/lexmark/mv_pro/mvWeb/www/Webapps/markvision/lib.`
2. Launch Safari.
3. Access `http://localhost:9180` (if MVP is installed on a local MAC machine) or `http://<IP address or hostname of the remote machine>:9180` (if MVP is installed on a remote machine).
4. Launch the MVP Web client.

### **MVP Operator Panel Does Not Change to Reflect Device Operator Panel Changes**

On devices that support the operator panel feature, any changes made on the device's physical operator panel are dynamically reflected in the *Operator Panel* task in MVP. However, if a user deletes, re-discovers, and re-selects a device, the *Operator Panel* task in MVP no longer dynamically changes to reflect actions performed on the physical operator panel.

If this occurs, to view the current operator panel status in MVP, press F5. This refreshes the MVP screen. To re-enable the *Operator Panel* task's ability to dynamically reflect changes made on the physical operator panel, restart the MarkVision Server.

### **Linux - "Connection Refused" Message When Connecting to MarkVision Server**

On Linux systems, users may receive a "Connection Refused" message when trying to connect to the MarkVision Server from a remote MarkVision client. This can occur if the SUSE server's hostname is mapped to the localhost IP address in the `/etc/hosts` file. You can determine this by logging into the SUSE server where the MarkVision Server is running and pinging the server's hostname. If the IP address shown is 127.0.0.x, then this is the problem.

To work around this issue, modify the `/etc/hosts` file so that the server's IP address is assigned to its real IP address. Then restart the MarkVision Server before trying to connect again.

### **Devices May Not Display a Fully-Qualified Hostname**

When discovering Lexmark devices, MarkVision does not obtain fully-qualified domain names for some newer devices. As a result, devices may not display a fully-qualified hostname (including the domain components) for these devices.

To work around this issue, set the following MarkVision Server parameter to TRUE: `device.hostName.FQDN` (to configure the MarkVision Server operating parameters, enter the URL `http://[IP address or hostname]:9180/~MyServer/index.jsp` in a compatible Web browser, substituting the IP address or hostname of the computer running MarkVision Server).

**WARNING:** This workaround may significantly impact the performance of discovery operations.

### **Limited Lines Per Inch**

MVP allows lines per inch on the PPDS task to be set as high as the value for which the devices officially claim support, which is 3,000 (the number 3,000 maps to the real number 30 on the device). Current devices do not actually support values higher than 1,900 (or 19.0), so attempts to set higher values, even though MVP will allow the attempt, may fail on the device.

### **Supply Notifications May Not Be Applicable to All Device Models**

The *Supply Notifications* task and corresponding device policy entries show all possible supply notifications, some of which may not be applicable to all device models. When configuring multiple devices or devices with different capabilities, be aware that some values may not be applicable.

### **Instance Settings in eSF Solutions Not Handled Correctly**

Some instance settings in eSF solutions are not handled correctly in the *Solutions Management* task's *Add* dialog. Some setting types do not pre-select default values and validation for numeric data in text fields is missing.

To work around this issue, ensure that numeric data is valid and select desired values manually in the *Add* dialog for all settings. Settings that do not pre-select defaults cannot be left blank because the *OK* button will not be enabled until a valid value is entered/selected for each setting.

### **"Authentication Method" Print Server Device Policy Present in Two Places**

The *Authentication Method* Print Server device policy is present in two different places. One appears under *Settings* → *Security* → *Device Security* → *On-Board Security* and the other appears under *Settings* → *Security* → *Basic Security* → *Manage Function Access*.

When creating and applying a Print Server policy based on a specific device, if a user changes the value of any one of these two *Authentication Method* settings, the user's modified value may not be applied. To work around this issue, use one of the following methods.

1. Change the value of any one of the two *Authentication Method* settings in the Print Server policy, then un-check the other *Authentication Method* setting. The desired setting change will be applied throughout the policy.
2. Modify both of these settings with the same value while applying the policy.

### **Embedded Solutions Settings May Not Be Populated**

In some cases, embedded solutions settings implemented as check boxes may not be populated when a user edits the solution configuration.

### **“Korea” and “Japan” Time Zone Values Not Supported on Older Devices**

The “Korea” and “Japan” time zone values are not supported on older (pre-2008) devices. On a pre-2008 device’s embedded Web page, if a user goes to *Links & Index* and clicks *Date & Time*, they can select “Korea” and “Japan” from the *Time Zone* drop-down list. However, if a user applies one of these values and then views the *Time Zone* field in MVP under *Settings* → *Network* → *Date/Time* → *Network Time Protocol(Print Server)*, the field is blank. The value is not applied, but the user does not receive an error message stating that the value is not supported.

### **Custom Media Paper Type Bin Errors**

Errors may occur when a user applies a printer device policy using settings under *Settings* → *Printer* → *Paper* → *Custom Media - Paper Type Bin* if the printer policy also has a value enforced (checked) under *Paper* → *Configure Bin*. To work around this issue, make sure this value is not enforced by un-checking *Configure Bin* before applying the policy.

### **“Tray 5 Hp” Option Missing When One Device is Selected**

The *Tray 5 Hp* option is missing under *IPDS Map Input Trays* → *Tray Mapping* for Printer Device Policy, but is available when multiple devices are selected.

### **Power Saver and Duplex Settings Are Dependent on Eco Mode**

On devices that support the *Eco Mode* setting, the *Power Saver* and *Duplex* settings are dependent on *Eco Mode*. As a result, after a user applies a policy containing these settings, the values of *Power Saver* and *Duplex* may be different than the values the user selected before applying the policy. This is because the *Power Saver* and *Duplex* settings changed when *Eco Mode* was configured. This issue affects the following devices.

- Lexmark C540, C543, C544
- Lexmark E260, E360, E460
- Lexmark T650, T652, T654
- Lexmark X651de, X652de, X654de, X656de, X658de

### **Changes Made in “Enable Call Log” Reflected in “Enable Receive Log”**

Changes made to the *Enable Call Log* setting under *Fax Log Settings* on a device’s embedded Web page are reflected in the *Enable Receive Log* setting in MarkVision under the *Fax Log Settings* heading under *Settings* → *Fax* → *Print Server*.

### **IPv6 Settings Prefix Length Error**

In the *IPv6 settings* task, if a user clears the *Prefix Length* setting and clicks *Apply*, a default value of 64 appears and an error message is displayed stating that the setting cannot be applied. To work around this issue, enter valid values for *Prefix Length* and do not leave this setting blank.

### **“Fax Transmit Level” and “Fax Receive Threshold” Input Error**

Under *Settings* → *MFP* → *Special Configuration/Debug (Print Server)*, for both *Fax Transmit Level* and *Fax Receive Threshold*, input from the keyboard is accepted only if there are values already present in the fields. To work around this issue, always modify existing values; do not highlight a value and press *Delete*.

### **Fax Holding Schedule Does Not Report Errors**

The Fax Holding schedule does not report errors if multiple actions are scheduled at the same time.

### **Command Line Cannot be Executed on a Remote Windows Machine**

An error is displayed when a user attempts to execute a command line on a remote Windows machine while creating a new action in MarkVision Messenger. Messenger cannot run the command because the remote host does not provide the necessary Rexec service.

### **PIN Cannot be Entered in Red Hat Enterprise Linux Client 5**

In the MVP client under *Settings* → *Security* → *Advanced Security* → *Building Blocks* → *PIN*, users cannot enter a value in the PIN field. To work around this issue:

1. Go to *System* → *Preferences* → *More Preferences* → *SCIM Input Method setup*.
2. Select the keyboard and un-check the *Embed Predit String into Client Window* option.
3. Go to *Panel* → *GTK* and un-check all options present.

For more information, visit the following URLs.

- <http://java.sun.com/javase/6/Webnotes/ReleaseNotes.html>
- <http://www.cs.wisc.edu/twiki/bin/view/CSDocs/RhelFiveFaq>

### **Double-Byte Character Set (DBCS) Issues**

- DBCS characters cannot be entered for custom paper names from *Configuration* → *Paper Menu* → *Custom Name* on a device's embedded Web page. To work around this issue, enter DBCS characters for custom paper names only from within MVP and not from the embedded Web page.
- When running Windows XP or Windows Vista, the import certificate GUI may disappear when characters are entered through the Chinese Input Method Editor. If this happens, un-check the *At-carat* option from the context menu and try again.
- DBCS characters are not supported in passwords at this time.
- If a user enters more than thirteen DBCS characters into the "Custom Message," "Default," or "Alternate" fields under *Settings* → *Printer* → *Custom Messages*, after the user clicks *Apply*, the fourteenth character is displayed as a small box.
- The "Language" drop-down list under *General Settings (Printer)* contains the options "???" and "?esky." If a user sets the language to "???", the device policy does not fetch anything from the printer and an error is generated.
- For the E460 and X658de devices, if a user enters DBCS characters into the "Custom Message" fields under *Settings* → *Printer* → *Display Messages*, after the user clicks *Apply*, the DBCS characters are displayed as question marks (????).
- For the X543 and X544 devices, when the printer's operator panel language is set to Traditional Chinese, the *Operator Panel* task in MVP does not display the Chinese characters. When the printer's operator panel language is set to English, the *Operator Panel* task in MVP displays "Ready." However, if a user clicks the *Menu* button, the MVP operator panel display goes blank.
- For the X651de, X652de, X654de, X656de, and X658de devices, if a user enters more than ten DBCS characters into the "Custom Text 1" or "Custom Text 2" fields under *Settings* → *Printer* → *Displayed Information*, after the user clicks *Apply*, the DBCS characters are not displayed.
- The LCD display on the C540, C543, and C544 devices does not wrap DBCS characters correctly.

### **“LDAP Configurations” Window Clipping Issue**

When a user is setting configuration preferences in the *LDAP Configurations* window, incorrect clipping of the text box may occur due to the mode in which Windows is running. To correct this, change the Windows theme to “Classic.”

### **Distorted Drop-Down Lists in Safari Browser**

When the MVP Web client is launched in the Safari Web browser, all drop-down lists appear distorted. Some options in the drop-down lists are crowded together and some options are cut off at the top or bottom.

### **“Top Bin Timeout” Setting Issues**

The value “0” cannot be applied to the *Top Bin Timeout* setting under *Settings* → *Printer* → *General Settings*. If a user sets the value of *Top Bin Timeout* to “0” and applies this setting, the “Disable” option is automatically selected.

There is also an inconsistency in the range of values that can be applied to the *Top Bin Timeout* setting. The range of possible values for this option is different depending on whether one device is selected or multiple devices are selected. If one device is selected, *Top Bin Timeout* has a range of “0-255.” If multiple devices are selected, *Top Bin Timeout* has a range of “5-255.”

### **Limitations for Creating a Printer Driver**

- Creating a printer driver from an older operating system to a newer operating system (i.e. Windows XP to Windows 2003) is currently not possible.
- Creating a printer driver between the same level of operating system (i.e. Windows XP to Windows XP) remotely is currently not possible.
- Creating a printer driver in the Windows Vista operating system either locally or remotely is currently not possible.
- When users try to create a print object from a client while connecting through a remote MarkVision Server, the driver displays the following error message: “No installable drivers found.” This is only a problem when the client is connected through a remote server.

### **Launching MVP Messenger in Windows Vista**

When using Internet Explorer 7 with Windows Vista, users cannot launch the MVP Messenger from the MarkVision Web client. Use one of the following workarounds.

1. Navigate to *Internet Options* → *Security* and select the *Local intranet* icon. Next, uncheck the *Enable Protected Mode* box and click *Apply*. Then click *OK* and restart Internet Explorer.
2. Launch Internet Explorer 7 as an administrator (right-click and click *Run as administrator*).

### **Contact Name and Location Not Populated in Custom Table**

When users create a custom table, if the number of columns displayed is limited, the *Contact Name* and *Contact Location* fields are populated correctly. If the custom table is created with all columns displayed, the *Contact Name* and *Contact Location* fields are not populated.

### **“Page Mode” Option Disappears After Unacceptable Value is Applied**

When an unacceptable value is applied to multiple devices in the *Page Mode* field under *Settings* → *Printer* → *General Settings*, an error message should appear. Instead, the unacceptable value is applied, causing the *Page Mode* option to disappear under *General Settings* for each device. To restore the *Page Mode* option, re-select all of the devices and then apply a valid value to *Page Mode*.

**MVP Client Fails to Launch After Migration to MVP 11.2.1**

In some very rare instances, after a user migrates from a previous version of MVP to MVP 11.2.1 on Windows platforms, the MVP client fails to launch. This occurs when the client JRE files are not copied properly to the C:\Program Files\MarkVision Professional\jre directory during the migration install. To work around this issue, copy the MarkVision Server JRE folder (located in C:\Program Files\Lexmark\MarkVision Server\jre) to the client JRE location, then launch the MVP client.

## **DEVICE SPECIFIC ISSUES**

### **Lexmark C500, X342**

#### **Cartridge Percentages Not Displayed**

These devices do not report cartridge percentages. As a result, "Device Incapable of Task" is displayed for each cartridge in the *Supplies* task.

### **Lexmark C540, C543, C544, E260, E360**

#### **Diagnostics Configuration Page Sometimes Shows Incomplete Data**

For these devices, the *View* → *Diagnostics* → *Configuration Page* task may show incomplete data (device data only, no diagnostics information).

### **Lexmark C540, C543, C544, E460**

#### **Date/Time Field Issue in Event Log**

After selecting a device, if a user navigates to *View* → *Diagnostics* → *Event Log*, the system sometimes reports incorrect values for the date and time. This problem occurs when the system time is not updated. Usually, device crashes are a common source of this kind of problem, especially when occurring in the early stages of Power On Reset. The "???" is an indication that this problem may have occurred.

### **Lexmark C540, C543, C544, C546, X543, X544, X546**

#### **Picture in MVP Incorrectly Displays Cartridge Cover Open**

If the front door of a device is opened, the picture of the device in MVP (under *View* → *Picture of Printer*) displays both the front door and the cartridge cover open.

### **Lexmark C760, C762**

#### **"Restricted Server" Setting Not Populated Correctly**

When a Print Server policy is generated, the *Restricted Server* setting is not populated correctly. To work around this issue, manually edit the value for this setting.

### **Lexmark C912**

#### **Toner/Cartridge Serial Number Not Available**

The toner/cartridge serial number is not available in MVP for this device.

### **Lexmark E260, E360, E460**

#### **Emulation Setting Cannot Be Changed from Device Policy**

The value of *Printer* → *General Settings* → *Emulation* cannot be changed from a device policy based on a specific device if the *PPDS > Active* setting under the device policy is activated (checked). To work around this issue, un-check *PPDS > Active* before changing and applying the emulation setting.

## **Lexmark Forms Printer 2580, 2581, 2590, 2591**

### **Device Policy-Related Issues**

- Settings nodes appear under the Print Server device policy instead of under the Printer device policy where a user may expect to find them.
- The *Configure Macro* table in the *Settings* → *258x/259x* → *Configure* menu is not supported in device policy.

### **Macro-Related Issues**

- When the default macro is set to “Disable macro” on the device’s embedded Web page, the default macro value (in MVP in the *Settings* → *258x/259x* → *Configure* menu) appears blank when it should appear as disabled.
- After the “Disable macro” option is applied, it is no longer displayed as an option. After any other Macro (1 to 4) is applied, the “Disable macro” option is available.
- In the *Configure Macro* table (in the *Settings* → *258x/259x* → *Configure* menu), converted values of “Top-of-Form \*\*\*” columns may differ slightly if centimeter units are used when set from MarkVision.

### **Wait Period for Automatic Device Resetting**

Users may have to wait for some time after applying any settings that result in automatic device resetting.

## **Lexmark T620, T622**

### **“Special Configuration/Debug (Printer)” Task Not Supported**

The *Special Configuration/Debug (Printer)* task under *Settings* → *Printer* is not supported on these devices.

## **Lexmark X203n, X204n**

### **“Send me a copy” Values When Multiple Printers Are Selected**

If one printer is selected, the following two values are available for the “Send me a copy” option under *Settings* → *MFP* → *Default Scan to Email Settings*: “Yes” and “No.” If multiple printers are selected, the following four values are available for the “Send me a copy” option: “Disabled,” “Enabled: Off by default,” “Enabled: ON always,” and “Enabled: ON by default.” If a user selects multiple printers and chooses “Enabled: ON by default,” the value will be set to “Yes.” If a user selects multiple printers and chooses “Disabled,” the value will be set to “No.”

### **Scan Job History Data Cannot be Collected**

Scan Job History data cannot be collected for these devices. These devices do not send fax/scan complete alerts. This data can be found under *Actions* → *Job Statistics and Trend Analysis*.

### **Unsupported Diagnostics Options**

The “Meters/Counters” and “Event Log” options under *View* → *Diagnostics* are not supported.

## **Lexmark X264dn, X363dn, X364dn, X364dw, X543, X544, X546**

### **PCL Font Settings Cannot Be Applied**

Due to a firmware limitation, the PCL font settings (“Name,” “Symbol Set,” etc.) under *Settings* → *Printer* → *PCL* → *Default Font* cannot be applied. If a user attempts to change and apply these settings, the MVP client displays a “Default Font Could Not Be Applied” error message.

To work around this issue, select the font from the device's operator panel.

#### **Scan Job Statistics Not Recorded in RAWJASCANJOB Table**

Data related to scan job statistics (on the "Job Statistics and Trend Analysis" task in MVP) is not recorded in the RAWJASCANJOB table.

**Lexmark X463de, X464de, X466de, X466dte, X466dtwe, X546, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de**

#### **Missing "Custom Background Image" Task**

The *Custom Background Image* task is missing under *Device Policy*. This task is available under *Settings* → *MFP* → *Custom Background Image*.

**Lexmark X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, C734, C736**

#### **Applying Changes to Internal Account "Required User Credentials" Settings**

On a device whose remote management is secured by the Internal Account building block, if the *Required User Credentials* parameter is changed from "User ID" to "User ID and Password" (either from the MVP task or the print server Web interface), the user should not be able to access the printer from MVP unless they enter both an Internal Account User ID and its password on the *Advanced Credentials* task. However, after deleting and rediscovering the device, the change to "User ID and Password" does not seem to have been applied and the user can still access the device by entering only the User ID.

This occurs because deleting a printer object in MVP does not terminate the current LS session; instead, it starts another one. When a user deletes and rediscovers a device after changing the *Required User Credentials* parameter to "User ID and Password," the existing authenticated connection remains active, allowing the user to access the device using only the User ID.

To reset all existing connections after making changes, reset the device.

**Lexmark X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de**

#### **Fax Cover Page Settings Not Supported**

Fax Cover Page settings are not supported for these devices.

#### **Lexmark X500 Series**

##### **Firmware Limitations**

Due to firmware limitations:

- The *Actions* → *Reset* task is not supported.
- The value of *Gateway Address* is not populated in the *Feature Overview (Print Servers)* task.
- The *Supplies* task and the *Custom View* component are not supported.

## **Lexmark X543, X544**

### **Unsupported Page Counts**

The following page counts are not supported in the *Page Counts* task or in *Custom Tables*.

- Copy Page Count
- Fax Page Count
- Copy Scan Count
- Network Scan Count
- Fax Scan Count

## **Lexmark X560n**

### **Incorrect Printing Speed Displayed**

For this device, *Speed* is incorrectly displayed as “0 – Impressions Per Minute” in MVP under *Feature* → *Capabilities*. The device’s embedded Web page displays the correct speeds of 20 Pages/Minute (Color) and 30 Pages/Minute (Mono).

## **Lexmark X644e, X646e**

### **“DST Mode” Value Not Retrieved When Editing A Device Policy**

The value for the *DST Mode* setting under *Settings* → *Network* → *Date/Time* is not retrieved when a user edits a device policy. In addition, MarkVision may report an error when a value is applied to this setting even though the value has been applied successfully.

## **Lexmark X651de, X652de, X654de, X656de, X658de**

### **Scanner Jam Alert Not Displayed Correctly**

When a scanner jam occurs, the “Scanner Jam” alert is not displayed correctly under *View* → *Status of Printer*. An incorrect alert that says “Scanner ADF Cover Open” is displayed instead of the correct “292.00 Scanner Jam” alert.

### **Fax Cover Page Settings Not Supported**

Fax Cover Page settings are not supported for these devices.

## **Lexmark X734de, X736de, X738de**

### **Missing “Tray 5 Adjust” Settings on Mac OS X 10.4**

For IPDS-connected printers, the *Tray 5 Adjust* settings are missing from the “Margins” list under *Settings* → *Printer* → *IPDS*. These settings are available on a device’s embedded Web page. This issue occurs only with the Mac OS X 10.4 operating system.

## **Lexmark X860de, X862de, X864de**

### **Picture in MVP Incorrectly Displays Door Closed**

If “Door J” (Front Cover) on a device is opened, then “Door A” is opened, the picture of the device in MVP (under *View* → *Picture of Printer*) displays “Door J” closed even though it is still open on the actual device.

### **Scanner Alerts Not Displayed**

MVP does not display the “Scanner Jam” alert or the “Replace all originals, if restarting job” alert if a paper jam or error occurs in the ADF (Automatic Document Feeder).

### **Lexmark X860de, X862de, X864de, W850**

#### **Cannot Fetch Printer-Related Settings or Printer Policy for Secured Devices**

MVP cannot fetch or apply printer-related settings or a “Printer Policy” based on a specific device after an Advance Security Template (created by using any building block, such as LDAP, PIN, Password, etc.) is applied to the “Remote Management” field of the “Access Control” task. The device must be discovered by providing the advanced security credentials from *Settings* → *Security* → *Server Security* → *Advance Credentials*.

To work around this issue, remove the corresponding Advance Security Template from the “Remote Management” field of the “Access Control” task and rediscover the device from MVP.

#### **Cannot Lock/Unlock Operator Panel for Secured Devices**

MVP cannot lock/unlock (from *Action* → *Operator Panel Lock/Unlock*) a device’s operator panel after an Advance Security Template (created by using any building block, such as LDAP, PIN, Password, etc.) is applied to the “Remote Management” field of the “Access Control” task. The device must be discovered by providing the advanced security credentials from *Settings* → *Security* → *Server Security* → *Advance Credentials*.

To work around this issue, remove the corresponding Advance Security Template from the “Remote Management” field of the “Access Control” task and rediscover the device from MVP.

### **Lexmark X940e, X945e**

#### **Missing Check Box for “Enable PPM Mib”**

When navigating to *Settings* → *Security* → *Device Security* → *SNMP*, users should find a check box called *Enable PPM Mib*; however, this check box currently does not exist.

## UNSUPPORTED SETTINGS

The following device settings are not supported in MarkVision Professional 11.2.1. MarkVision is continually updated to expand device support. Support for these settings may be added in a future release.

Setting	Device(s)	Location on Embedded Web Page	Location on MVP Client
802.1x Device Certificate	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Security → 802.1x	
Blank Pages	X651de, X652de, X654de, X656de, X658de	Settings → Print Settings → Finishing Menu	Settings → Printer → General Settings
Certificate Authority Management	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Security → Certificate Management	
Character encoding	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Security → Edit Security Setups → Kerberos 5	
Custom Background Image	T656, X651de, X652de, X654de, X656de, X658de, X463de, X464de, X466de, X466dte, X734de, X736de, X738de, X860de, X862de, X864de	Settings → General Settings	Settings → MFP → Custom Background Image
Custom Scan Sizes	E460dn, E460dw, E462dtn, X264dn, X363dn, X364dn, X364dw, X463de, X464de, X466de, X466dte, X466dtwe, X543, X544, X546, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Paper Menu	

Dialing Prefix Rules	X651de, X652de, X654de, X656de, X658de, X463de, X464de, X466de, X466dte, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Fax Settings → Analog Fax Setup → Fax Send Settings	
Enable Analog Receive	X651de, X652de, X654de, X656de, X658de, X463de, X464de, X466de, X466dte, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Fax Settings → Fax Server Setup → Fax Server Default Scan Setup	Settings → Fax → Analog → Fax Receive Settings → Enable Fax Server Mode
Enable Event Logging	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Security → 802.1x	
Flash Drive Menu → Print Setting	C540, C543, C544, C546, C734, C736, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X543, X544, X546, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Print Settings	
Flash Drive Menu → Scan Setting	C540, C543, C544, C546, C734, C736, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X543, X544, X546, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Print Settings	
HTTPS Device Certificate	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Network/Ports → TCP/IP	
Import Fax Logo	X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Fax Settings → Analog Fax Setup → Fax Cover Page	

LAA*	All supported devices	Settings → General Settings	
Manage Copy Shortcuts	X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Manage Shortcuts	
One Page Copy	X651de, X652de, X654de, X656de, X658de	Settings → General Settings	
PictBridge Menu	C540, C543, C544, C546, C734, C736, X543, X544, X546, X734de, X736de, X738de	Settings → Print Settings	
Register Domain	All supported devices	Links & Index → Security → Edit Security Steps → NTLM (newer devices) Links & Index → Security → NTLM Authentication Setup (older devices)	
Resource Capture	X651de, X652de, X654de, X656de, X658de	Settings → IPDS Settings → IPDS Configuration	
Restricted Server List	All supported devices	Settings → Network/Ports → TCP/IP	
Select Device Certificate	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de	Settings → Security → IPSec	
Separator Sheets	All supported devices	Settings → Print Settings → Finishing Menu	Settings → Printer → General Settings
Separator Source	All supported devices	Settings → Print Settings → Finishing Menu	Settings → Printer → General Settings
Size Error Message	X264dn, X363dn, X364dn, X364dw, X543, X544, X546	Settings → E-mail/FTP Settings → E-mail Settings	
Tray 5 Adjust	Devices with 5 trays and an IPDS card	Settings → IPDS Settings → IPDS Configuration	

Tray Renumber	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de, C540, C543, C544, C546, E260, E360, E460, E462dtn, X543, X544, X546, X264dn, X363dn, X364dn, X364dw	Settings → Print Settings → PCL Emul Menu	
Universal Setup	C734, C736, E460dn, E460dw, E462dtn, T650, T652, T654, T656, W850, X463de, X464de, X466de, X466dte, X466dtwe, X651de, X652de, X654de, X656de, X658de, X734de, X736de, X738de, X860de, X862de, X864de, C540, C543, C544, C546, E260, E360, E460, E462dtn, X543, X544, X546, X264dn, X364dn, X363dn, X364dw	Settings → Paper Menu	

## DISPLAYED SETTINGS DIFFERENCES

### E-mail Alert Setup and Supply Notifications Settings Differences

Some of the “E-mail Alert Setup” and “Supply Notifications” settings available in MVP do not match the settings available on a device’s embedded Web page and vice versa. This applies to all supported devices.

Lexmark and Lexmark with diamond design are trademarks of Lexmark International, Inc., registered in the United States and/or other countries.

Other trademarks are the property of their respective owners.

**© 2009 Lexmark International, Inc. All rights reserved.**