

Markvision Enterprise Release Notes (2.3.0)

[Support Statements](#)

[System Requirements](#)

[Operating Systems](#)

[Firewall Rules](#)

[Browsers](#)

[Databases](#)

[Firebird \(included\)](#)

[Microsoft SQL Server \(not included\)](#)

[Languages](#)

[Supported Models \(oldest to newest\)](#)

[Upgrading Markvision Enterprise](#)

[New and Noteworthy](#)

[Known Issues](#)

[Using Firmware policies with the MS610](#)

[Certificates used for SSL will need to be reimported when upgrading from 1.8.x](#)

[Bookmark Causing Communication Error](#)

[Error#:2032 when accessing MVE client](#)

[Permanent](#)

Support Statements

System Requirements

- CPU
 - Minimum: 1 physical 2GHz (Hyper-Threaded/Dual Core)
 - Suggested: 2+ physical 3+ GHz (Hyper-Threaded/Dual Core+)
- RAM

- Minimum: 2 GB
- Suggested: 4GB
- Storage space: 60 GB
- Screen resolution: 1024x768 or greater

Operating Systems

It is expected the Operating System will have the latest patches/updates installed.

- Windows
 - 32-bit
 - Windows 7
 - Windows 7 via VMWare ESX 3.5 U5
 - Windows 7 via VMWare vSphere 4 U1
 - 64-bit
 - Windows 7
 - Windows 7 via VMWare ESX 3.5 U5
 - Windows 7 via VMWare vSphere 4 U1
 - Windows Server 2008 R2
 - Windows Server 2008 R2 via VMWare ESX 3.5 U5
 - Windows Server 2008 R2 via VMWare vSphere 4 U1
 - Windows Server 2012 Standard Edition
 - Windows Server 2012 R2
 - Windows 10

Firewall Rules

The installer will attempt to create several Windows firewall rules. If the Windows Firewall is not running at the time of installation, but is enabled later, these rules need to be created manually.

Rules:

- `firewall add allowedprogram "<installdir>/tomcat/bin/tomcat8.exe"`
`"MarkVision Enterprise Tomcat"`
- `firewall add portopening UDP 9187 "MarkVision Enterprise NPA UDP"`
- `firewall add portopening UDP 6100 "MarkVision Enterprise LST UDP"`

Browsers

It is expected the Browser will have the latest patches/updates installed. It must also have the latest version of both Adobe Flash Player (to run the client) and Adobe Reader (to view reports).

- Microsoft Edge
- Microsoft Internet Explorer 11.x
- Mozilla FireFox - Latest version
- Google Chrome - Latest version
- Apple Safari 5.1.7
- Apple Safari 5.1.7 (all platforms)
- Apple Safari 8.0.3 (Mac only)

Databases

Firebird (included)

- 32-bit

Microsoft SQL Server (not included)

It is expected the database will have the latest patches/updates installed.

- 32-bit
 - 2008
 - 2012
- 64-bit
 - 2008
 - 2012

Languages

1. English
2. French
3. Italian
4. German
5. Spanish
6. Brazilian Portuguese
7. Simplified Chinese

Supported Models (oldest to newest)

The following table lists the models supported by Markvision Enterprise. The second column indicates models that support the Security settings. The third column indicates models that support a limited number of security settings. These devices do not support :

- The Access Controls, Security Templates, and Miscellaneous Settings sections of the security settings within a Configuration
- The Embedded Web Server Remote Management access control
- The user name, realm, password and PIN communication credentials

Model	Security Settings	Limited Security
T642/T644 with 4600 MFP		✓

T640/T642/T644		✓
W840		✓
C520/C522/C524		✓
C920		✓
X850/X852/X854		✓
X644/X646		
X642		✓
C770/C772		✓
C772 with 4600 MFP		✓
E350/E352		
E250		
E450		
C530/C532/C534		✓
C780/C782		✓
C930/C935		✓
X940/X945		✓
C780/C782 with 4600 MFP		✓

T650/T652/T654	✓	
C734/C736	✓	
E260		
C540/C542/C544/C546		
X658	✓	
X734/X736/X738	✓	
X543/X544/X546		
X264/X363/X364		
E360		
E460/E462	✓	
X463/X464/X466	✓	
C792	✓	
X654/X656	✓	
X651/X652	✓	
W850	✓	
X860/X862/X864	✓	
X792	✓	

T656	✓	
C925	✓	
X925	✓	
Forms Printer 2580/2581/2590/2591		
C950	✓	
X950/X952/X954	✓	
6500e	✓	
X548	✓	
Pro5500 Series		
Pro710 Series		
Pro910 Series		
Pro4000 Series		
X746/X748	✓	
C746	✓	
C748	✓	
MS810 Ln/MS811Mn /MS812 Hn	✓	
MS 810 Lne/ MS812 Hne	✓	

CS310/CS410	✓	
CS510	✓	
MS310/MS410/MS510	✓	
MS610	✓	
MS710dn/MS711dn	✓	
CX310	✓	
MX310	✓	
CX410 / CX510	✓	
MX410/ MX510 / MX511	✓	
MX610 / MX611	✓	
MX710 / MX711	✓	
MX810 / MX811 / MX812	✓	
M5155	✓	
M5163	✓	
M5170	✓	
XM7155	✓	
XM7163	✓	
XM7170	✓	

XM5163	✓	
XM5170	✓	
XC2130	✓	
XC2132	✓	
C2132	✓	
M3150	✓	
M1140	✓	
M1145	✓	
XM3150	✓	
XM1140	✓	
XM1145	✓	
MX6500e	✓	
MS312dn	✓	
MS315dn	✓	
MS415dn	✓	
M1140 Plus	✓	
MX910de	✓	
MX910dxe	✓	

MX911de	✓	
MX911dte	✓	
MX912de	✓	
MX912dxe	✓	
XM9145	✓	
XM9155	✓	
XM9165	✓	
MS911de	✓	
CS720	✓	
CS725	✓	
CX725	✓	
C4150	✓	
XC4150	✓	
XC2130	✓	
CS820	✓	
C6160	✓	
CX820	✓	
XC6152	✓	
CX825	✓	
XC8155	✓	

CX860	✓	
XC8160	✓	
CS820	✓	
CS725	✓	
C4150	✓	
CX725	✓	
XC4150	✓	

Toshiba Device Support

Model	Security Settings	Limited Security
e-Studio305CP	✓	
e-Studio305CS	✓	
e-Studio385P	✓	
e-Studio385S	✓	
e-Studio470P	✓	
e-Studio520P	✓	
e-Studio525P	✓	

Source Technology Device Support

Model	Security Settings	Limited Security
ST9530		
ST9620		
ST9630		
ST9712	✓	
ST9717	✓	
ST9720	✓	
ST9722	✓	
ST9730	✓	

Upgrading Markvision Enterprise

Beginning with MVE 1.6, most major versions can now be skipped during the upgrade process.

If upgrading from the 1.x product to the 2.x product, MVE 2.0.0 must be an intermediate step in the process. The policy migration process is performed in MVE 2.0.0 and no other release.

Valid

1.6.x -> 2.0 -> 2.x.x

1.7 -> 1.9 -> 2.0

2.0 -> 2.3.0

Invalid

1.6.x -> 2.1.x

1.8 -> 2.3.x

New and Noteworthy

● General

- Added support for Kerberos authentication to Markvision Enterprise
- Addressed a security vulnerability as outlined in CVE-2016-1487
- Removed 'Font Cartridges' and 'Ports' from Audit and Data Export
- Dropped support for Internet Explorer 9 & 10
- Added a configurable login disclaimer within System Configuration
- Improved device communication performance
- Added support for the following Lexmark models:
 - XC2130, CS820, C6160, CX820, XC6152, CX825, XC8155, CX860, XC8160, CS820, CS725, C4150, CX725, XC4150
- Added support for the following Source Technology models:
 - ST9712, ST9715, ST9717, ST9720, ST9722, ST9730, ST9630, and ST9530
- Miscellaneous security improvements
- Added device authentication method to Audit window
- Firebird can now only be accessed by localhost
- Removed unsupported and unused SNMPv3 parameters in Discovery Profiles
 - AES-192
 - AES-256

● Configurations

- Added the ability to author general security settings without having to clone a device (Note: Cloning is still required in order to obtain security templates, FACs, and other miscellaneous security settings)

- Added support for the following settings in supported models:
 - Print With Display Off
 - Restricted Server list
 - Sleep - Timeout
 - Homescreen Fax
 - Color option in email settings
- Fixed various French translations
- Fixed an issue where a leading 0 in an IP address within a Discovery Profile caused failures

Known Issues

Importing Configurations into MVE 2.3.0

- Configurations from previous versions of MVE can not be imported into MVE 2.3.0 and forward.

Variable Settings Data File Migration

- MVE no longer requires a separate Data File for security settings and device settings. As such, the following logic will be used during an upgrade:
 - If separate Data Files are used for Device Settings and Security Settings: Only the Data File linked to Device Settings will be used
 - A Data File is linked to Device Settings and no Data File is linked for Security Settings: MVE will use the Device Settings Data File
 - A Data File is linked to Security and no Data File is linked for Device Settings: MVE will use the Security Data File
 - If the same Data File is used for Device Settings and Security Settings: MVE will keep one of the files and no further user intervention is needed.

A Subset of Devices May Fall Into the Managed (Changed) State Upon Auditing After Upgrade

- In some cases, devices may fall into the Managed (Changed) state upon an initial audit after an upgrade due to the way that input and output options are reported. Auditing a second time will resolve this issue.

Cloned Configurations and Solutions

- When a Configuration is cloned from a device, the current Security settings from the device are saved as part of the Configuration. When some Solutions are added to a device, they add new Function Access Controls to the Security settings of the device. These new Function Access Controls can cause the Configuration to always show as out of conformance, because the Configuration does not contain these new Function Access Controls. To avoid this problem, install all desired Solutions to the device before cloning the configuration. Upload those Solutions to the MVE library and add them to the Configuration. The Configuration can now be assigned and enforced to other devices that require the same settings and Solutions.

Error#:2032 when accessing MVE client

- The MVE client is an Adobe Flash application. Adobe requires internet access for the first execution of an Adobe Flash application. Workstations or networks without internet access will not be able to run the MVE client. If internet access can be granted temporarily, the MVE client can be executed successfully the first time and will then execute properly thereafter without further internet access.
- **If you can allow temporary internet access to the client:**
 - Add "*.local" to the exception list in the Proxy Server settings of the browser, to give temporary internet access to load <http://localhost:9788/mve> (assuming MVE is being accessed from the server from which it resides).
- **If you are unable to give temporary internet access to the client:**
 - Adobe Flash Player (whether web installer or offline installer), needs internet connection the first time you run the client after an installation. It will not work in an intranet-only environment.

Permanent

- General
 - If you export log file in CSV format junk characters may be displayed. Excel

seems to expect csv files to be ANSI encoded. To resolve this problem use the following work around :

- Open the exported log file in NotePad
 - Save it as ANSI encoding - when you click File > 'Save As' look at the bottom of the dialog and click ANSI in the drop down. The new file will display correctly in Excel.
- If a task is dealing with a large number of printers, it might take longer than expected to stop it, if the user chooses to do so. (DE923)
 - 2032 Error when attempting to connect to the MarkVision server from the server machine. If the PC where MVE is running has access to the intranet, but does not have access to the internet, this error will occur. To correct the problem add "*.local" to the exception list in the Proxy Server settings in your browser.
- Installation/Uninstallation
 - There are known limitations to running MVE and Lexmark Document Solution Suite (LDSS) 4.x, simultaneously, on the same machine; due to the same LST limitation mentioned in the preceding note.
 - Uninstalling Markvision Enterprise (MVE) that has been configured to use MS SQL Server will not drop created tables or databases. Administrators should manually drop the MS SQL Server databases created (named FRAMEWORK, MONITOR, and QUARTZ) after the uninstall.
 - Device Statistics
 - "install dates" are showing in the locale of the MVE server instead of the locale of the printer (DE914)
 - Configuration
 - Due to limitations in Lexmark device firmware, in order for MVE to be able to send files to a printer (Generic File Download & Firmware updates), the Firmware Function Access Control must not be set.
 - Due to limitations in Lexmark device firmware, in order for MVE to be able to enforce policies on a printer, the NPA Network Adapter Setting Changes Function Access Control must not be set.
 - Due to changes in Lexmark device firmware, enforcing a Configuration with security settings on a Lexmark X651 may fail after firmware is updated. To resolve the issue, recreate the security template on the device and try it again.
 - Service Desk
 - Picture of Printer
 - Devices added in this release (and all future devices) will not support Picture of Printer.
 - The Lexmark X264 does not support the "Tray Open/Close" events.
 - The Lexmark X464 does not support the "Tray Open/Close" events.
 - Supply status level percentages for a supply nearing end-of-life becomes less accurate. The percentages retrieved from each device and each supply for that

device are dependent on how that device handles low supplies.

- Example: When toner gets below a certain threshold on one device, that device may simply return 1% remaining, while on a different device it may return percentages that are below that threshold.
- Lexmark C746 does not support the remote operator panel.
- Event Manager
 - Perceived duplicate alert emails. Depending on how the email body is set up in MVE, the email could be seen as a duplicate. Email body can contain any messages, including the printer's and alert's variables. If the variable(s) that differentiate between alerts are omitted, then the email body will be the same. This becomes more apparent with active conditions that trigger multiple alerts. Users will see that one active condition has become active, but two emails are received.
 - Example: waste toner bottle: nearly full. This condition will generate two alerts. If the user creates the email body containing all the variables but missing the alert.type, then the email body will be identical.
 - (DE976/PTR389550) A Lexmark C935 can send multiple alerts, seemingly for the same condition. For example, when registered for a 'Supply Low' alert with 'On Active and Clear' option & the device enters a 'Black_Toner_Low' condition, it issues four alerts, which are received by MVE:
 - Nov 15, 2010 5:38:29 PM \${configurationItem.ame} 10.195.7.106
Lexmark C930 Supply Low Black Toner Active Warning
 - Nov 15, 2010 5:38:34 PM \${configurationItem.ame} 10.195.7.106
Lexmark C930 Supply Low Black Toner Active InterventionRequired
 - Nov 15, 2010 5:38:41 PM \${configurationItem.ame} 10.195.7.106
Lexmark C930 Supply Low Black Toner Cleared Warning
 - Nov 15, 2010 5:38:41 PM \${configurationItem.ame} 10.195.7.106
Lexmark C930 Supply Low Black Toner Cleared InterventionRequiredMVE processes them correctly and separately.
 - (PTR389667) A Lexmark C935 will not issue a 'Close Door' alert.
 - (DE983/PTR389664/PTR389667) A Lexmark X792 will not issue a 'Cover Open' alert when the ADF cover is opened and closed.
 - Due to enhanced security restrictions in Windows Server 2003 & Windows Server 2008, instances of Event Manager's Command Destination may fail. By default the Lexmark MarkVision Enterprise Windows Service runs as the *Local System* account. This seems to be the problem, as the OS returns a code of 128 (ERROR_WAIT_NO_CHILDREN). To remedy the situation, the Service must be allowed to run as an *Administrator*; to do so, follow these steps:
 - Navigate to Control Panel->Administrative Tools->Services
 - Stop the 'Lexmark MarkVision Enterprise' service
 - Right click on 'Lexmark MarkVision Enterprise' service and click on 'Properties'

- Go to 'Log On' tab and enable 'This account:' radio button and enter appropriate Administrator-level user credentials
 - Start the 'Lexmark MarkVision Enterprise' service
- Reports
 - If CSV output format is selected for report generation and the resulting CSV file is imported into Excel or Open Office Calc, leading zeros and/or spaces may be trimmed. This is a known issue with any CSV file import into a spreadsheet application. For any numeric field that contains leading zeros, Excel will trim the zeros unless the field is prefixed with an equals sign prior to the double quotation OR the user changes the type of the field during the import process. However, if equals signs are prepended to fields, MVE will be violating accepted CSV format conventions and may lose interoperability with other applications using CSV data.
- Browsers
 - Due to the way Firefox, Google Chrome, Safari, Internet Explorer 9+ and possibly other browsers load flash applications, it is not possible to force the initial focus to be on the password field; the user has to click on the application to give it focus and have the caret appear in the password field.
 - Due to the way Internet Explorer 9+ and possibly other browsers handle shortcuts, special care must be taken to use them within MVE. IE will not pass shortcut key combinations it defines for itself (e.g. CTRL+A) on to Flash applications running within it. To work around this, add the ALT key to the combination (e.g. ALT+CTRL+A). IE does not define this combination so it is passed on to the Flash application.
 - Generic File Download does not work in the Safari browser running on Windows.
- Device Support
 - Lexmark
 - Due to firmware/hardware issues with the Forms 2580/2581/2590/2591 printers, if they boot up in the *Not Ready* state, MVE will be unable to communicate with them. The problem being, the NIC cannot talk to the printer when it's *Not Ready* so it cannot retrieve the Serial Number, which MVE needs in order to successfully discover it. Once the NIC can communicate with the printer, it will cache the Serial Number so subsequent *Not Ready* states will not be an issue (until the next reboot). The printer can come up in the *Not Ready* state for multiple reasons, including if it is out of paper. Pressing the Ready button should remedy the situation.
 - Due to a firmware issue, across multiple models, MVE cannot discover a printer whose SNMP Read Community Name contains a space. To remedy this, make sure the latest firmware is being used. If it still does not work, then the latest firmware does not contain this particular fix; contact

Lexmark.