Markvision Enterprise (MVE) Release Notes (4.3.3)

New and Noteworthy

1. Added the following Lexmark models:

   The new Lexmark 9-Series:
   Lexmark MX953, Lexmark XM9655, Lexmark CS963, Lexmark C9655, Lexmark CX960, Lexmark CX961, Lexmark CX962, Lexmark XC9625, Lexmark XC9635, Lexmark XC9645, Lexmark CX963

   Lexmark CS73x and CX73x:
   Lexmark CS737, Lexmark CX737

   Lexmark XM3146:
   Lexmark XM3146

2. SNMP v3 fields added in Discovery Profile- Context Name and Privacy Password.
3. These three missing SNMP V3 settings have been added in the configuration under network category - SNMP V3 Context Name, SNMP V3 Read only Privacy Password & SNMP V3 Read/Write Privacy Password.
4. Newly added Security Settings in all applicable sections- Configurations, Saved Search, Views and Dashboard Security Information.
   a. Enable Airprint
   b. Enable Mopria Print Discovery
   c. Anonymous Data Collection
   d. Disk Encryption
   e. Allow self e-mails only
   f. Force HTTPS Connections
   g. Domain - Enable Auto Cert Update
   h. Domain - Repeat Cert Update Interval
   i. Enable Password/PIN Reveal
   j. Enable IPP Print
   k. Enable IPP Fax
   l. Enable IPP Over USB
   m. Enable IPP Scan
   n. LES Applications(Enable eSF Framework)
   o. LDAP Certificate Verification
   p. TCP 9198 (PrintCryption)
   q. Enable Optional Parallel Port
   r. Disable Printer Message Access
   s. Page Timeout
   t. Reset Emulator After Job

u. PJL File Access Control
v. USB Scan to Local
w. Enable USB Port
x. Enable Wi-Fi Direct
y. Wireless Security Mode
z. 802.1x Encryption Mode

Bug Fixes

1. After upgrading MVE v4.2 to v4.3, Imaging Unit Levels coming as blank in the printer listing view for printers released prior to 2016.
2. For printers released on or after 2016, TCP 9198 (PrintCryption) setting is unavailable.
3. SNMP V3 discovery profile run hangs having addresses in the search space where there is no printer.
4. Printer or Supply alert returned as blank in case of printers released prior to 2016.
5. MVE 'Help' ? icon link is broken.
6. CVE-2023-24998 is addressed by upgrading Apache Commons FileUpload version's to 1.5.

Known Issues

1. Redundant IndexOutOfBoundsException in DefaultPreferencesService of LSAS log, inside tomcat > logs folder.

2. TLS 1.2 setting must be enabled from Printer. If disabled, MVE would fail to communicate with the printer.
3. There is a problem with “saving” the discovery profile if Privacy parameters for SNMP V3 are included. What is seen that when an Authentication Password is included, but no Privacy Password, the initial save seems to correctly populate. However, if the profile is edited and any other setting is changed and saved it again, the Privacy Password is changed. It looks like this is encoding the asterisks that are included with the obfuscated UI element for that password if it’s left “blank” for it to match the Authentication Password, then saving this to the database. As a work-around, if the printer is configured to have the same password for both Authentication and Privacy, then in the discovery profile be sure to enter the same password for both fields and avoid clicking the Show Password checkbox.
4. SNMPv3 discovery run using Context Name may fail sometimes. It’s a little silly to have Context Name defined for a printer in EWS, though. The context name is used to specify a unique instance of the SNMP engine. Since there’s only one instance of SNMP on the printer and that setting only allows naming one instance, it provides little or no value.
5. Conformance check/enforcement of configuration containing "HTML: Font Name" always fails for FW 22.1 or later in printers released on or after 2016.
6. Configuration enforcement having “E-mail: PDF Compression” fails where this setting is not present in EWS. The EWS field name for it is “Highly Compressed”. The EWS path for that setting is: Settings/E-mail/E-mail Defaults/PDF Settings. Same problem is seen for other PDF Compression settings - Flash Drive Scan: PDF Compression, FTP: PDF Compression & Scan to Doc: PDF Compression. Please note, the conformance check task does not fail.

7. Configuration enforcement having “Flash Drive Scan: TIFF Compression” (value = LZW) fails where this setting is not present in EWS. The EWS field name for it is “TIFF Compression”. The EWS path for that setting is: Settings/USB Drive/Admin Controls. Also, the other 2 settings (i.e. “E-mail User Defaults: TIFF Compression” & “FTP Scan: TIFF Compression”) are not shown as unsupported where these are not present. Please note, the conformance check task does not fail.
8. Configuration conformance/enforcement having "Force HTTPS Connections" fails for printers released in 2010. Please note this setting is actually unsupported on those models.
9. Configuration conformance/enforcement having "Disk Encryption" fails for printers released in 2010. It works okay if the device has a disk but if device doesn't have a disk, it causes the communications error.
10. For MS811, configuration conformance/enforcement having "SMBv3 Enabled" and/or "USB Scan to Local" and/or "LES Applications(Enable eSF Framework)" always fails.
11. For CS310, conformance check/enforcement fails if configuration contains "Display Info: Left Side Msg" or "Display Info: Right Side Msg" or "Display Info: Custom Text 1" or "Display Info: Custom Text 2" settings.
12. Configuration/Deploy file to printers tasks fail if a shortcut is present in homescreen json inside a VCC bundle, though the shortcut gets deployed on the printer.
13. For MSCEWS protocol, Certificate Authority configuration fails if "Use Kerberos only" is selected under "Trust this user for delegation to specified services only". If it’s set to Use any authentication protocol, then only Certificate Authority configuration succeeds. These settings are present in CES service account properties window inside Active Directory.
14. Custom View's order of columns takes the previously selected view's order in Printer Listing page.
15. An Advanced Security Component cloned from a printer using the Internal Accounts Building Block and multiple internal accounts will be read from a printer correctly. Once the various passwords are added and the component is saved, it becomes assignable. However, no changes to this component are saved despite appearing as if the Save Changes button records these.
16. MVE does not identify any local accounts or other security settings that are outside of the advanced security component. This means it's possible for there to be a "back door" account on the printer, and the admin will have no way of knowing this because MVE won't flag that as out of conformance.
17. The key, “configuration.enforcementOrder.ucfVcc.beforeDeviceSettings” in the platform.properties file of the MVE installed directory takes care only Basic settings, not Advanced Security of the configuration.
18. Enforcing configuration with advanced security component can change the saved authentication mechanism. For example, if there are two username/password accounts in the device and advance security is cloned from it, then under local account tab the ORDER of account decides which one will be enforced as security credential. If order is B, A then always B will get enforced as authentication mechanism and will be visible in Security dropdown, even if in cloned configuration’s Printer Credentials tab, it was A.
19. If user clones an Advanced Security Component from a CAESAR2_LITE model, that component will show in the "Full account based authentication" list apart from showing in “Partial account based authentication”. Now, if the user selects that component from the Full Account Based Authentication list, that component will not be enforced to a CAESAR2_LITE printer. The same scenario is applicable for CAESAR1_LITE printer.
20. Advanced Security Component type of the Partial account based authentication printers (e.g., B3340, B3442, MS331, MS431, MB3442, MX331, MX431, MB3442, MX331, MX431, C3426,

CS431 etc.) gets changed to Full account based authentication after export and import it back. This problem is not seen for the built-in component, "Simple account-based authentication".

21. When the Lexmark Cloud Printer Configuration Agent is installed on a printer, it creates a Username/Password account with a randomly generated password. This password is not known to the customer. If a user would like to manage printer security settings in an Advanced Security Component using MVE, these settings are cloned from the printer. Unfortunately, since there is no known password, there is no “valid” way for a user to create that component (it will not ‘complete’ unless the password is added). If the user inadvertently assigns what he/she thinks is the correct password and then enforces this security configuration to their fleet, all connectivity to the cloud will fail as a result of this.
22. With a printer released on or after 2016 that has security enabled and has an SNMP Read/Write User/Password assigned, when a credential is assigned to the device and the printer is Audited, this is successful. However, if the printer is rebooted, the Audit will fail. Also, without the reboot, this problem is seen after a certain interval depending on the printer model.
23. If user assigns a configuration to a printer, then enforce this successfully, the Conformance State is set to "In Conformance". If something creates a problem (network loss, printer powered off, import a security bundle to change the credentials, etc.), a conformance or enforcement that shows in the task log as "failed" will not change the Conformance State, i.e., it remains at "In Conformance".
24. From discovery profile Use SNMP dropdown, if “Version 3” is selected and “No authentication, no privacy” is selected in the Authentication level, then also the Read/write user field remains mandatory. If a random value is also put to save the profile, discovery will always fail as the user name won’t match with the EWS.
25. At installation time, if multiple network adapters are detected the user is presented a dialog that allows the selection of the active interface, or one of the specific adapters (chosen by IP address). The user's selection is written to the platform.properties file, but incorrect key is being used here. As a result if user selects any specific adapter value, then it won’t be got effective.
26. MVE silent installer does not work with serviceRunAsUsername; it only works for LOCAL SYSTEM.
27. If a View is created using all columns, then Printer Listing page throws 500 internal error in UI. If Export Data is performed for that view, exported file contains only the column headers, but no data.
28. "SMTP: Use Default Reply Address" is shown as unsupported against conformance check/enforcement for printers released in 2010, 2012 & 2014.
29. General setting “Remote Operator Panel: Authentication Type” is a problematic one in printers released on or after 2016, e.g. on a conformance/enforcement check, its value “VNC Password Authentication (Standard)” is shown as “This value is not supported for this model”.
30. "Remote Operator Panel: VNC Password for standard authentication" is a problematic one for printers released on or after 2016. Its value is not getting deployed upon configuration enforcement.
31. The Schedule USB devices section/setting in MVE is missing the ability to Disable Every Day (Mon-Sun) value in all printers.
32. Mono printers released on or after 2016 are missing the Imaging Kit Supply Notification Settings. These are available in a general configuration, but when a mono printer is selected, these settings are no longer available. Color printers released on or after 2016 have different supplies defined for this (Black Imaging Unit, Color Imaging Kit) and these are "unique" to the

printers released on or after 2016. The printers released prior to 2016 share the Imaging Kit settings.

33. Recipient's email addresses (i.e. "E-mail List 1" & "E-mail List 2") and "Subject Text" fields are missing for any supply notification settings.
34. In EWS page of printers released on or after 2016, go to Settings > Device > Notifications > E-mail Alerts Setup > Setup E-mail Lists and Alerts. Pre-requisite is SMTP gateway has to be configured. Then under E-mail Events, following settings are missing in configuration:
    a. Cartridge Nearly Low
    b. Cartridge Very Low
    c. Photoconductor Nearly Low
    d. Photoconductor Very Low
    e. Developer Nearly Low
    f. Developer Very Low
    g. Imaging Unit/Kit Nearly Low
    h. Imaging Unit/Kit Very Low
    i. Replace maintenance kit
    j. Fuser Very Low
    k. Waste Toner Missing

    Please note, for Waste Toner Missing, E-mail List 1 is present in MVE configuration, but E-mail List 2 is missing.

35. Under View > Printer Statistics, MVE has the following columns, but these do not show the percentage levels, rather these show the status of the supplies, like OK, Intermediate etc.
    a. Maintenance Kit Supply Level
    b. Maintenance Kit 100k Supply Level
    c. Maintenance Kit 160k Supply Level
    d. Maintenance Kit 200k Supply Level
    e. Maintenance Kit 300k Supply Level
    f. Maintenance Kit 320k Supply Level
    g. Maintenance Kit 480k Supply Level
    h. Maintenance Kit 600k Supply Level
36. The following Maintenance Kit supplies are missing in grid View columns which are applicable for CX92x and some other series, but these are visible in printer details page.
    a. 300K Maintenance Kit
    b. 200K HCF Maintenance Kit
    c. 200K MPF Maintenance Kit
    d. 240K Maintenance Kit
    e. 480K Maintenance Kit
    f. ADF Maintenance Kit, etc.
37. Port Access Web Services is a setting of printers released prior to 2016 that is mapped to or corresponds to the WSD Port 65002. Setting that value to "True" and enforcing causes an Error on printers released in 2010. Setting that value to "False" will allow you to proceed and looks successful, but it doesn't do anything. The correct setting in MVE configuration is "Port Access WSD Print Service (TCP 65002)".
38. There are two close settings in MVE to enable HTTP server - HTTP Enabled & HTTP Server Enabled. It appears that "HTTP Enabled" supports printers released in 2010, 2012 & 2014 and

printers released on or after 2016 whereas “HTTP Server Enabled” supports only printers released in 2010. So, the suggestion is do not use “HTTP Server Enabled”.

39. Setting the "Quality: Toner Darkness (Light [0-2], Normal [3-7], Dark [8-10])" value in a configuration and assigning and enforcing to a printer released on or after 2016 sets the printer's value incorrectly. The value set on the printer is always one greater than the value set in the configuration.
40. All 3-in-1 Models are not supported. The missing list contains, but may not be limited to MB2236i,MB3442i,MC3326i,MC3426i,XC2326i,XC4240i,XM1246i,XM1342i,XM3250i,XM5365i, XM5370i , XM7355bi , XM7355i , XM7370i.
41. If MVE has the email event configured, then email comes for the existing alert condition (e.g. Supply low) which is present in the Managed device, but email contains information about the Missing device, e.g. Model, Serial Number etc.
42. Signed VCC Settings Bundle cannot be imported into resource library. A little bit details about this file - A digitally signed file bears a trusted signor's certificate and a checksum/CRC/hash that represents the contents of the file. If something changed within the file, the calculated representation wouldn't match the signed value and would be flagged as tampered. Some settings within the printer can only be changed with a signed settings bundle file. This could include engine code changes, operation settings values for items within the printer (like a chip on a supply), etc.
43. In an export of the data view, we send this information to a comma delimited file. The field shown for firmware information is a comma delimited list, so this presents a problem for reporting. Also the sorting of this column, firmware information is not done in a consistent way. Currently, the string value of this column is represented as it's retrieved, which can be inconsistent. In some lines, BASE is listed first and in others it could be NETWORK etc.
44. If a printer has a text field that would normally be cloned, and that field contains text that is in the format of a variable setting (e.g. ${Contact_Name}, ${Contact_location}), the clone will fail.
45. If a configuration contains only basic settings, and the settings contained are only to set the various password fields in a printer, that configuration is unenforceable, and the conformance check operation also always fails.
46. MVE has a limitation of 19 characters it can enforce to the SNMP community name of a printer released on or after 2016; 20 characters and it fails. However, the device supports more than 19 characters and the MVE conformance check is also able to exceed the 19 characters. EWS of printers released on or after 2016 supports up to 32 chars. In printers released prior to 2016, EWS supports up to 19 chars.
47. SHIFT + Select i.e. multiselect for checkboxes does not work.
48. Although TCP Port 8000 was removed for printers released on or after 2016 in firmware 070.217, conformance check/enforcement operation using "Port Access HTTP (TCP 8000)" in MVE configuration does not show it as Unsupported.
49. “Context Name” cannot be enforced unless the printer is discovered via SNMP v3 with the existing context name.
50. In printers released prior to 2016, for settings- Wireless Security Mode and its child setting 802.1x Encryption mode- Value WEP is deprecated for being in low security category.
51. In case of Upgrade Scenario (only) Supply Notification Behavior settings have undergone certain changes:
    a. Configurations before 4.3.0 containing Supply Notification settings should be checked for Conformance once after the upgrade regardless of the Conformance state.

    b. Strings “End of Life” & “Near End of Life” in brackets have been added to represent “Replace” & “Very Low Behavior” respectively as applicable for printers released prior to 2016 and printers released on or after 2016.
52. MSCEWS Certificate management will fail if the CA Server Hostname field is populated with a value that is not set as the CN of the CA Server’s certificate. In most cases, the CN is changed from the default value of the server’s hostname.
53. For printers released prior to 2016, the configuration settings for disk wiping do not function.
54. In case of printers released prior to 2016, for Standard USB Buffer setting, Auto (Value = 2) cannot be set and enforced from MVE configuration. The checkbox (Best for Content) corresponds to Disable or Off in printers.
55. Variable settings files cannot be deleted directly from the list shown in the UI. De -select references to the settings file, then remove the settings file from the filesystem of the server hosting MVE.
56. Configurations for some models include both a Quality: Print Darkness setting and a Toner Darkness and Color Saver setting. If not set up properly, these values will conflict, and conformance checks will fail.
57. Changing the NTP server setting does not immediately update the time on the printer. In some cases, a restart of the printer may be required.
58. Licenses are not included in configuration exports.
59. MVE doesn’t support adding applications with trial licenses to the resource library.
60. When LDAP is enabled for authentication with Binding type set to Kerberos and Authentication Type set to Kerberos authentication:
    a. attempts to login to MVE with a valid user that does not have MVE permission will NOT result in a User Log entry.
    b. If the client machine does not include the MVE server in its Local intranet zone, then an attempt to access MVE will result in a login page that will not allow the user to login.
61. An Advanced Security Component containing a network account with LDAP setup is not supported for B3340, B3442, MS331, MS431, MB3442, MX331, MX431, MB3442, MX331, MX431, C3426, CS431.
62. In Automated Certificate Management, automated CRL management for Microsoft CA Enterprise is not supported when using SCEP.
63. Importing versions of Downloadable Emulation (e.g., IPDS, Prescribe, FMBC, etc.) firmware prior to EC 7.2 version 0.30 to the resource library will cause an exception when trying to list available firmware for use in a configuration. This exception prevents any firmware from being selected for use in a configuration until the offending Firmware is removed.
64. For Microsoft Certificate Authority server using the SCEP, the challenge password is not Supported. Recommendation is to use Microsoft Certificate Enrollment Web Service.
65. HTTPS is not supported in Automated Certificate Management using SCEP protocol.
66. Conformance checks fail for MS810 when apps are added as part of a configuration.
67. Enforcement can fail if there are certain eSF apps on the printer. Increasing the timeout and/or retry conditions may help mitigate this problem. Edit the {$INSTALL_DIR}\apps\dm-mve\webinf\classes\transportParameter.properties file and add the values:
    a. npa.offline_mode.retries = 5
    b. npa.online_offline_polling_interval = 5000 (value in ms) [increase this value in increments of 1000, (i.e., 5 seconds = 5000)]
68. Some tasks might appear to get stuck at 99% although the task is complete. A restart of the MVE service will resolve this.

69. When executing MVE as a run-as domain user, passwords containing some combination of " (double quote), < > (angle brackets) might fail.
70. In some cases when upgrading to 4.2 or 4.3, if keywords are assigned to printers, attempts to delete a keyword can cause a “500 internal server error”. To work around this problem, delete and re-create any existing discovery profiles after upgrading.
71. The system provided Printer List View appears in the Views list but is not directly selectable in the main Printers UI. It can be selected for data export and can be copied to a new user created view.
72. Sorting a custom view that contains Tray n columns may cause a “500 internal server” error when clicking on the Tray n header to sort the data.

Browser Quirks

Safari doesn’t support the task badge showing the number of running tasks on the server.