Markvision Enterprise (MVE) Release Notes (4.5.1)

New and Noteworthy

1. New model support for Lexmark XC2342, Lexmark M3346, Lexmark XM3346, Lexmark XM3146
2. Added support for Form Based Authentication.
   Note:
   Onwards MVE 4.5.x please use "//<ipaddress>/mve" to login.
   Introduced support for form-based authentication onwards MVE 4.5.x., so "/mve" path will automatically redirect to MVE login URL page, ensuring MVE to be more secure.
3. During the MVE installation process, SQL is selected, with added support for authentication through Group Managed Service Accounts (gMSA).
4. Obfuscate the "certificateKeystorePassword" in the server xml file.
5. Various library updates, including, but not limited to the following:
   Apache Tomcat v10.1.40
   Spring Framework v6.2.3
   SpringBoot v3.4.3
   Hibernate v6.6.11
   Apache Groovy v4.0.15

Bug Fixes

1. Fixed the issue showing "IP Restricted Server List" and "Remote Operator Panel: Enable (External VNC Connection)" showing incorrectly as Unsupported during conformance check/enforcement for the new Mono and Color A3, Color 8xx products.
2. Fixed the issue in upgrade scenario with MVE 4.4.x where the "CertificateKeyAlias" value in server.xml gets changed to default "mve" after upgrade from earlier versions.
3. Addressed issue for System Log cleanup task hang.
4. Fixed issues with system name and host name with combination of upper case and lower-case sensitivity in saved search criteria with Firebird DB.
5. Addressed issues to include the missing recipient email addresses aka"E-mail List 1" & "E-mail List 2" and "Subject Text" fields for any supply notification settings.
6. Resolved the issue when getting "500 Internal Server Error" after a few seconds, while attempting to edit a configuration linked with a discovery profile.
7. Fixed the upgrade issue with MVE 4.4.x from MVE earlier versions when the SSL port configured as custom port other than default port 443.
8. Addressed the audit failure issue if the signed certificate is present on the device.
9. Resolved the RIP FW crash issue while audit is performed with printers using firmware at or below 230.307.
10. Addressed the issue to show the setting "Job Accounting: Disk Near Full Level (MB)" as unsupported settings correctly during conformance check, with those printers that don't support the setting (e.g.: CX625ade, CX625adhe and CX625de etc.)
11. Fixed the issue with deleted keyword causing "500 Internal Server Error" in the upgrade path.
12. Addressed issue when editing a discovery profile with SMNPv3 with Authentication level set to "no privacy" that causes a "400 error".

13. Audit failure in MVE 4.5 in printers released prior to 2016 is resolved.

Known Issues

1. For automated certificate management with MSCEWS protocol, user must create and publish a certificate template with a Certificate Recipient version 3 or lower. Templates with version 4 or higher will not work due to a limitation in Microsoft CEP server design.
2. Certificate defaults settings are not supported for printers released prior to 2016.
3. Certificate Authority goes into invalid state after MVE upgrade. Workaround is to click on save changes and validate in the MVE System Configuration.
4. Known issues related to Conformance/Enforcement
    a. Conformance/enforcement will fail when a variable settings data file includes a HOSTNAME used as printer identifier and there is a mismatch related to case (i.e. upper or lower) between the user provided hostname and the MVE fetched hostname.
    b. A communication error will occur if a conformance/enforcement operation is run with a Configuration that includes the disk encryption setting selected, but the device(s) does not including a hard disk. This affects devices released in 2010.
    c. When conducting a conformance check for a configuration that includes the deployment of a no-app license bundle and results an Out of Conformance status, no Out of Conformance table appears. The enforcement operation works properly.
5. For the MSCEWS protocol, Certificate Authority configuration fails if “Use Kerberos only” is selected under "Trust this user for delegation to specified services only". If “Use any authentication protocol” is used, the Certificate Authority configuration succeeds. This setting is in the CES service account properties within Active Directory.
6. Enforcing a Configuration that includes an Advanced Security Component can change the order of the saved authentication mechanisms.
7. If an Advanced Security Component is cloned from a current small workgroup device, this template will show in the "full account-based authentication" list apart from showing in the “partial account-based authentication” list. If this template is selected from the full account-based authentication list, it will not be applied to a small workgroup device.
8. MVE silent installer does not support using serviceRunAsUsername; it only supports LOCAL SYSTEM.
9. If the SNMPv3 passwords are modified on the device, the MVE discovery profile will need to be updated, and the associated devices will need to be deleted and rediscovered in MVE.
10. Any changes to the SNMPv3 form will require the reentry of the SNMPv3 passwords.
11. When creating a discovery profile after generating a view for a device conformance check, the side bar links may not work correctly, and scrolling the page may cause the window to flicker. The workaround is to clear the browser cache.
12. While exporting FW24 (mega firmware files) from MVE may take longer time to complete the task depending upon the exported file size which can be around 50GB (eg like MXTGM.240.229 which supports more than 30 models). The workaround would be to add the firmware file into the resource library.
13. Audit task with SNMPv3 protocol will fail on FW 22.1. This is a firmware issue. The FW recommendation is to is to update to at least FW 23 (230.408) and FW 24 (240.207) which are the iEC web releases for both FW23 and FW24 having the fix for the issue.

14. Audit doesn’t fetch Disk Encryption value in case hard disk is present for printers released in 2012 & 2014. Hard disk parameter comes under Capabilities.
15. Enforcement fails to change value from disable to enable, of setting "Disk Encryption" in case hard disk is present for printers released in 2012 & 2014.
16. FAX server settings are shown as Unsupported for the new 9-series models - Lexmark MX953, Lexmark XM9655, Lexmark CS963, Lexmark C9655, Lexmark CX960, Lexmark CX961, Lexmark CX962, Lexmark XC9625, Lexmark XC9635, Lexmark XC9645, Lexmark CX963
17. Currently in the installer for MVE 4.5, the translations for the new option to select the “gMSA Authentication” and the associated messaging is currently translated in English only.

Browser Quirks

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