Markvision Enterprise (MVE) Release Notes (4.6.0)

New and Noteworthy

1. Added new model support for Lexmark CX950, Lexmark CX951, Lexmark MX953, Lexmark XC9525, Lexmark XC9535
2. Added support for Windows Server 2025
3. Upgraded built-in Firebird® database to v5.0.3.1683_0_x64.
4. Added ability to configure the ca.onbehalf.keysize parameter in the platform.properties file to support custom key lengths for validating Signer-on-Behalf certificates. (default: 2048, supports 4096+).
5. Simplified process to update the custom TLS keystore password in the tomcat server.xml
6. Component and library updates, including, but not limited to the following:
   Apache Tomcat v11.0.13
   Spring Framework v6.2.14
   SpringBoot v3.5.8
   Hibernate v6.6.18
   Liquibase v4.31.1
   Zulu Open JDK v17.0.17

Bug Fixes

1. Fixed an issue on the printer listing page when clicking on "Hide" in filters makes the screen go blank.
2. Fixed an issue when enforcing a configuration that includes Advanced Security and a VCC bundle, where security settings were not honored.
3. Lexmark_PCA_User app is not being cloned during a settings clone operation.
4. When hostname is used as printer identifier, addressed an issue with variable setting data file lookup (CSV) being case-sensitive.
5. Fixed an issue with the Event Manager role where a logout was triggered after clicking on a secured legacy device.
6. Fixed an out of conformance issue where MVE treats the CSTGV & CSNGV firmware files differently, although the latest mega firmware files were used.
7. Fixed an issue when enforcement fails for Port Access Telnet & Port Access XML.
8. Fixed issue when sorting view with tray sizes causes a 500 Server Error.
9. Fixed issue when port status returned as unknown instead of unavailable.
10. For legacy printers, addressed an issue when a printer or supply alert returned as blank.
11. Addressed an issue when a signed VCC settings bundle could not be imported into the resource library.

Known Issues

1. When using the Firebird DB and upgrading from MVE 4.3.x or MVE 4.4.x to MVE 4.6 it is required to upgrade to MVE 4.5.1 first, to avoid any upgrade issues.
2. For automated certificate management with MSCEWS protocol, the 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.
3. Certificate defaults settings are not supported for printers released prior to 2016.
4. Certificate Authority goes into invalid state after MVE upgrade. Workaround is to click on save changes and validate in the MVE System Configuration.
5. Known issues related to Conformance/Enforcement
    a. A communication error will occur if a conformance/enforcement operation is run with Configuration that includes the disk encryption setting selected, but the device(s) does not include a hard disk. This affects devices released in 2010.
    b. 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.
6. 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.
7. Enforcing a Configuration that includes an Advanced Security Component can change the order of the saved authentication mechanisms.
8. 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.
9. MVE silent installer does not support using serviceRunAsUsername; it only supports LOCAL SYSTEM.
10. 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.
11. Any changes to the SNMPv3 form will require the reentry of the SNMPv3 passwords.
12. 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.
13. 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 (Ex. MXTGM.240.229 which supports more than 30 models). The workaround is to add the firmware file to the resource library.
14. Audit task with SNMPv3 protocol will fail on FW 22.1. This is a firmware issue. The FW recommendation is to update to FW 23 (230.408) or FW 24 (240.207) which are the iEC web releases and include the fix for this issue.

15. If the “mve_encryption.jceks” file is moved to a custom location, the MVE upgrade process will fail. The workaround is to copy the encryption file to the default location, /Lexmark/mve_encryption.jceks.
16. When using ADFS as the authentication mechanism for MVE, if MVE is being accessed via its hostname, it uses the IP address for the redirection URLs in the SAML ticket.
17. When using ADFS to login to MVE, the public certificate won’t get downloaded if MVE’s truststore file (Ex. mve_truststore.p12) does not reside in the \Lexmark folder.
18. Currently, MVE does not support these parameters in the discovery profile for SNMPv3 (SHA-2 (Hash) and AES-256 (Privacy algorithm)). As a result, device discovery’s will be successful, however, other operations such as audit, enforcement, etc.
19. CS963 or CX96x series printers support statement as a valid paper size. MVE shows this value as inapplicable when configuration enforcement is performed.
20. If a configuration is created and enforced to update both the PCL Font Name and Font Pitch on devices, the Font Pitch is successfully updated, but the Font Name remains unchanged on the device despite MVE reporting the task as successful and the device as "In Conformance”.
21. Firmware updates are not completed for devices released in 2012 and 2014. Intermittently, the task is completed, but the FW package is not deployed to the noted printers.

Browser Quirks

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