Markvision Enterprise (MVE) Release Notes (4.4)

New and Noteworthy

1. Various library upgrades, including, but not limited to the following:
   a. Java 17
   b. Spring Framework 6.0.23
   c. Spring Boot 3.1.5
   d. Hibernate 6.2.2
   e. Apache Tomcat 10.1.28
   f. Apache Groovy 4.0.15
2. Added IPv6 support
3. Added TLS 1.3 support for MVE to device secure communication.
4. Added support for the Auto check for updates – "Update Firmware from Server: Auto Update" setting. Requires device firmware version 230.039 or newer.
5. Added support to view the Downgrade Firmware Supported value in the firmware section of the printer details page. Requires device firmware version 230.307 or newer.
6. Added support for the following two settings – Certificate Defaults - Common Name and Certificate Defaults - Subject Alternate Name.
7. Added support for the following network settings - Enable LLDP and 2 general settings – Show Echo Key and TTM Tray Configuration.
8. Added support for deploying no-app license bundles via deploy file to printers.
9. HTTP access security enhancements
   a. For new installs, non-secure HTTP access (i.e. port 9788) has been removed from non-localhost connections.
   b. For MVE upgrades, stop the MVE service, add the following string ***address="127.0.0.1"*** into the non-SSL HTTP/1.1 connector of server.xml ("<install location>\Lexmark\Markvision Enterprise\tomcat\conf\ server.xml") and then restart the MVE server.

Bug Fixes

1. An Advanced Security Component using the internal accounts building block and multiple internal accounts is cloned correctly from the device.
2. On the printer listing page, the order of the custom views columns uses the previously selected views.
3. LSAS log improvements related to redundant IndexOutOfBoundsException in DefaultPreferencesService.
4. No-app license bundle deployments via enforcement through configuration path.
5. SMTP: Use Default Reply Address is shown as unsupported against conformance check/enforcement for printers released in 2010, 2012, and 2014.
6. Configuration/Deploy file to printer's task fails if a shortcut is present in the VCC bundle-homescreen.json, however, the shortcuts are still applied to the device.
7. Conformance/enforcements will fail on MVE Configurations that include the "Force HTTPS Connections" on devices released in 2010.
8. For OEM, audits will fail when using certain versions of firmware.

9. When creating a configuration for printers released in 2012 & 2014, the toner darkness settings may fall outside of the normal parameters.
10. Devices launched in 2016 and newer that have security enabled, SNMP read/write credentials assigned to the device, and the printer is audited, the operation is successful. However, if the printer is rebooted, the audit fails.
11. Corrected a misspelling in the tomcat server.xml for the element compressableMimeType.
12. 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.
13. For devices launched before 2016, Standard USB Buffer setting, Auto (Value = 2) cannot be set and enforced from an MVE configuration.
14. For an MS811, the configuration conformance/enforcement operation fails when selecting "USB Scan to Local" and/or "LES Applications (Enable eSF Framework)".
15. Addressed issue related to the secure e-mail feature using SSL & STARTTLS encryption.
16. MSCEWS certificate management feature is unable to fetch templates after selecting save and validate.
17. For devices released before 2016, the following settings are cloned and reflected in the conformance table, but enforcement is unsuccessful: 802.1x encryption mode, LES applications (enable eSF framework) and wireless security mode.
18. Addressed an issue when saving a discovery profile that includes the SNMPv3 privacy password. As a work-around, if the printer is configured to have the same password for both authentication and privacy in the discovery profile, enter the same password for both fields and avoid clicking the show password checkbox.
19. For the CS310, conformance/enforcement fails if the configuration contains Display Info: Left Side Msg, Display Info: Right Side Msg, Display Info: Custom Text 1, or Display Info: Custom Text 2 settings.
20. Corrected non-translated strings for discovery profiles and update status in non-English languages.

Known Issues

1. Certificate Authority goes into invalid state after MVE upgrade. Workaround is to click on save changes and validate in the System Configuration.
2. 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 include a hard disk. This affects devices released in 2010.
    c. For the MS811, conformance/enforcement operations will fail with Configurations that include SMBv3 Enabled.
    d. IP Restricted Server List is shown as unsupported against conformance check/enforcement for the new Lexmark 9-series devices (CX96x, CX83x etc.) and for devices using FW22 and newer.

e. 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.

3. 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.
4. Enforcing a Configuration that includes an Advanced Security Component can change the order of the saved authentication mechanisms.
5. 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.
6. MVE silent installer does not support using serviceRunAsUsername; it only supports LOCAL SYSTEM.
7. When upgrading to MVE 4.x, if keywords are assigned to printers, an attempt to delete a keyword may cause a 500 internal server error. The workaround is to delete and re-create any impacted discovery profiles after the upgrade.
8. 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.
9. Any changes to the SNMPv3 form will require the reentry of the SNMPv3 passwords.
10. 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.
11. When opening a previously created saved search, the System Log Cleanup task and a SYSTEM task may hang intermittently. The workaround is to restart the MVE service.

Browser Quirks

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