Markvision Enterprise (MVE) Release Notes (4.0)

New and Noteworthy

- Common Device Settings Configuration – Printer model specific configurations are no longer required to configure device settings. Model specific settings may still be accessed within the configuration.
- Added support for Custom Database names; FRAMEWORK, MONITOR, QUARTZ not required.
- Added support for Microsoft SQL Server 2019.
- Out-of-conformance items now include the setting category in Single Printer View.
- While deploying Firmware, the task status is set to warning until complete.
- Add the ability to upload UCF/VCC settings files to resource library.
- Include link to documentation in MVE's User Interface (requires internet access).
- Add pre-populated Advanced Security Configuration for Partial Template based authentication.
- Add ability to change database port and/or instance name in password utility.

Bug Fixes

- MVE Console Page spins/constant load if browser closed without logging out.
- Improper permissions for members of Configuration group causing abrupt log out.
- Max-Email Size & Limit Text values fail conformance checks in some cases.
- Multi-Purpose Feeder Paper Type settings fail for some printers
- Fail to clone security settings for legacy device when LDAP setup name has dot (.) in it
- Enhance MVE Certificate Signing Requests generated from UI.
- SMBv3 setting not supported on legacy Devices.
- Missing 2-sided option for Finishing Sides Duplex in some configurations.
- Added missing settings for E-mail Alerts.
- Added missing Erase Temporary Data File Setting.
- Added missing 'Remote Operator Panel' settings.
- Added missing settings for TCP/IP ports: WS-Discovery, WS-Eventing
- Added missing printer network setting 'Force HTTPS Connections'
- Added missing Settings for printer's Country/Region
- Added missing Settings for "Protected Features" in CX923
- Fixed incorrect Custom Supply Message settings
- Fixed incorrect Color Cartridge custom message settings
- Clarified MVE's LDAP setup settings
- Added missing Access Controls enabled by updated firmware
- Added missing TLS 1.0, TLS 1.1 settings
- Fixed conformance error when enforcing 'Enable Drive Option' setting
- Fixed incorrect name of Fax Mode setting.
- Application setting Use Reverse DNS Resolution not honored with audit or discovery

Known issues

- Some versions of firmware for printers released 2016+ with Fax support will remove the Fax Security Function Access Control and permissions if the Fax Mode is set to disabled and the printer is restarted. This can cause enforcement or conformance checks for configurations with the Fax FAC enabled to fail.
    - Firmware fixes for this issue are available in 073.232 or higher.
- 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.
- Configurations for some models include both a Quality: Print Darkness setting and a Toner Darkness and Color Saver setting. If not setup properly, these values will conflict, and conformance checks will fail.
- 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.
- Licenses are not included in configuration exports.
- When LDAP is enabled for authentication with *Binding type* set to *Kerberos* and *Authentication Type* set to *Kerberos authentication:*
    - attempts to login to MVE with a valid user that does not have MVE permission will NOT result in a User Log entry.
    - 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.
- 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.
- In Automated Certificate Management, automated CRL management for Microsoft CA Enterprise is not supported.
- 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.
- For Microsoft Certificate Authority server, the challenge password is not supported.
- HTTPS is not supported in Automated Certificate Management using SCEP protocol.
- Authenticating with e-mail servers from MVE using HTTPS is not supported.
- Conformance checks fail for MS810 when apps are added as part of a configuration.
- 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\web-inf\classes\transportParameter.properties file and add the values:
    - npa.offline_mode.retries = 5
    - npa.online_offline_polling_interval = 5000 (value in ms) [increase this value in increments of 1000, (i.e., 5 seconds = 5000)]

Browser Quirks

- At times IE11 will prevent users from downloading files from MVE. In these cases, you may need to enable file downloads in your security settings.
- Safari doesn't support the task badge showing the number of running tasks on the server
- When editing a view in IE11 any column added to the view remains in the possible columns list.