

Markvision Enterprise (MVE) Release Notes (4.4.2)

New and Noteworthy

1. New model support for Lexmark CX950, CX951, MX953, XC9525, XC9535.
2. Additional debug logging for the MSCEWS certificate configuration process

Bug Fixes

1. Addressed save search issues with firmware level information and hostname.
2. Corrected: For MS811 and similar non-eTask models, configuration conformance/enforcement having "SMBv3 Enabled" fails.
3. Corrected: Configuration enforcement for setting "E-mail: PDF Compression" value = high, as inapplicable value.
4. Corrected: Unable to upload Firmware 24 into MVE resource library. (Ex. Firmware version 240.205, etc.)
5. Addressed variable setting support for certificate defaults for printers released on or after 2016.

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. Attempting to edit a configuration linked with a discovery profile displays a "500 Internal Server Error" after a few seconds.
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. 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. 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. 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.
11. 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.
12. Any changes to the SNMPv3 form will require the reentry of the SNMPv3 passwords.
13. 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.
14. The System Log Cleanup 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.