



Mobile Content Management (MCM)

Solution must employ advanced DRM capabilities for shared downloaded files and folders in the following forms:

- ✓ Downloaded Protected: Full Access
- ✓ Downloaded Protected: Edit, Copy, and Print
- ✓ Downloaded Protected: Edit and Print
- ✓ Downloaded Protected: Print
- ✓ Downloaded Protected: Edit 4
- ✓ Downloaded Protected: View
- ✓ Online View: Full Access
- ✓ Online: view and print Online: view
- ✓ Online: Spotlight view (prevent surreptitious photo taking)

- Support for installation and operations in VDI environments
- Solution must support different user/security group roles, such as visitor, contributor, and owner
- Admins can create different roles based on security requirements
- Solution must support watermark and annotation of Office and PDF documents
- The watermark should show the user's email address and IP address of user and all shared documents.

Solution must support advanced logging of all files and folders with detailed actions:

- ✓ email
- ✓ activity details
- ✓ date location
- ✓ device ID
- ✓ IP address

- Administrators must be able to set an expiration date for all shared files or folders for online and/or offline users.
- Solution must employ built-in protection against Ransomware without the required third-party add-ons or agents for all files and folders with versioning for protected files.
- Users should be able to lock any shared file for a specified period of time with the ability to notify users and unlock your computer at any time for shared documents offline and online.
- Users can open and edit shared files and folders in a secure, proprietary browser built into the solution.
- Admins must be able to revoke access and permissions to any shared file and folder online or offline.

