MOBILE IRON

By implementing the security policies and configurations provided by MobileIron, administrators can apply enhanced protections to mobile devices in use across the enterprise. Enterprises can choose the combination of security policies and configuration that they want MobileIron to apply on your device. These settings help organizations add additional security around apps that handle sensitive data.

There are three kinds of security policies available on MobileIron to help administrators prevent data leakage.

- Copy and Paste: This policy is used to either allow or disallow users from copying and pasting content to and from an app managed by MobileIron.
- Print: Using this policy, administrators can set whether users are allowed to print content from an app managed by MobileIron. When you disallow this privilege, no data can be printed from the app.
- Open in: This policy is used to determine where users can open files in specific apps managed by the MobileIron VSP. The administrator can choose to allow users to open files in all apps, apps that are managed by MobileIron, or apps in a white list.

Capabilities and benefits

PROVISIONING AND AUTHENTICATION

Adds an additional EMM-specific authentication, e.g. PIN with configurable security settings. This is in addition to the authentication required by the MicroStrategy application.

DATA LEAKAGE PREVENTION

Controls to govern whether data can be transmitted, shared, or copied outside of the application ecosystem.

APPLICATION ECOSYSTEM

Allows data to be transmitted to other applications in the EMM ecosystem (i.e. other applications that are integrated with the EMM SDK) in a secure manner.

TUNNELING

Uses a secure channel or gateway provided by the EMM platform to transmit data from client to server.

DATA ENCRYPTION

Ensures that all persisted data are automatically encrypted on the device.

MicroStrategy