mobileiron

Federal information processing standard (FIPS 140-2) compliance in MobileIron Core

Federal information processing standard (FIPS 140-2) compliance in MobileIron Sentry

Federal information processing standard (FIPS 140-2) compliance in Mobile@Work for iOS

Federal information processing standard (FIPS 140-2) compliance in Mobile@Work for Android

Federal information processing standard (FIPS 140-2) compliance in MobileIron Core

The US Federal information processing standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-2 mode, MobileIron Core version 10 (Physical Appliance) and MobileIron Core version 10 (Virtual Appliance) use the FIPS 140-2 approved cryptographic providers:

FIPS 140-2 Module Name	Certificate
Red Hat Enterprise Linux OpenSSL Cryptographic Module (Software Version 5.0)	Cert. #3016
BC-FJA (Bouncy Castle FIPS Java API) (Software Version 1.0.1)	Cert. #3152

Red Hat Enterprise Linux OpenSSL Cryptographic Module

MobileIron affirms that the Red Hat Enterprise Linux OpenSSL Module 5.0 is initialized and operated on the MobileIron Core version 10.0.1.0 (Physical Appliance) and

MobileIron Core version 10.0.1.0 (Virtual Appliance), using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3016

BC-FJA (Bouncy Castle FIPS Java API) Module

MobileIron affirms that BC-FJA (Bouncy Castle FIPS Java API) is initialized and operated on the MobileIron Core version 10.0.1.0 (Physical Appliance) and MobileIron Core version 10.0.1.0 (Virtual Appliance), using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3152

In addition to FIPS 140-2 compliance mode, MobileIron Core meets the NIAP Mobile Device Management Protection Profile v3.0:

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10934

Enabling FIPS compliance on the MobileIron Core

- FIPS mode is OFF by default.
- FIPS mode can be enabled only via the CLI (command line interface) shell interface.

Federal information processing standard (FIPS 140-2) compliance in MobileIron Sentry

The US Federal information processing standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-2 mode, MobileIron Sentry version 9.7 (Physical Appliance) and MobileIron Sentry version 9.7 (Virtual Appliance) use the FIPS 140-2 approved cryptographic providers:

FIPS 140-2 Module Name	Certificate
Red Hat Enterprise Linux 6.6 OpenSSL Module (Software version 4.0)	Cert. #2441
RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software version 6.1)	Cert. #2058

Red Hat Enterprise Linux 6.6 OpenSSL Module

MobileIron affirms that the Red Hat Enterprise Linux 6.6 OpenSSL Module is initialized and operated on the MobileIron Sentry version 9.7 (Physical Appliance) and MobileIron Sentry version 9.7 (Virtual Appliance), using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2441

RSA BSAFE® Crypto-J JSAFE and JCE Software Module

MobileIron affirms that the RSA BSAFE Crypto-J JSAFE Java Cryptographic Module is initialized and operated on the MobileIron Sentry version 9.7 (Physical Appliance) and MobileIron Sentry version 9.7 (Virtual Appliance), using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2058

Enabling FIPS compliance on the Sentry Server

- FIPS mode is OFF by default.
- FIPS mode can be enabled only via the CLI (command line interface) shell interface.

Federal information processing standard (FIPS 140-2) compliance in Mobile@Work for iOS

The US Federal information processing standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-2 mode, Mobile@Work for iOS, Version 10, Docs@Work, and AppConnect SecureApp Manager use the FIPS 140-2 approved cryptographic providers:

FIPS 140-2 Module Name	Certificate
OpenSSL FIPS Object Module SE (Software Version 2.0.16)	Cert. #2398
Apple CoreCrypto Module v8.0 for ARM	Cert. #3148
Apple CoreCrypto Kernel Module v8.0 for ARM	Cert. #3147

The cryptographic operations performed, apply to both data in transit and data at rest. The specific uses of the FIPS modules with the Mobile@Work, Docs@Work, and AppConnect SecureApp Manager applications are specified as follows:

OpenSSL FIPS Object Module SE

MobileIron affirms that the OpenSSL FIPS Object Module SE module is initialized and operated on Mobile@Work, Docs@Work, and AppConnect SecureApp Manager, using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2398

Apple CoreCrypto Module v8.0 for ARM

MobileIron affirms that the Apple CoreCrypto Module v8.0 for ARM module is initialized and operated on Mobile@Work, Docs@Work, and AppConnect SecureApp Manager, using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3148

Apple CoreCrypto Kernel Module v8.0 for ARM

MobileIron affirms that the Apple CoreCrypto Kernel Module v8.0 for ARM module is initialized and operated on Mobile@Work, Docs@Work, and AppConnect SecureApp Manager, using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3147

Enabling FIPS compliance on the Client

- FIPS mode for the above applications is ON by default.

Federal information processing standard (FIPS 140-2) compliance in Mobile@Work for Android

The US Federal information processing standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-2 mode, Mobile@Work for Android, Version 5.x and above use the FIPS 140-2 approved cryptographic providers:

FIPS 140-2 Module Name	Certificate
OpenSSL FIPS Object Module SE (Software Version 2.0.16)	Cert. #2398

The cryptographic operations performed, apply to both data in transit and data at rest. The specific uses of the OpenSSL FIPS Object Module with the Mobile@Work application are specified as follows:

OpenSSL FIPS Object Module SE

MobileIron affirms that the OpenSSL FIPS Object Module SE module is initialized and operated on the Mobile@Work for Android (versions 5.x and above), using the associated FIPS 140-2 security policy as a reference.

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2398

In addition to FIPS 140-2 compliance mode, MobileIron@Work for Android meets the NIAP Extended Package for Mobile Device Management Agents Version 3.0:

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10934

Enabling FIPS compliance on the Client

- FIPS mode is ON by default.