Ivanti U.S. Federal Information Processing Standards Compliance

Ivanti Endpoint Manager Mobile federal information processing standard (FIPS 140-2) compliance

The U.S. 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, Ivanti Endpoint Manager Mobile version 12 (i.e., physical appliance) and Ivanti Endpoint Manager Mobile version 12 (i.e., virtual appliance) uses the FIPS 140-2 approved cryptographic providers listed below:

FIPS 140-2 Module Name	Certficate
Oracle Linux 8 OpenSSL Cryptographic Module	Cert. 4215

Oracle Linux 8 OpenSSL Cryptographic Module

Ivanti affirms that the Oracle Linux 8 OpenSSL cryptographic Module version 1.1.1g-15.el8_3.x86_64 is initialized and operated on the Ivanti Endpoint Manager Mobile version 12 using the associated FIPS 140-2 security policy as a reference.

Ivanti Endpoint Manger Mobile meets the Cryptographic Algorithm Validation Program (CAVP) for Bouncy Castle version 1.0.2.4.

In addition to FIPS 140-2 compliance mode, Ivanti Endpoint Manager Mobile meets the NIAP Protection Profile for Mobile Device Management Version 4.0.

Enabling FIPS compliance on the Ivanti Endpoint Manager Mobile:

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

Federal information processing standard (FIPS 140-2 and FIPS 140-3) compliance in Ivanti Sentry

The U.S. federal information processing standard 140-2 and 140-3 (FIPS 140-2 and FIPS 140-3) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-2 and FIPS 140-3 mode, Ivanti Sentry version 10 uses the FIPS 140-2 and FIPS 140-3 approved cryptographic providers listed below:

FIPS 140 Module Name	Certficate
Oracle Linux 8 OpenSSL Cryptographic Module	Cert. 4215 (FIPS 140-2)
Bouncy Castle FIPS Java API (BC-FJA) Software Version 2.0.0	Cert. 4743 (FIPS 140-3)

Oracle Linux 8 OpenSSL Module I

Ivanti affirms that the Oracle Linux 8 OpenSSL Module version 1.1.1g-15.el8_3.x86_64 is initialized and operated on the Ivanti Sentry version 10 using the associated FIPS 140-2 security policy as a reference.

BC-FJA Module

Ivanti affirms that BC-FJA version 2.0.0 is initialized and operated on the Ivanti Sentry version 10 using the associated FIPS 140-3 security policy as a reference.

Enabling FIPS compliance on the Ivanti Sentry server:

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

Federal information processing standard (FIPS 140-3) compliance in Mobile@Work for Android

The U.S. federal information processing standard 140- 3 (FIPS 140-3) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software.

In FIPS 140-3 mode, Mobile@Work for Android, Version 12.6 and above uses the FIPS 140-3 approved cryptographic provider listed:

FIPS 140-3 Module Name	Certficate
CryptoComply 140-3 FIPS Provider (Software Version 3.0.0-FIPS 140-3)	Cert. 5040

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 below.

OpenSSL FIPS Object Module SE

Ivanti affirms that the OpenSSL CryptoComply 140-3 FIPS Provider module is initialized and operated on the Mobile@Work for Android (versions 12.6 and above), using the associated FIPS 140-3 security policy as a reference.

In addition to FIPS 140-3 compliance mode, Mobile@Work for Android meets the NIAP Protection Profile for Mobile Device Management Version 4.0.

Enabling FIPS compliance on the client:

- FIPS mode is ON by default

ivanti