NetMotion Wireless and 2FA Deliver CJIS-Ready Solutions

Is Your Agency Ready For CJIS Compliance?

To access sensitive information in the nation's Criminal Justice Information System (CJIS), state and local agencies will soon need to comply with the CJIS Security Policy. This means that public safety personnel who access criminal justice information from the field must use advanced authentication (two-factor or stronger) over a reliable, secure mobile network connection.

Forward-looking agencies are deploying turnkey solutions to CJIS compliance requirements with NetMotion Mobility for connectivity and user authentication methods from 2FA ONE. This technology duo provides agency workforces with secure, persistent access to CJIS data and mobile applications while in the field. The two products are certified interoperable and support widely available versions of Windows and Android.

To prepare your network for CJIS compliance, discover the combination of 2FA ONE and NetMotion Mobility. These complementary technologies are helping government agencies simplify authentication, meet CJIS requirements, improve productivity in the field and future-proof their investments as mobility and security continue to evolve.

The combination of connectivity, visibility and control in NetMotion Mobility and advanced authentication in 2FA ONE is strong insurance for your IT personnel tasked with fulfilling the requirements of the CJIS Security Policy.

NetMotion Wireless and 2FA Delivering Secure, Authenticated Connectivity

For mobile deployments requiring high performance, strong security, reliable connectivity and advanced authentication, NetMotion Wireless teams with 2FA to deliver. Together, they ensure that your field personnel are at their most productive while complying with demanding requirements like CJIS. NetMotion Mobility enables secure, remote connectivity with its mobile virtual private network (VPN) functionality designed specifically to keep your users in the field connected, even with all the moving parts and changing conditions of wireless networks.

NetMotion Mobility provides greater performance than native cellular, delivering up to 300 percent faster downloads than its closest competitor and significantly enhancing cross-team collaboration and efficiency of real-time applications like VoIP and video over wireless. Also important, NetMotion Mobility ensures that network sessions persist through any disruption – such as gaps in coverage, power cycles on the device, pauses in the application – then pick up again when the connection is restored. Data transfers resume where they left off, even after days of interruption.

Furthermore, NetMotion Mobility prevents problems and unnecessary risks with Network Access Control (NAC) by allowing you to grant access to applications and sensitive company data only to devices with adequate security measures installed. It also helps to solve problems centrally and improve productivity by prioritizing application access and keeping bandwidth-intensive processes off slower networks.

On real-world networks, NetMotion Mobility successfully transmits data despite packet loss, low signal strength and high latency. Its mobile VPN provides mobile workers with reliable access and it assures IT staff of data-in-flight security with encryption certified to meet the FIPS 140-2 standards, as required by the CJIS Security Policy.

Flexible and Future-Proof Advanced Authentication with 2FA ONE

You need more than a simple user ID and password for CJIS compliance. For Mobile workers who access the CJIS database to do their jobs and ensure public safety, they will need advanced authentication that uses at least two of three factors for identity verification: something they know, like a password; something they have, like a card or token; and something they are, like a fingerprint.

2FA ONE includes all the software, hardware and services needed to fulfill these advanced authentication requirements for CJIS. 2FA ONE lets you select the authentication methods that strike the best balance between convenience in the field and security on your network:

- **Biometric systems – scanning fingerprints**
- **Public key infrastructure (PKI) – recognizing certificates**
- **Smart cards – inserting card to reader or token into USB slot**
- **Software tokens – using one-time passwords (OTP) sent to phone**
- **Hardware tokens – entering OTP from battery-operated token**
- **Risk-based authentication – answering security questions**
- **ID cards – swiping driver's license or agency ID in reader**
- **Proximity cards – tapping RFID badges**

2FA ONE lets you easily set policies and deploy client software to all connected devices and PCs, then enroll users. Besides offering authentication, 2FA ONE offers password management, single sign-on and fast switching among users, and it is the only product that simultaneously supports both primary, token-based authentication and secondary, risk-based authentication.

The flexibility, cost-effectiveness and ease of deployment of NetMotion Mobility and 2FA ONE allow you to meet the needs of the CJIS Security Policy without expensive hardware upgrades to devices in the field or servers in the building.

CJIS-Compliant Security You Can Trust
Delivering Secure, Authenticated Connectivity

LEARN MORE

For more information, or to read about NetMotion Wireless software, please visit **www.NetMotionWireless.com.**

CONTACT US
NetMotion Wireless
TEL 866.262.7626
www.NetMotionWireless.com