

# CJIS Compliance: A Mobile Best Practice Guide

Every law enforcement agency in the U.S. relies on access to Criminal Justice Information (CJI) such as criminal records, fingerprints, driver's licenses, and more. To maintain access to this critical resource, agencies must ensure compliance with the CJIS Security Policy. Specifically, CJIS Security Policy Area 13 outlines specific requirements for protecting mobile devices used in law enforcement.

## **CJIS mobile compliance rule #1: MDM is critical**

The CJIS security policy recommends any law enforcement agency that uses mobile devices to access CJI have a Mobile Device Management (MDM) solution in place. The MDM solution must be able to meet all of the compliance requirements set forth by the CJIS Security Policy. If you don't have an MDM solution, or if you're not sure if your current provider complies with CJIS, now is the time to do some homework. Agencies that are not compliant with the CJIS Security Policy can potentially lose access to CJIS resources. The following chart summarizes the key policies for CJIS compliance on mobile, and how Ivanti supports all of them.



CJIS Policy Area 13 - Mobile Devices	Ivanti Solution
5.13.2 (1) Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.	<ul style="list-style-type: none"> <li>■ <b>For iOS devices:</b> Ivanti iOS restrictions protect data at rest without touching personal data by creating a virtual container on the device. Each app in this container is connected to other authorized apps, so they can easily and securely share CJI data between them.</li> <li>■ <b>For Android devices:</b> Ivanti supports the Android Enterprise Work profile, which containerizes authorized apps on the device. Apps that access CJI can be installed in the secure container, which encrypts the app data and protects it from unauthorized access or sharing outside of the container.</li> </ul>
5.13.2 (2a) Remotely lock lost or stolen devices.	<ul style="list-style-type: none"> <li>■ The Ivanti admin can instantly lock down a device that's lost or stolen. A temporary password lock is placed on the device to prevent unauthorized access. The admin can remove the lock later if the device is located.</li> </ul>
5.13.2 (2b) Remotely wipe data from lost, stolen, or compromised devices.	<ul style="list-style-type: none"> <li>■ Ivanti MDM capabilities can selectively wipe agency data while leaving other apps and data intact on the device. Admins can also choose to wipe the device completely by performing a factory reset of the device, which removes all apps and data. A factory reset is usually chosen when a device is reported as stolen or retired.</li> </ul>
5.13.2 (2c) Set and lock device configurations.	<ul style="list-style-type: none"> <li>■ Ivanti allows admins to set and lock device configurations that can't be removed or modified by the end user. This ensures security policies, such as passcode enforcement, can't be bypassed.</li> </ul>
5.13.2 (2d) Detect "rooted" and "jailbroken" devices.	<ul style="list-style-type: none"> <li>■ Ivanti can quickly detect and quarantine jailbroken or rooted iOS and Android devices. By quarantining the device, the admin can remove email, VPN, Wi-Fi, and CJI data either permanently or until the device is secured.</li> </ul>
5.13.2 (2e) Enforce folder or disk-level encryption.	<ul style="list-style-type: none"> <li>■ Ivanti supports multiple encryption options for individual folders or across the entire device through FIPS 140-2 certified encryption on Android or iOS devices.</li> </ul>
5.13.2 (2f) Apply mandatory policy settings on the device.	<ul style="list-style-type: none"> <li>■ Ivanti admins can configure and enforce a wide range of policies and configurations for iOS and Android. These include policies for automatic device encryption, password complexity, and policies for camera, microphone, or Bluetooth usage. If a device does not comply with these policies, it can be quarantined and access to CJI data denied until the device is compliant.</li> </ul>
5.13.2 (2g) Detect unauthorized configurations.	<ul style="list-style-type: none"> <li>■ Ivanti allows admins to define and push configurations to devices based on device type, user or group, agency- or employee-owned devices, OS version, and other criteria. Ivanti's compliance engine ensures these device configurations cannot be altered or deleted by the end user.</li> </ul>
5.13.2 (2h) Detect unauthorized software or applications.	<ul style="list-style-type: none"> <li>■ Ivanti allows admins to inventory all apps on the device and create app blacklists to prevent users from installing unauthorized software.</li> </ul>
5.13.2 (2i) Locate agency-controlled devices.	<ul style="list-style-type: none"> <li>■ Ivanti can track and identify the location of any managed device, which can help recover a lost or stolen device quickly.</li> </ul>
5.13.2 (2j) Prevent unpatched devices from accessing CJI or CJI systems.	<ul style="list-style-type: none"> <li>■ Ivanti enables admins to quickly see which OS version any managed device is running. Admins can set policies based on OS version and block devices from accessing CJIS resources if the OS is not current or if a vulnerability is discovered.</li> </ul>


CJIS Policy Area 13 - Mobile Devices	Ivanti Solution
5.13.2 (2k) Automatically wipe devices after a specified number of failed access attempts.	<ul style="list-style-type: none"> <li>IT can enforce several actions to meet CJIS requirements, such as wiping a device after a failed number of access attempts.</li> </ul>
5.13.3 (1) Apply available critical patches and upgrades to the operating system as soon as they become available.	<ul style="list-style-type: none"> <li>Ivanti can notify IT about OS version updates and block devices from accessing resources until the latest OS version is installed on the device.</li> </ul>
5.13.3 (2) Configure devices for local device authentication.	<ul style="list-style-type: none"> <li>With Ivanti, IT can: <ul style="list-style-type: none"> <li>Enforce device passcode requirements, including length and complexity.</li> <li>Control access to services based on role, group, organizational unit, or attributes.</li> <li>Manage certificate-based authentication on devices.</li> <li>Enforce multi-factor authentication on devices.</li> </ul> </li> </ul>
5.13.3 (3) Use advanced authentication or CSO-approved compensating controls.	<ul style="list-style-type: none"> <li>Ivanti can provision certificates to mobile devices for authentication with third-party VPN solutions, thus eliminating brute force attacks against remote access accounts. Ivanti also meets two-factor authentication requirements.</li> </ul>
5.13.3 (4) Encrypt all CJI that resides on the device.	<ul style="list-style-type: none"> <li>Ivanti support device PIN/password requirements, which encrypts all data on the device.</li> </ul>
5.13.3 (5) Erase cached information when the session is terminated.	<ul style="list-style-type: none"> <li>Ivanti provides secure access to data even after a session has terminated. However, if the device is out of compliance for any reason, Ivanti can wipe all agency data in order to prevent data loss.</li> </ul>
5.13.3 (6) Employ personal firewalls or run an MDM system that facilitates firewall protection.	<ul style="list-style-type: none"> <li>The Ivanti platform employs a layered security approach. Ivanti's Sentry provides firewall controls that limit access to sensitive resources. To ensure a closed-loop compliance action, when a device falls out of compliance, the secure mobile gateway will block access to the device until it is brought back into compliance. This capability is unique to mobile, and is not something legacy network firewall vendors can provide.</li> </ul>
5.13.3 (7) Employ malicious code protection or run an MDM system that facilitates the ability to provide anti-malware services from the agency level.	<ul style="list-style-type: none"> <li>Through a single app on the device, Ivanti can quickly identify malicious and risky apps and take swift security actions. Depending on the threat level, these actions can include quarantining the device until the threat is remediated. NOTE: Ivanti Threat Defense requires additional licensing</li> </ul>
5.13.4.1 OS Patching and updates	<ul style="list-style-type: none"> <li>Ivanti identifies which OS version a device is currently running and can force an upgrade to ensure the most up-to-date security patches are installed.</li> </ul>
5.13.4.2 Malicious code protection	<ul style="list-style-type: none"> <li>Admins can inventory all apps on the device and ensure that malicious apps are blocked.</li> </ul>

## About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit [ivanti.com](https://www.ivanti.com)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

ivanti®

A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

For more information, or to contact Ivanti, please visit [ivanti.com](https://www.ivanti.com).