Caliber

PUBLIC SAFETY

Protecting Tomorrow–Today.™

Online RMS

Version 11.19.3

Product Change Notice

4 Nov 2025

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	4 Nov 2025	1.0	Service Pack Available

TABLE OF CONTENTS

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.19.3 release of the Online RMS product and will assist with release preparation activities including:

- Internal staff training
- Customer release training
- Customer Release Notes
- Release announcement and promotion
- Online help and eLearning updates
- Updates to web site product information and product collateral

PRODUCT REQUIREMENTS

For best performance and security, we recommend a computer, laptop, or tablet purchased within the last 3 years; running an industry common web browser that is actively supported and updated to the most recent web standards by the browser manufacturer and connecting to the internet by DSL, Cable, or cellular (4G or higher).

Your browser must support the TLS 1.2 security protocol or higher. Browsers running the TLS 1.0/1.1 security protocols have known security vulnerabilities and are no longer supported by Caliber Online RMS. Please make sure your web browser has TLS 1.2 or higher enabled.

IMPORTANT NOTICE FOR ONLINE RMS AGENCIES USING INTERNET EXPLORER (IE)

On August 17, 2021, Microsoft announced that Internet Explorer 11 will no longer work optimally with Microsoft 365 services. Microsoft ended support for the Internet Explorer 11 desktop application for certain versions of Windows 10 on June 15, 2022. Internet Explorer no longer supports new web standards used by modern applications. See Microsoft's website announcement page for more information.

Caliber strongly recommends that you use an industry popular web browser that is supported and updated to the most recent web standards. Caliber is unable to provide support and issue resolutions on web browsers that are not supported and maintained to the most recent web standards.

RELEASE MILESTONES

The following table contains the high-level release milestones for the Online RMS 11.19.3 release.

End Date	Milestone
28 Oct 2025	11.19.3 Code Lock
04 Nov 2025	11.19.3 Service Pack Available

We hope you share our enthusiasm for the production release of Online RMS 11.19.3. Please contact us by email at rms@caliberpublicsafety.com if you have any questions about the release.

Our Very Best,

Caliber Public Safety

APPENDIX: 11.19.3 PRODUCT CHANGE NOTICE (PCN) – DETAILED JIRA LISTING

TABLE A: Release Enhancements and Product Software Issue Resolutions

This table contains enhancement, software issue, and interface JIRAs contained in the 11.19.3 release. An * symbol - denotes a software resolution that was deployed prior to the 11.19.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-81663		Subject: [Carroll County SO/ IN0080000] CAD to Online RMS Mapping	Configuration	Interface	The Online RMS to the Caliber CAD Interface has been configured and enabled for Carroll County, IN.
IA-81678	459659	RMS - McLean Certain users not receiving the Intake Decision from Prosecutor notification	Bug/Defect	Notifications	User notification upload processing has been adjusted to filter for active user accounts.
IA-81700	459295	RMS - ISP Incidents taking a long time to load	Bug/Defect	Incidents	We found a performance issue with loading people associated to incident narratives. We have corrected this and it will result in faster load times for incidents with several narratives that have people associated with them
IA-81334		Data Submission: Incident not removed from the	Bug/Defect	State Submissions	

		open dataset when there are multiple supps, Supp 0 is edited and not approved			
IA-81634		Hybrid Data Exchange - Asynchronous XML Status Update	Enhancement	Interface	Hybrid data exchange upload processing has been modified to be executed as an asynchronous background process.
IA-81739*		Interface Warrant Updates - Audits and Logs	Bug/Defect	Interface	Warrant upload processing has been adjusted to incorporate audit information for changes made through the interface data exchange.
IA-81756*		TN NIBRS: Group B XML does not write Arrest Location details if Field Arrest is associated and arrest address has lat/long	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for Tennessee (TN NIBRS) has been updated to correct an issue with the Group B Arrest Location. In the case where a field arrest is associated to the incident for a person and the address of the arrest contains a valid latitude and longitude. Then this address is used for the Group B TN NIBRS submission. In this case there was an issue with the address id returned, this issue has now been resolved. This update only impacts the TN NIBRS RMS clients.
IA-81763		Hybrid Person Data Exchange - Exclude Unknown	Bug/Defect	Interface	The Hybrid person data exchange has been adjusted to exclude

		Offenders and No Primary			unknown offenders with no name information.
IA-81725		Online RMS- Install script for 11.19.3	DevTask	Admin	
IA-81673		Interface Integration - ARIES Interface to Online RMS for Carroll County (IN8) - JIRA	Configuration	Interface	The ARIES interface has been configured and activated for Carroll County.
IA-81804	460915	PORT - IL NIBRS Victim to offense sequence errors	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for Illinois (IL NIBRS) has been updated to correct an issue with the victim offense associations. In some cases the victim was not associated to the correct offense due to the victims being re-numbered in the XML processing of the Incident for IL NIBRS. This issue was fixed and the Incidents will now correctly associate the offense to the correct victim sequence.

--END--

APPENDIX: SERVICE COMMITMENTS

Caliber Public Safety designs its processes and procedures related to its RMS system based on the service commitments that Caliber Public Safety makes to its business units, the laws and regulations that govern the system and the operational and compliance requirements that Caliber Public Safety has established.

Security, availability, confidentiality, and processing integrity commitments include, but are not limited to, the following:

Security Commitments

- Secure Socket Layer (SSL) FIPS140-2 compliant encryption is used to encrypt the transmission of data with Caliber hosted systems.
- Access to customer data is restricted to Caliber employees and/or subcontractors whose job function requires access.
- RMS Development, operations, and customer service personnel are required to maintain active CJIS certification.
- Systems are subject to vulnerability scanning.

Availability Commitments

- Caliber will maintain a highly available platform (99.9% uptime) that includes redundancy for critical system components except during planned downtime as communicated to users or unplanned downtime caused by circumstances beyond its reasonable control. In practice, Caliber routinely exceeds 99.99% uptime.
- User entity data is backed up daily and replicated to a secondary location.
- User entity data is maintained and stored within the United States.

Confidentiality Commitments

- Upon termination of services, Caliber will return confidential data to customers subject to the terms of the current RMS SaaS agreement.
- Caliber shall protect information designated as confidential from unauthorized access.
- Confidential data shall only be stored within Caliber’s company information systems.

Processing Integrity Commitments

- The organization communicates requirements to user entities regarding the information, data, or other specifications necessary to complete processing in alignment with standard business operations.
- Data processing requests are only performed as authorized by the user entity.
- Data shall be stored and maintained in the system with no unauthorized alteration.