



Protecting Tomorrow–Today.™

Online RMS

Version 11.17.3

Product Change Notice

4 March 2025

REVISION HISTORY

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

TABLE OF CONTENTS

Revision History 1

Introduction 3

Product Requirements..... 4

Release Milestones..... 5

Appendix: 11.17.3 Product Change Notice (PCN) – Detailed JIRA Listing 6

 TABLE A: RELEASE ENHANCEMENTS AND PRODUCT SOFTWARE ISSUE RESOLUTIONS..... 6

Appendix: Service Commitments 9

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.17.3 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 11.17.3 release.

End Date	Milestone
25 Feb 2025	11.17.3 Code Lock
04 Mar 2025	11.17.3 Service Pack Available

We hope you share our enthusiasm for the production release of Online RMS 11.17.3. Please contact us by email at rms@caliberpublicsafety.com if you have any questions about the release.

Our Very Best,

Caliber Public Safety

APPENDIX: 11.17.3 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 11.17.3 release. An * symbol - denotes a software resolution that was deployed prior to the 11.17.3 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-80494	450461	IL NIBRS Zero report getting errors file structure incorrect on submission	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for Illinois (IL NIBRS) has been updated to generate an ILNIBRS Zero Reporting segment in the correct format required by the state of Illinois. Illinois has a specific structure and values that are required for a successful zero segment submission that the Online RMS now uses. This change only impact RMS clients from Illinois using IL NIBRS.
IA-80526		Boomi Integration - McLean	Enhancement	Interface	The Online RMS has updated the RMS Hybrid processing to provide the functionality for Arrest transactions to be sent via Boomi to an external system. This

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					functionality is implemented in Mclean County, IL. To transfer arrest data from the RMS upon approval to an external Jail system. This Jira allows the client system to be configured to use a Boomi OAuth2 token for authorization and pass the arrest XML in RMS format through Boomi to the external jail system. This functionality is only being configured and deployed for Mclean County, IL, but could potentially be used for other clients using a Boomi Arrest Interface.
IA-80544		CAD to Online RMS Interface Set Up JIRA for Danville PD (VA107)	Configuration	Interface	<p>The Online RMS to the Caliber CAD Interface has been configured and enabled for the Danville Police Department, VA.</p> <p>The client is scheduled to go live with the interface on 3/4/2025</p>
IA-80626		Add 50th Anniversary Image to product splash screen	Enhancement	Other	
IA-80648		Online RMS- Install script for 11.17.3	DevTask	Admin	

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-80523	451156	ODL - Log cannot be edited	Bug/Defect	ODL	The query we used to determine if the officer has access to edit an officer daily log was not taking master officer id into consideration. So if a log was made by an officer and then they got their officer information archived, an error would be thrown when editing the log.
IA-80704		Allow the Location to be a Redaction Option on an Incident Report	Enhancement	Incidents	Added Redact Incident Locations print option to the Incident Print. Also went ahead and defaulted it to checked for the Media Template. Selecting this option will remove the Incident Location Section and Additional Locations section.
IA-80718		Federal NIBRS XML submission	Bug/Defect	State Submissions	Federal NIBRS XML submission - DataSetHeaderFileMessage the parameters order in the constructor have been updated.
IA-80726		Crash XML Submission	Bug/Defect	State Submissions	Crash - XML should have CrashAtIntersectionWith = false if distance is provided

--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.