



Protecting Tomorrow–Today.™

Online RMS

Version 11.18.1

Product Change Notice

6 May 2025

REVISION HISTORY

Revised By	Revision Date	Version	Notes
B. Chapman	6 May 2025	1.0	Service Pack Available

TABLE OF CONTENTS

Revision History 1

Introduction 3

Product Requirements..... 4

Release Milestones..... 5

Appendix: 11.18.1 Product Change Notice (PCN) – Detailed JIRA Listing 6

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

Appendix: Service Commitments 13

INTRODUCTION

This document provides an overview of the software changes delivered in the 11.18.1 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 11.18.1 release.

End Date	Milestone
29 Apr 2025	11.18.1 Code Lock
06 May 2025	11.18.1 Service Pack Available

We hope you share our enthusiasm for the production release of Online RMS 11.18.1. Please contact us by email at rms@caliberpublicsafety.com if you have any questions about the release.

Our Very Best,

Caliber Public Safety

APPENDIX: 11.18.1 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 11.18.1 release. An * symbol - denotes a software resolution that was deployed prior to the 11.18.1 service pack installation date.

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-75725		Performance enhancement IBR Data set screen loading	Enhancement	State Submissions	Increase performance when Data set screen is loading
IA-80981		Crash - allow user to search crash by submission document number	Enhancement	Crash Reporting	Enhance Crash search functionally
IA-81062	454530	MSP - Auditing	Bug/Defect	Incidents	Improve query
IA-80570	448252	TN NIBRS Custom Fields Data Deleted needs to Delete the Submission data	Release Defects	State Submissions	The Online RMS Incident Based Reporting for the state of Tennessee (TN NIBRS) has been updated to correctly report the Gang Activity data elements in the XML Submission file for TN NIBRS. This value was being reported in certain cases where there was no gang activity it should not have been

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					submitted. This issue has been corrected. This modification only impacts TN NIBRS RMS clients.
IA-80682		Houston PD, MS - CAD to Online RMS Mapping to Chickasaw County 911, MS	Configuration	Interface	The Online RMS to the Caliber CAD Interface has been configured and enabled for the Huston PD, MS
IA-80774	451991	Add to this validation message confirm Offenders were working in concert/Offense separation of time and space	Bug/Defect	State Submissions	<p>The online RMS Incident Validations have been updated to modify the wording on error message 2061 for</p> <p>Category Victim was Offender requires at least two participants in an incident where both were the victim and offender of the same offense. Additionally, verify that the offenders were acting together and that there was no significant separation in time or location between the offenses. If the offenders were not working together and/or the offenses took place at different times or locations, the incident should be reported separately for NIBRS purposes.</p>

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-80883		The Interface Maintenance Missing from the Knox County (IN42) Schema	Bug/Defect	Admin	The permission was corrected
IA-80900		TN NIBRS TN36 Previous Domestic Violence Arrest	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for the state of Tennessee (TN NIBRS) has been updated to correctly report the Previous Domestic Violence Arrest data element (TN36) in the XML Submission file for TN NIBRS. This value was not being reported in certain cases where it should have been and this issue has been corrected. This modification only impacts TN NIBRS RMS clients.
IA-80940		Crash - displays submission status and history	Enhancement	Crash Reporting	<p>A new "Submission Status" entry has been added to the sidebar which will show the submission status + the submission doc # (if applicable)</p> <p>In addition, if the crash has a doc #, it will show a "submission history" link in the crash links area. You can click this to get a dialog showing the submission history</p>

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					for a given crash report. It will be ordered by the date submitted, descending
IA-80945		TN NIBRS: <nc:Substance missing when 35A offense is Attempted and Drug Property Loss = None	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting for Tennessee (TN NIBRS) has been updated to correctly report the Substance in the TN NIBRS XML file in the case where the drug property loss is of type NONE. Previously the XML was not reporting the Substance in this case, this has been corrected.
IA-80946		TN NIBRS: Incident Rules and Validations - Add Drug Related Condition when NIBRS offense = 35A	Bug/Defect	State Submissions	An Additional Incident Rule and Validation has been configured for TN NIBRS that is added to Incident Offense Rules and Validations to prompt user to enter Drug Related = Yes when NIBRS offense = 35A. This will then prompt Origin of Drug and Drug Type custom fields to be displayed for the user to enter values when an offense is drug related. This incident rule and

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					validation is only applied to TN NIBRS RMS clients.
IA-80973		Interface Integration - Odyssey Courts to Online RMS for Tipton County Sheriff's Office - IN (IN80)	Configuration	Interface	The Odyssey Warrant interface has been set-up and configured for Tipton County.
IA-81042		Incident Offense tab does not display Validation error for Incident Rules and Validations	Release Defects	Admin	Tab now displays validation errors
IA-81045		CPS Public website Warrant List	Bug/Defect	Community Portal Service	The Online RMS Community Portal Service (CPS) has been updated to not retrieve active warrants where the person is less than 18 years old. Previously some warrants of 17 year olds were being displayed in the CPS application. This modification currently only impacts the Danville, VA client.
IA-81057		Crash - add officer dialog auto-complete can't find any officers in VA107	Bug/Defect	Crash Reporting	Corrected auto-complete query
IA-81091		Auditing Queries - Extra Performance Gain	Release Defects	Auditing	Enhanced performance

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
IA-79123	438060	RMS - Warrants coming over from Odyssey are removing the Ethnicity value in the Person Record	Bug/Defect	Interface	The Online RMS Odyssey Warrant Interface has been updated to correctly process a warrant where the ethnicity code of the person is not in the warrant transfer XML, but the person in the RMS has an ethnicity value. Previously the interface was replacing the persons defined ethnicity with a blank/null value. This has been modified to only update the ethnicity from the warrant if the value is non-blank (not null).
IA-79985		NJ Datasets is taking minutes to load	Bug/Defect	State Submissions	The Online RMS Incident Based Reporting has been updated to improve the performance on the data submission screen. For some users this screen would take a long time to load and create a new dataset based on the submission month. The screen has been optimized to eliminate some of the excess searching and processing when preparing the data set, especially for agencies that have auditing turned

JIRA #	Client Ticket #	Summary	Type of Issue	RMS Module	Functional Documentation
					on or have multiple agencies submitting a significant number of reports each month.
IA-80889		Civil - Log entry writing incorrect person served name	Bug/Defect	Civil Process	Corrected log entry
IA-80902		Add spaces to Serving Officers Name on Warrant info screen	Bug/Defect	Warrants	Corrected Serving Officers name with spacing
IA-80904		Add Field Arrest Print Options	Enhancement	Field Arrest	Added 3 new print options to the Field Arrest Print. These options can be found in a new section labeled Hide Options. These options allow the user to hide arrestee information. new options: -Hide Drivers License # -Hide Phone Numbers -Hide Caution Codes
IA-80935	453891	Crime Mapping - Issue with filtering on Crime Mapping	Bug/Defect	Public Crime Map	Filtering has been updated
IA-80413		Crash - flip error/warning on custom validations	Bug/Defect	Crash Reporting	Wrote a script to change the data in CRASH_VALIDATIONS as written in the description.

--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.