NOTICE and AGENDA for

Kalamazoo County Consolidated Dispatch Authority
Technical Advisory Committee
September 2, 2026

PLEASE TAKE NOTICE that a REGULAR Meeting of the Kalamazoo County Consolidated Dispatch Authority Technical Advisory Committee will be held on **Wednesday, September 2nd** at 10:00 a.m. in the Chief Switalski Meeting Room at Kalamazoo County Consolidated Dispatch Authority, 7040 Stadium Drive, Kalamazoo Michigan for consideration of items, namely, on this Agenda.

ITEM 1 – CALL TO ORDER

ITEM 2 – ROLL CALL

Western Michigan University Public Safety *Scott Merlo, Chair* (Alt. Ryan McGregor)		Kalamazoo Department of Public Safety *Matt Huber, Vice-Chair* (Alt. Chris Franks)	
Michigan State Police (Alt. Dale Hinz)		Kalamazoo County Sheriff's Office *Richard Fuller* (Alt. Logan Bishop)	
Township of Kalamazoo Police Department *Darien Smith* (Alt. Derek Thompson)		Portage Department of Public Safety *Matt Wolfe* (Alt. Bryan Mayhew)	
Kalamazoo County Medical Control Authority *Michael Bentley* (Alt. William Fales)		Kalamazoo County Fire Chief's Association *Chip Everett* (Alt. Todd Kowalski)	

ITEM 3 – APPROVAL OF MEETING MINUTES

A. July 1st – Regular Meeting

ITEM 4 – CITIZENS' TIME

The Committee welcomes members of the public to express their ideas or concerns about issues affecting Kalamazoo County Consolidated Dispatch Authority. Members of the public wishing to speak are requested to stand and state their full name and address for the record. Each member of the public is limited to four minutes or less.

ITEM 5 – FOR CONSIDERATION

A. Administrative Monthly Report (will be distributed once compiled)
B. Old Business
   1. Radio Readiness Program Update
C. New Business
   1. Drone Units & CAD Integration
   2. Uknown Accident – Crash Notification (Notify)
   3. Tyler Public Safety System Upgrade 26.3 SP1
      a. September 3rd – Test Environment
      b. October 27th – Production Environment

ITEM 6 – OTHER ITEMS

A. Announcements and Member Comments
B. Next Regular Meeting – November 4th, 2026

ITEM 7 – ADJOURNMENT

KCCDA meetings are open to all without regard to religion, race, color, national origin, sex, sexual orientation, gender identity or expression, height, weight, familial status, marital status, disability, or any other legally protected class. The KCCDA will provide special aid or assistance to attend a KCCDA meeting and will provide necessary reasonable auxiliary aids and services, such as signers for the hearing impaired and audio tapes of printed materials being considered at the meeting/hearing, to individuals with disabilities, upon four (4) business days' notice to the KCCDA. Individuals with disabilities requiring auxiliary aids or services should contact KCCDA by emailing admin@kccda911.org or calling (269) 488-8911.

MEETING MINUTES

Kalamazoo County Consolidated Dispatch Authority
TECHNICAL ADVISORY COMMITTEE
July 1, 2026 – Regular Meeting

ITEM 1 – **CALL TO ORDER**

The Regular Meeting of the Technical Advisory Committee was called to order by Lt. Scott Ernstes at 10:00 a.m. on Wednesday, July 1, 2026, in the Chief Switalski Meeting Room at Kalamazoo County Consolidated Dispatch Authority, 7040 Stadium Drive, Kalamazoo, Michigan.

ITEM 2 –**ROLL CALL**

<u>Members Present:</u> Scott Ernstes (MSP), Scott Merlo (WMUPD), Matt Huber (KDPS), Logan Bishop (KCSO), Darien Smith (KTPD), Bryan Mayhew (PDPS), Mike Bentley (KCMCA), Chip Everett (KCFCA)

<u>Others Present:</u> Ryan McGregor, Jeff Heppler, Jairus Baird, Scott Smith, Chris Franks, Scott Sanderson, Kacey Coffey, Jeff Troyer, Jon Moored, Marty Ftacek, Justin Johnson and Chris McComb

ITEM 3 – **APPROVAL OF MEETING MINUTES**

A. May 6– Regular Meeting

"Motion by Mr. Merlo, second by Mr. Huber to approve the minutes for the May 6, 2026, Regular Meeting as presented."

On a voice vote, **MOTION CARRIED**.

ITEM 4 - **CITIZENS TIME**

There was none.

ITEM 5 – **FOR CONSIDERATION**

A. Administrative Monthly Report

Mr. Troyer stated the report would be completed and distributed soon, as today was the first of the month.

B. Old Business

Mr. Troyer stated that Item 5.B.2. was removed from the agenda.

1. Radio Readiness Program Updates

Mr. Troyer stated the program was going well. All agencies had been notified that the 2026 funding allocation limit had been reached through executed MOUs. The Finance Committee will consider whether they will proceed with an additional allocation in 2026. He stated the remaining potential allocation would use nowhere close to the $8 million cap for the two-year project. The additional allocation to take care of the remaining agencies would be $1.65 million.

C. New Business

1. Revised MPSCS Agreements – Member Subscriber and Integration Agreements

Mr. Troyer stated these agreements were the result of a two-year update of member subscriber agreement. All agencies have these agreements, though dispatch has part one and two integration agreements because of towers. Administration is recommending approval and Board recommendation.

> "Motion by Mr. Huber, second by Mr. Merlo to approve and recommend Board approval of the Revised MPSCS Agreements – Member Subscriber and Integration Agreements as presented."

On a voice vote, **MOTION CARRIED**.

2. Automated Emergency Alert Guidelines

Mr. Troyer stated the draft guidelines were presented for consideration. Administration has been contacted by schools, private organizations, and religious centers that are using third party alerts for emergencies, and they would like to send it directly to the center by text. Notifications need to come in as a priority call and text to 911 is limited. We have obtained a number that these calls can go to, and the number will remain confidential, but it needs to be limited to active assailants and threats. The number cannot be used for medicals or any other situation. Recommending approval so guidelines are in place prior to acceptance of outside agencies. The system must identify the exact location of the incident, so third parties will need to work on that. This is step 1 in the process.

> "Motion by Mr. Merlo, second by Mr. Everett to approve the Automated Emergency Alert Guidelines as presented with a special note about the importance of still calling 911."

On a voice vote, **MOTION CARRIED**.

3. Radio ID's and Alias Updates

Mr. Troyer stated staff was trying to clean up the alias database. If we do not have an alias associated to a radio, the radio consoles will just show the subscriber unit id. The alias helps KCCDA staff identify who the user is. He stated he sent out a request for agencies to update their users and reiterated that request.

4. Rave Alert System (contract expires end of 2026)

Mr. Troyer stated that Dispatch holds the Rave contract for the county and it expires at the end of 2026. He asked if there was any interest in evaluating other systems. He stated that since other agencies use the system, he wanted to make sure no one would like to explore options. There was agreement that everyone was satisfied with the service and supported the renewal of the contract with Rave.

ITEM 6 – **OTHER ITEMS**

A. Election of TAC Chair and/or Vice-Chair

Mr. Ernstes announced that he would be stepping back to Trooper and relocating to Wayland. Mr. Hinz will be taking over at Paw Paw and will arrange for the appointment of an alternate.

> “Motion by Mr. Merlo, second by Mr. Huber for Mr. Merlo to move up to Chair and Mr. Huber to serve as Vice Chair for the remainder of year.”

On a voice vote, **MOTION CARRIED**.

B. Announcements and Member Comments

Mr. Troyer thanked Mr. Ernstes for his service and wished him good luck in Wayland.

C. Next Meeting

The next regular scheduled Technical Advisory Committee meeting will be Wednesday, September 2, 2026, at 10:00 am, and will be held in the Chief Switalski Meeting Room at KCCDA, 7040 Stadium Drive, Kalamazoo, MI 49009.

ITEM 7 - **ADJOURNMENT**

The meeting adjourned at 10:38 a.m.

Public Safety
Hardware and Software Prerequisites

Version 2026.3

Last revised on 8-26-26

Empowering people who serve the public®

Table of Contents

Introduction

Introduction

This document is intended to give *Tyler Technologies Public Safety* agencies a clear picture of the hardware and software requirements needed for their situation. Client specifications are the same regardless of the size of the agency. However, server specifications will vary according to the size of the agency and factors such as the number of concurrent power users (such as CAD dispatchers or someone who is actively using the system the majority of their day) signed into the system at any one time. For this document, the server minimum requirements are separated into small/medium and large clients. Clients that are running a single application such as *LE Records* will need to contact their *Tyler Technologies* Account Management team for specifications for their unique situation. Conversely agencies with needs greater than what is defined as large will also need to contact a *Tyler Technologies* representative.

Criteria	Small/Medium Agency	Large Agency
Number of Concurrent Power Users (Estimated)	26 - 100	101 - 250
City Population	15,000 - 110,000	110,000 - 400,000
County Population	30,000 - 220,000	220,000 - 800,000

Concurrent Power Users is defined as the maximum number of simultaneous users who use the system the majority of their day. This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

Warning: If you are in a physical server configuration rather than a virtual, please contact your *Tyler Technologies* Customer Care Representative.

Changes in 2026.3

See the table below for an overview of changes since the previous release.

Application	Old Value	New Value
In *MSP*, Microsoft Edge WebView2 is required on client machines. This is included with *Windows 11* and recent updates of *Windows 10*.		

Application	Old Value	New Value
MSP servers no longer require Microsoft Office.		

Changes in 2025.2

See the table below for an overview of changes since the previous release.

Application	Old Value	New Value
Support for Windows SQL versions older than 2019 were dropped. For example, mainstream SQL 2016 has not been supported by Microsoft since July 2022.		
Support for Windows Server 2016 was dropped. Microsoft ended mainstream support for that release in 2016.		

Changes in 2025.1

See the table below for an overview of changes since the previous release.

Application	Old Value	New Value
MSP, Enterprise Mobile, and Enterprise CAD clients require Microsoft Visual C++ Redistributable (x64) 2015-2019. Refer to Microsoft for the correct version.		
Enterprise Records, MSP, *Enterprise CAD*, and *Enterprise Mobile* servers now require *Microsoft .NET 8.0.*		8.0

Application	Old Value	New Value
Updates were made for *Enterprise Mobile*: • Port 9300 is no longer needed for PrePlans. • For servers, Microsoft SQL Server Compact Edition, Microsoft Sync Framework (for use with pre-plans), and Microsoft Report Viewer (for use with pre-plans) is no longer required. • For clients, Microsoft .NET Framework 3.5 is no longer required • For clients, Microsoft SQL Server Compact Edition is no longer required. • For clients, Microsoft Sync Framework (for use with pre-plans) is no longer required. • For clients, Microsoft Report Viewer (for use with pre-plans) is no longer required.		
Updates were made for *Enterprise CAD:* • Microsoft Sync Framework is no longer required. • For clients, Microsoft Sync Framework (for use with pre-plans) is no longer required.		

Changes in 2024.2

See the table below for an overview of changes since the previous release.

Application	Old Value	New Value
The GIS Server software components hadn't been updated for a few releases and were brought to current. Refer to "GIS Server Software" on page 6.		
Enterprise Updater	1.7.4	2.0.20
Support for *Microsoft Office* 2013 discontinued.	2013	
Enterprise Mobile no longer uses Mobile Interop. Additionally, the Mobile Ports and diagram were updated to reflect the change. Refer to "Enterprise Mobile Ports and Services" on page 47.		

Style Conventions

Below are the formatting conventions that are used within this document.

Formatting Convention	Type of Information Represented
Italic	Windows, tabs, sub-tabs, as well as vertical tabs and sub-tabs.
Initial Caps Only	Grid and frame names.
Bold or **<bold in brackets>**	Buttons, specific keystrokes, and keystroke combinations (example: <**ctrl**>+<**p**>). Also, options that are being selected appear in bold text.
Bold Italic	Control names, data entry fields, and display fields.
ALL CAPS	Modes of operation.
As Appears in List	Options within drop-down lists, etc.

Icon Legend

Below is a list of icons that may be used in this document.

Icon	Type
	Note
	Tip
	Best Practice
	Warning

Chapter 1
Common Components

Introduction

The software and hardware specifications presented in this chapter are used by multiple *Public Safety* applications. Unless a prerequisite is specifically stated to be different within the *MSP*, *Enterprise CAD*, *Enterprise Mobile*, or *Enterprise Records* chapters, the prerequisites listed in this chapter should be used.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

Best Practice: Although not required, encrypted hard drives are recommended to satisfy any "encryption at rest" concerns your agency may have.

The information in this document is presented in the following order:

- "Software Requirements" on page 5
- "Recommended Hardware Requirements" on page 8

❖ ❖ ❖ ❖ ❖

Software Requirements

Software required on target machines prior to installing *MSP* is listed separately for the server and client machines.

Refer to the following sections for more information:

- "Windows Server Operating System" on page 5
- "Windows Client Operating System" on page 6
- "GIS Server Software" on page 6
- "SQL Server Software" on page 6
- "Office Requirements for MSP, Enterprise CAD, Enterprise Records, DSS, and Web Reporting" on page 7
- "Enterprise Security Server Software" on page 7

❖ ❖ ❖ ❖ ❖

Windows Server Operating System

Application	Version/Information
Operating System	Windows Server 2019 or 2022

Windows Client Operating System

Application	Version/Information
Operating System[a]	Windows 10 64-bit or Windows 11 64-bit

a. Tyler Technologies products continue to be tested with the latest maintenance/security updates from operating systems (Microsoft/iOS/Android). We utilize Tyler Community to warn our users if we encounter problems or areas of concern as soon as we know them. We recommend that all updates of this nature are put into a test system and have an agency-determined soak time before putting the change in a production environment.

GIS Server Software

Application	Version/Information
Microsoft .NET Framework	4.8
Operating System	Refer to "Windows Server Operating System" on page 5
Microsoft SQL Server Management Studio	Refer to "SQL Server Software" on page 6
ArcGIS Server (Esri)	11.1
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Wildcard Certificate
Enterprise Updater	2.0.20
Python	3.9.16
.NET Desktop Runtime	6

SQL Server Software

Application	Version/Information
Operating System	Refer to "Windows Server Operating System" on page 5
Microsoft SQL Server	2019 CU13 (supported in 2020.1 HF1) or 2022
Microsoft SQL Server Management Studio	2019, or 2022
Microsoft SQL Command Line Utility	2019, or 2022

Office Requirements for MSP, Enterprise CAD, Enterprise Records, DSS, and Web Reporting

Application	Version/Information
Operating System	Refer to "Windows Server Operating System" on page 5
Microsoft .NET Framework	4.8
Microsoft ASP.NET	4.0
Microsoft Windows Server Client Tools	2012, 2014, or 2016
Microsoft SQL Server Standard Edition with the following components installed: **SQL Server Management Studio** **Microsoft Database Engine** **SQL Server Integration Services (SSIS) Utilities** **SQL Server Analysis Services (SSAS) Utilities**	Refer to "SQL Server Software" on page 6
Internet Information Services (IIS)	7.0
Microsoft Office	2016 (Standard, Home and Business, Professional 32-bit for all) 2016/365 (Professional Plus Edition 32-bit) 2019 (Standard, Home and Business, Professional 32-bit) 2021 (Standard, Home and Business, Professional 32-bit)

Enterprise Security Server Software

Application	Version/Information
Operating System	Refer to "Windows Server Operating System" on page 5
Microsoft ASP.NET Core	3.1
.NET Core Runtime & Hosting Bundle	2.0.8

General

Application	Version/Information
Browsers	Chrome, Firefox, Edge, or Safari. Note that cookies should be enabled and pop-ups allowed.

Enterprise Updater

Certificates

During installation, Enterprise Updater imports certificates into the following stores:

- Add certificates to LocalMachine\TrustedPeople.
- Add certificates with private keys to LocalMachine\My.

Folder Permissions

All listed directories must grant BUILTIN\Users the following permissions: Modify (OI)(CI) → Object Inherit and Container Inherit enabled. This ensures client components (Updater) can properly read, write, and update configuration and runtime files.

Program Files (x86)

- C:\Program Files (x86)\New World Systems

ProgramData

- C:\ProgramData\New World Systems

Registry Keys

The Enterprise Updater Service runs under the Local System account, which must have permissions to create, modify, and delete registry values required for application updates. During the update, this service modifies registry keys associated with the Enterprise Updater components.

New World Enterprise Updater Service

- HKEY_LOCAL_MACHINE\Software\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\New World Systems

Recommended Hardware Requirements

Not every agency will require all of these virtual servers. These are examples to show what is needed if particular applications are licensed.

Please note the Virtual Memory assigned to the SQL Server includes Operating System requirements. For memory allocation on the SQL server, systems should include 8 GB of RAM for the Operating System, 20 GB of RAM for the production instance of SQL Server, and 4 GB of RAM for each non-production instance of SQL server (for training, testing, etc.).

The tables that follow are not applicable for *Enterprise Records.*

Database Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	32 GB	32 GB
Virtual Hard Drive (OS)	150 GB	150 GB

Database Server	Small/Medium Agency	Large Agency
Virtual Hard Drive (SQL)	500 GB	1 TB

Reporting Server (DSS & Web Reporting)	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	32 GB	64 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Hard Drive (SQL)	Five times the size of the combined *MSP* and *Enterprise CAD* databases	Five times the size of the combined *MSP* and *Enterprise CAD* databases

GIS Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	32 GB	64 GB
Virtual Hard Drive (not including aerial imagery)	500 GB	500 GB

Enterprise Security Server	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	8 GB	16 GB
Virtual Hard Drive (OS)	150 GB	150 GB

Windows Tablet

Tablets can be used for various applications. The minimum requirements are listed in this table.

Tablet	Information
Processor	Intel Core or AMD Ryzen Processor
System Memory	16 GB
Hard Drive	M.2 PCIe SSD System Disk (50GB Available)

Chapter 2
MSP

Introduction

The software and hardware specifications presented in this document are the minimum recommended general requirements necessary to optimally run the *MSP* software in most application environments. Specific requirements may vary based on unique circumstances at customer sites. The *Tyler Technologies* team of experts evaluates all actual customer requirements and may add or change these specifications for individual implementations.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

Best Practice: Although not required, encrypted hard drives are recommended to satisfy any "encryption at rest" concerns your agency may have.

Refer to the following sections for more information:

- "Software Requirements" on page 11
  - "MSP Server Software" on page 12
  - "MSP Client Software" on page 12
- "Recommended Hardware Requirements" on page 14
  - "MSP Server Hardware" on page 14
  - "MSP Client Hardware" on page 15

❖ ❖ ❖ ❖ ❖

Software Requirements

Software required on target machines prior to installing *MSP* is listed separately for the server and client machines.

Refer to the following sections for more information:

- "MSP Server Software" on page 12
- "MSP Client Software" on page 12

❖ ❖ ❖ ❖ ❖

MSP Server Software

Application	Version/Information
Microsoft .NET Framework	3.5 SP1 and 4.8
Microsoft .NET	8.0
Operating System	Refer to "Windows Server Operating System" on page 5
ASP.NET	2.0
GeneX	8.1.222 or later
Enterprise GIS Components	4.0 (32 and 64-bit)[a]
Microsoft SQL Server	Refer to "SQL Server Software" on page 6
Microsoft SQL Command Line Utility	Refer to "SQL Server Software" on page 6
Microsoft OLE DB Driver for SQL Server	18.6.3
Windows Identity Foundation	Windows Server 2012 – 3.5
Enterprise Updater	2.0.20

a. 64-bit systems require both to be installed

MSP Client Software

Application	Version/Information
Operating System	Refer to "Windows Client Operating System" on page 6 with UAC Disabled
Microsoft .NET Framework	2.0 SP2, 3.5 SP1, and 4.8
Microsoft System CLR Types for SQL Server	2017
Microsoft Visual Studio Tools for Office Runtime	2010 (for reporting) version 10.0.50903
Microsoft Visual C++ Redistributable (x32 and x64)	2015-2019. Refer to Microsoft for the correct version.
Supported Web Browsers	"General" on page 7
Adobe Acrobat Reader	X, XI, DC. Note that Adobe Acrobat Pro is not supported.

Application	Version/Information
Windows Media Player	Windows Media Player must be turned on in Windows Features, otherwise it is uninstalled, which can cause issues.
Microsoft Edge WebView2	Can be installed as a stand-alone or is included with Microsoft Edge. If missing, user receives an error when launching the application and cannot log in.

Certificates

During installation, the MSP client application imports certificates into the following stores:

- Add certificates to LocalMachine\TrustedPeople.
- Add certificates with private keys to LocalMachine\My.

Folder Permissions

All listed directories must grant BUILTIN\Users the following permissions: Modify (OI)(CI) → Object Inherit and Container Inherit enabled. This ensures client components (MSP) can properly read, write, and update configuration and runtime files.

Program Files (x86)

- C:\Program Files (x86)\New World Systems

ProgramData

- C:\ProgramData\New World Systems
- C:\ProgramData\Tyler Technologies

Users AppData Folder

- C:\Users*USERNAME*\AppData

Windows Fonts

- C:\Windows\Fonts

Windows SysWow64

- C:\WINDOWS\SysWow64

Registry Keys

The Enterprise Updater Service runs under the Local System account, which must have permissions to create, modify, and delete registry values required for application updates. During the update, this service modifies registry keys associated with the *MSP* components.

MSP Client

- HKEY_LOCAL_MACHINE\SOFTWARE\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

GIS Components and Data Entries

- HKEY_LOCAL_MACHINE\SOFTWARE\New World Systems\New World Automatic Updater
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

Microsoft .NET Framework 4.8

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup

Microsoft System CLR Types for SQL Server

- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Microsoft SQL Server
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server

Microsoft Visual Studio Tools for Office Runtime

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\VSTA Runtime Setup

Microsoft Visual C++ Redistributable (2015–2019 x64)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VisualStudio

Recommended Hardware Requirements

Hardware required on target machines prior to installing *MSP* is listed separately for the server and client machines.

Refer to the following sections for more information:

- "MSP Server Hardware" on page 14
- "MSP Client Hardware" on page 15

❖ ❖ ❖ ❖ ❖

MSP Server Hardware

Not every agency will require all of these virtual servers. These are examples to show what would be needed if particular applications are licensed. For *Enterprise Mobile*, see the *Enterprise Mobile* chapter and for *Enterprise CAD,* see that chapter.

Please note the Virtual Memory assigned to the SQL Server includes Operating System requirements. For memory allocation on the SQL server, systems should include 8 GB of RAM for the Operating System, 20 GB of RAM for the production instance of SQL Server, and 4 GB of RAM for each non-production instance of SQL server (for training, testing, etc.).

Application Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	8 GB	12 GB
Virtual Hard Drive (OS)	150 GB	150 GB

Application Server	Small/Medium Agency	Large Agency
Virtual Disk (File Storage)	1 TB	2 TB

Test/Training Server	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	8 GB	8 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Disk (File Storage)	1 TB	2 TB

MSP Client Hardware

Enterprise Security Server	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	4 GB	8 GB
Virtual Hard Drive (OS)	150 GB	150 GB

The client hardware required depends upon the application that will be run on the client. The size of the agency does not matter.

Record/Corrections Workstations	Information
Processor	Intel Core, Intel Xeon or AMD Ryzen Processor
System Memory	8 GB
Hard Drive	M.2 PCIe SSD System Disk (50GB Available)
Bar Code Scanner	Zebra MC67 KT-67NA-PDABAA0050

Chapter 3
Enterprise Mobile

Introduction

The software and hardware specifications presented in this document are the minimum recommended general requirements necessary to optimally run the *Enterprise Mobile* software in most application environments. Specific requirements may vary based on unique circumstances at customer sites. The *Tyler Technologies* team of experts evaluates all actual customer requirements and may add or change these specifications for individual implementations.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

Best Practice: Although not required, encrypted hard drives are recommended to satisfy any "encryption at rest" concerns your agency may have.

The information in this chapter is presented in the following order:

- "Software Requirements" on page 17
- "Recommended Hardware Requirements" on page 19

❖ ❖ ❖ ❖ ❖

Software Requirements

Software required on target machines prior to installing *Enterprise Mobile* is listed for the server and client machines.

Enterprise Mobile Server Software

Application	Version/Information
Microsoft .NET Framework	4.8
Microsoft .NET	8.0
Operating System	Refer to "Windows Server Operating System" on page 5
ASP.NET	4.0
Microsoft SQL Server	Refer to "SQL Server Software" on page 6
File Streaming	Enabled

Enterprise Mobile Client Software

Application	Version/Information
Microsoft .NET Framework	4.8
Microsoft Edge WebView2	Can be installed as a stand-alone or is included with Microsoft Edge. If missing, user receives an error when launching the application and cannot log in.
Microsoft Visual C++ Redistributable (x64)	2015-2019. Refer to Microsoft for the correct version.

Certificates

During installation, the *Enterprise Mobile* client application imports certificates into the following stores:

- Add certificates to LocalMachine\TrustedPeople.
- Add certificates with private keys to LocalMachine\My.

Folder Permissions

All listed directories must grant BUILTIN\Users the following permissions: Modify (OI)(CI) → Object Inherit and Container Inherit enabled. This ensures client components (*Enterprise Mobile*) can properly read, write, and update configuration and runtime files.

Program Files

- C:\Program Files\New World Systems
- C:\Program Files\Tyler Technologies

Program Files (x86)

- C:\Program Files (x86)\New World Systems

ProgramData

- C:\ProgramData\New World Systems
- C:\ProgramData\New World Systems\Aegis Mobile\Data
- C:\ProgramData\Tyler Technologies

Registry Keys

The Enterprise Updater Service runs under the Local System account, which must have permissions to create, modify, and delete registry values required for application updates. During the update, this service modifies registry keys associated with the *Enterprise Mobile* components.

Mobile Client

- HKEY_LOCAL_MACHINE\Software\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

GIS Components and Data Entries

- HKEY_LOCAL_MACHINE\SOFTWARE\New World Systems\New World Automatic Updater
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

Microsoft .NET Framework 4.8

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup

Microsoft Visual C++ Redistributable (2015–2019 x64)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VisualStudio

Microsoft Edge WebView2 Runtime\

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EdgeUpdate

Recommended Hardware Requirements

Hardware required on target machines prior to installing *Enterprise Mobile* is listed for the server and client machines.

Enterprise Mobile Server Hardware

Application	Version/Information
Virtual Processors	4
Virtual Memory	16 GB for Small/Medium Agencies 16 GB for Large
Virtual Hard Drive (OS)	150 GB
Virtual Disk (File Storage)	200 GB

Note: For an *Enterprise Mobile* test server, the stats remain the same except that the Virtual Memory is 8 GB regardless of if this is a small/medium or large customer.

Enterprise Mobile Client Hardware

Application	Version/Information
RAM	16 GB
Processor	Intel Core or AMD Ryzen Processor
Hard Drive	M.2 PCIe SSD System Disk (50GB Available)
Network	Optional Integrated 4G/LTE Mobile Broadband w/GPS

Application	Version/Information
Visual Display Resolution	12" or larger (Touchscreen Optional)

Wireless Connectivity

Application	Information
Supported IP-based Wireless Networks	EVDO, 4G/LTE Commercial Wireless, WiFi 802.11 g/n/ac
Mobile VPN	NetMotion Mobility or similar
Advanced Authentication (CJIS Compliance)	Duo Mobile 2FA, RSA or similar

Chapter 4
Enterprise CAD

Introduction

The software and hardware specifications presented in this chapter are the minimum recommended general requirements necessary to optimally run the *Enterprise CAD* software in most application environments. Specific requirements may vary based on unique circumstances at customer sites. The *Tyler Technologies* team of experts evaluates all actual customer requirements and may add or change these specifications for individual implementations.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

Best Practice: Although not required, encrypted hard drives are recommended to satisfy any “encryption at rest” concerns your agency may have.

The information in this document is presented in the following order:

- “Software Requirements” on page 21
- “Recommended Hardware Requirements” on page 24

❖ ❖ ❖ ❖ ❖

Software Requirements

Software required on target machines prior to installing *Enterprise CAD* is listed for theserver and client machines.

Enterprise CAD Server Software

Application	Version/Information
Microsoft .NET Framework	4.8
Microsoft .NET	8.0
Operating System[a]	**Refer to “Windows Server Operating System” on page 5**
To avoid performance issues, in Windows Settings for *Enterprise CAD*, turn off the ***Automatically update certificates in the Microsoft Root Certificate Program (recommended)*** setting on the Certificate Path Validation Settings Properties window of the Local Security Policy. For more information on how to do this, refer to the *Optimizing Windows Settings for Enterprise CAD* document.	

Application	Version/Information
ASP.NET	2.0
Microsoft SQL Server	Refer to "SQL Server Software" on page 6
Microsoft SQL Server Management Studio	Refer to "SQL Server Software" on page 6
Enterprise GIS Components	4.0 (64-bit)
Windows Identity Foundation	Windows Server 2012 – 3.5
Enterprise Updater	2.0.20 (for GIS updates)
Microsoft Internet Information Services (IIS)	7.0
Peer Name Resolution Protocol (PRNP)	Enable in server features (needed for Chat)
File Streaming	Enable
OpenSearch	1.3

a. Tyler Technologies supports both 32 and 64-bit operating systems. Due to processor and OS limitations, a 32-bit system can only take advantage of 4 out of a recommended 8 GB of RAM. For an enhanced end-user experience, we recommend a 64-bit OS.

Enterprise CAD Client Software

Application	Version/Information
To avoid performance issues, in Windows Settings for *Enterprise CAD*, turn off the ***Automatically update certificates in the Microsoft Root Certificate Program (recommended)*** setting on the Certificate Path Validation Settings Properties window of the Local Security Policy. For more information on how to do this, refer to the *Optimizing Windows Settings for Enterprise CAD* document.	
Microsoft .NET Frameworks	4.8
Microsoft Visual Studio Tools for Office Runtime	2010 (for reporting)
Microsoft Edge WebView2	Can be installed as a stand-alone or is included with Microsoft Edge. If missing, user receives an error when launching the application and cannot log in.
Microsoft Visual C++ Redistributable (x64)	2015-2019. Refer to Microsoft for the correct version.

Certificates

During installation, the CAD client application imports certificates into the following stores:

- Import certificates to LocalMachine\TrustedPeople.

- Import certificates with private keys to LocalMachine\My.

Folder Permissions

All listed directories must grant BUILTIN\Users the following permissions: Modify (OI)(CI) → Object Inherit and Container Inherit enabled. This ensures client components (*Enterprise CAD*) can properly read, write, and update configuration and runtime files.

Program Files

- C:\Program Files\New World Systems
- C:\Program Files\Tyler Technologies

Program Files (x86)

- C:\Program Files (x86)\New World Systems

ProgramData

- C:\ProgramData\New World Systems
- C:\ProgramData\Tyler Technologies

Registry Keys

The Enterprise Updater Service runs under the Local System account, which must have permissions to create, modify, and delete registry values required for application updates. During the update, this service modifies registry keys associated with the *Enterprise CAD* components.

CAD Client

- HKEY_LOCAL_MACHINE\Software\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\New World Systems
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

GIS Components and Data Entries

- HKEY_LOCAL_MACHINE\SOFTWARE\New World Systems\New World Automatic Updater
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

Microsoft .NET Framework 4.8

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup

Microsoft Visual C++ Redistributable (2015–2019 x64)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VisualStudio

Microsoft Edge WebView2 Runtime\

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EdgeUpdate

Enterprise CAD Standard Web Reporting

Application	Version/Information
Operating System	Refer to "Windows Server Operating System" on page 5
Microsoft .NET Framework	3.5, 4.5, 4.6[a] 4.7.2 and 4.8 are supported but not required.
Microsoft ASP.NET	4.0
Microsoft Windows Server Client Tools	2012, 2014, or 2016
Microsoft SQL Server Standard Edition with the following components installed: **SQL Server Management Studio** **Microsoft Database Engine** **SQL Server Integration Services (SSIS) Utilities** **SQL Server Analysis Services (SSAS) Utilities** **SQL Server Reporting Services (SSRS)**	"SQL Server Software" on page 6
Internet Information Services (IIS)	7.0
Microsoft Internet Explorer (Client)	11

a. SQL 2016 SP1 requires .NET Framework 4.6, which is automatically installed.

Recommended Hardware Requirements

Hardware required on target machines prior to installing *Enterprise CAD* is listed forserver and client machines. Virtual machine requirements are also listed in this section.

Note: For agencies using software High Availability, the virtual machine requirements for Enterprise CAD need to be duplicated.

Enterprise CAD Server Hardware

The following table contains information regarding the virtual machines needed for an *Enterprise CAD* live environment.

Enterprise CAD Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	12 GB	24 GB
Virtual Hard Drive	150 GB	150 GB

The following table contains information regarding the virtual machines needed for an *Enterprise CAD* test environment.

Enterprise CAD Server Test Side	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	8 GB	8 GB
Virtual Hard Drive	150 GB	150 GB

A Load Balancer server is only required if your agency is using software High Availability.

Load Balancer Server	Small/Medium Agency	Large Agency
Virtual Processors	N/A	2
Virtual Memory	N/A	8 GB
Virtual Hard Drive (OS)	N/A	150 GB

Enterprise CAD Client Hardware

The following table is requirements for *Enterprise CAD* client machines.

Call Taker/Dispatch Workstations	Version/Information
Processor	Intel Core, Intel Xeon or AMD Ryzen Processor
System Memory	32 GB
Hard Drive	M.2 PCIe SSD System Disk (50GB Available)
Graphics Card	Quad Port Graphics with 4GB Memory

Optional Dedicated Rip & Run Server

A separate, dedicated Rip & Run server is not a requirement but can prove useful for agency's that are experiencing system slowdowns because there are Rip & Run reports being sent to many Fire stations within their agency. This dedicated server would help alleviate these system issues.

It is recommended that any agency interested in running Rip & Run reports from a separate server ensure that the dedicated server has a minimum of 8 GBs of RAM and 2 CPUs. Agency's can scale this to 16 GBs of RAM and 4 CPUs based on their Rip & Run needs.

Chapter 5
Enterprise Records

Introduction

The software and hardware specifications presented in this document are the minimum recommended general requirements necessary to optimally run the *Enterprise Records* software in most application environments. Specific requirements may vary based on unique circumstances at customer sites. The *Tyler Technologies* team of experts evaluates all actual customer requirements and may add or change these specifications for individual implementations.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

The information in this document is presented in the following order:

❖ ❖ ❖ ❖ ❖

Software Requirements

Software required on target machines prior to installing *Enterprise Records* is listed separately for the server and client machines.

Refer to the following sections for more information:

- "All Enterprise Records Servers" on page 28

❖ ❖ ❖ ❖ ❖

All *Enterprise Records* Servers

The entries in this table are applicable for all *Enterprise Records* servers.

Application	Version/Information
Operating System	Windows Server 2016 or Windows Server 2019 or Windows Server 2022
Microsoft .NET Framework	4.8
Microsoft .NET	8.0

Application Server Software

Application	Version/Information
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Service Certificates Wildcard Certificate (if not using a load balancer)

Interfaces Server Software

Application	Version/Information
Signed Certificates	Service Certificates

Mobile Server Software

Application	Version/Information
Microsoft SQL Server Management Studio	2016, 2019, or 2022
Signed Certificates	Service Certificates

SQL Server Software

Application	Version/Information
Microsoft SQL Server	2016, 2019, or 2022
Microsoft SQL Server Management Studio	2016, 2019, or 2022

Reporting Server Software

Application	Version/Information
Microsoft SQL Server Reporting Services (SSRS)	2016, 2019, or 2022
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Service Certificates

Enterprise Security Server Software

Application	Version/Information
Internet Information Services (IIS)	7.0
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Service Certificates

Enterprise CAD Application Server Software

Only needed if *Enterprise CAD* is installed.

Application	Version/Information
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Service Certificates

Messaging Server Software

Application	Version/Information
Enterprise Records Communication Service	Latest
Java Runtime	11

OpenSearch Server Software

Application	Version/Information
Signed Certificates	Service Certificates
OpenSearch	1.3

TCM Application/File Storage Server

Application	Version/Information
Java Runtime	8
Java Development Kit (required by TCM/Tomcat)	8
Apache Tomcat	8.5
Tyler Content Manager (TCM)	2023.1
Signed Certificates (if running Tomcat HTTPS)	Domain CA or other trusted issuer (Verisign, etc)

Load Balancer Server Software

Application	Version/Information
Internet Information Services (IIS)	7.0
Signed Certificates	Domain CA or other trusted issuer (Verisign, etc) Wildcard Certificate

Enterprise Records Client Software

Application	Version/Information
Microsoft Office	2016 (Standard, Home and Business, Professional 32/64-bit 2016/365 (Professional Plus Edition 32/64-bit) 2019 (Standard, Home and Business, Professional 32-bit 2021 (Standard, Home and Business, Professional 32-bit)

Recommended Hardware Requirements

Hardware required on target machines prior to installing *Enterprise Records* is listedseparately for the server and client machines.

Refer to the following sections for more information:

- "Server Hardware" on page 31
- "Client Hardware" on page 35

❖ ❖ ❖ ❖ ❖

Server Hardware

Not every agency will require all of these virtual servers. These are examples to show what would be needed if particular applications are licensed.

Please note the Virtual Memory assigned to the SQL Server includes Operating System requirements. For memory allocation on the SQL server, systems should include 8 GB of RAM for the Operating System, 20 GB of RAM for the production instance of SQL Server, and 4 GB of RAM for each non-production instance of SQL server (for training, testing, etc.).

Records Application Load Balancer Server	Small/Medium Agency	Large Agency
Virtual Processors	N/A	2
Virtual Memory	N/A	8 GB
Virtual Hard Drive (OS)	N/A	150 GB

Records Service Node 1 Server ActiveMQ	All Agencies
Virtual Processors	4
Virtual Memory	32 GB

Records Service Node 1 Server ActiveMQ	All Agencies
Virtual Hard Drive (OS)	150 GB
Virtual Hard Drive (File Storage)	250 GB

Records Service Node 2 Server	Small/Medium Agency	Large Agency
Virtual Processors	N/A	4
Virtual Memory	N/A	32 GB
Virtual Hard Drive (OS)	N/A	150 GB
Virtual Hard Drive (File Storage)	N/A	250 GB

TCM Application/File Storage Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	32 GB	32 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Hard Drive (File Storage)	500 GB	1 TB

Enterprise Security/IMS Server	All Agencies
Virtual Processors	2
Virtual Memory	8 GB
Virtual Hard Drive (OS)	150 GB

A medium sized-agency can use one VM to house database and reporting, however larger agencies need separate servers for these two applications.

Database/ Reporting Server	Small/Medium Agency
Virtual Processors	4

Database/ Reporting Server	Small/Medium Agency
Virtual Memory	48 GB
Virtual Hard Drive (OS)	150 GB
Virtual Hard Drive (Production & Test Data)	250 GB
Virtual Hard Drive (Backup)	250 GB
Virtual Hard Drive (SQL Logs)	100 GB
Virtual Hard Drive (TempDB)	50 GB

Database Server	Large Agency
Virtual Processors	6
Virtual Memory	64 GB
Virtual Hard Drive (OS)	100 GB
Virtual Hard Drive (Production & Test Data)	500 GB
Virtual Hard Drive (Backup)	200 GB
Virtual Hard Drive (SQL Logs)	100 GB
Virtual Hard Drive (TempDB)	50 GB

Reporting Server	Large Agency
Virtual Processors	4
Virtual Memory	64 GB
Virtual Hard Drive (OS)	150 GB
Virtual Hard Drive (Production Data)	250 GB
Virtual Hard Drive (TempDB)	50 GB

GIS Server	Small/Medium Agency	Large Agency
Virtual Processors	4	4

GIS Server	Small/Medium Agency	Large Agency
Virtual Memory	32 GB	64 GB
Virtual Hard Drive (OS)	500 GB	500 GB

A medium-sized agency will need one OpenSearch node server whereas a larger one will need three.

OpenSearch Node Server 1	Small/Medium Agency	Large Agency
Virtual Processors	4	4
Virtual Memory	24 GB	64 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Hard Drive (File Storage)	500 GB	500 GB

OpenSearch Node Server 2	Small/Medium Agency	Large Agency
Virtual Processors	N/A	4
Virtual Memory	N/A	64 GB
Virtual Hard Drive (OS)	N/A	150 GB
Virtual Hard Drive (File Storage)	N/A	500 GB

OpenSearch Node Server 3	Small/Medium Agency	Large Agency
Virtual Processors	N/A	4
Virtual Memory	N/A	64 GB
Virtual Hard Drive (OS)	N/A	150 GB
Virtual Hard Drive (File Storage)	N/A	500 GB

Interface Server	All Agencies
Virtual Processors	2
Virtual Memory	8 GB

Interface Server	All Agencies
Virtual Hard Drive (OS)	150 GB
Virtual Hard Disc (File Storage)	100 GB

Records Service Node/ActiveMQ Test/Training Server	All Agencies
Virtual Processors	2
Virtual Memory	16 GB
Virtual Hard Drive (OS)	150 GB
Virtual Hard Disc (File Storage)	250 GB

OpenSearch Node Test/ Training Server	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	16 GB	16 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Hard Drive (File Storage)	500 GB	1 TB

TCM Application/File Storage Test/Training Server	Small/Medium Agency	Large Agency
Virtual Processors	2	2
Virtual Memory	16 GB	16 GB
Virtual Hard Drive (OS)	150 GB	150 GB
Virtual Hard Drive (File Storage)	500 GB	1 TB

Client Hardware

The client hardware required depends upon the application that will be run on the client. The size of the agency does not matter.

Records Workstations	Information
Processor	Intel Core, Intel Xeon or AMD Ryzen Processor
System Memory	8 GB
Hard Drive	M.2 PCIe SSD System Disk (50GB Available)
Document Scanning	32-bit Twain Driver
Topaz 4x3 Signature Pad	Windows 32-bit

Chapter 6
Mobility

Introduction

The software and hardware specifications presented in this chapter are the minimum recommended general requirements necessary to optimally run the *Enterprise Mobility* software in most environments. Specific requirements may vary based on unique circumstances at client sites. The *Tyler Technologies* team of experts evaluates all actual client requirements and may add or change these specifications for individual implementations.

This information is intended for use as a general guideline. Contact your *Tyler Technologies* Customer Care Representative for additional information on the requirements identified for your installation.

The information in this chapter is presented in the following order:

❖ ❖ ❖ ❖ ❖

Apple Requirements

Apple devices that support iOS 16.0 or higher can run *Mobility*. Apple devices released within the last two years are recommended; older devices may see degraded performance and battery life.

Application/Device
iPhone
iPad/Mini/Pro WiFi + Cellular option is recommended for all iPads as they include a built in GPS antenna

Android Requirements

Android devices must have a 64-bit processor/OS and be running Android 13.0 or higher. *Samsung* or *Google* devices released within the last two years are recommended; older devices or lower tier devices may see degraded performance and battery life.

Application/Device
Samsung Galaxy
Google Pixel
Samsung Note
Samsung Galaxy Tab

Chapter 7
Ports and Services

Introduction

This chapter outlines the services and ports used to communicate between different devices and applications when using *Tyler Technologies Public Safety* applications. Additional ports may need to be opened, perhaps on a temporary basis, for other applications/purposes such as running a data conversion. *Tyler Technologies* personnel will advise when appropriate.

Refer to the following:

- "Required for External Access" on page 39
- "Enterprise Security" on page 41
- "GIS Ports and Services" on page 41
- "MSP Ports and Services" on page 42
- "Enterprise CAD Ports and Services" on page 45
- "Enterprise Mobile Ports and Services" on page 47
- "Enterprise Records Ports and Services" on page 49
- "Decision Support Software Ports and Services" on page 52

❖ ❖ ❖ ❖ ❖

Required for External Access

Installation of various *Tyler Technologies* software requires access to external locations.

IMS

For installations using IMS, access to the following external locations is required:

- https://ims.tylerhost.net/
- email-smtp.us-east-1.amazonaws.com port 587

TCM

TylerDeploy is used for installing TCM, a requirement for *Enterprise Records*. TCM requires access to the following external locations:

- https://tylerdeployer.tylerdeploy.com:10943
- https://tylerdeployer2.tylerdeploy.com:10944
- https://tylerdeployer3.tylerdeploy.com:10945
- https://tylerdeployer4.tylerdeploy.com:10946

- https://tylerdeployer5.tylerdeploy.com:10947
- https://tylerdeployer6.tylerdeploy.com:10948
- https://tylerdeployer7.tylerdeploy.com:10949
- https://tylerdeployer8.tylerdeploy.com:10950
- https://edelivery.tylertech.com/
- https://edelivery2.tylertech.com/
- https://ecsworkbench.tyler-eagle.com/

If configuring TCM via a static IP address, use:

- 18.214.7.128
- 23.22.239.32

Note: The following port range must be open for both of these IP addresses: 10943 through 10950.

Person Data Sharing

For Person Data Sharing, access to port 443 in the following location is required:

- https://sqs.us-gov-west-1.amazonaws.com

EagleView

For agencies using EagleView (formerly known as Pictometry), access to the following external locations is required:

- https://api.eagleview.com
- https://connect-link.eagleview.com
- https://unpkg.com/react@17
- https://unpkg.com/react-dom@17

Tyler Quick Client Utility

For agencies that plan to use the Tyler Quick Client Utility to install client software, access to the following external location is required to receive updates automatically as they are posted.

- https://tylerutilityapi.azurewebsites.net

Enterprise Security

Service	TCP Listening Port	Communication	Purpose
Enterprise Security	88 636 389	Server to server	Ports for Integrated Authentication or Active Directory.

GIS Ports and Services

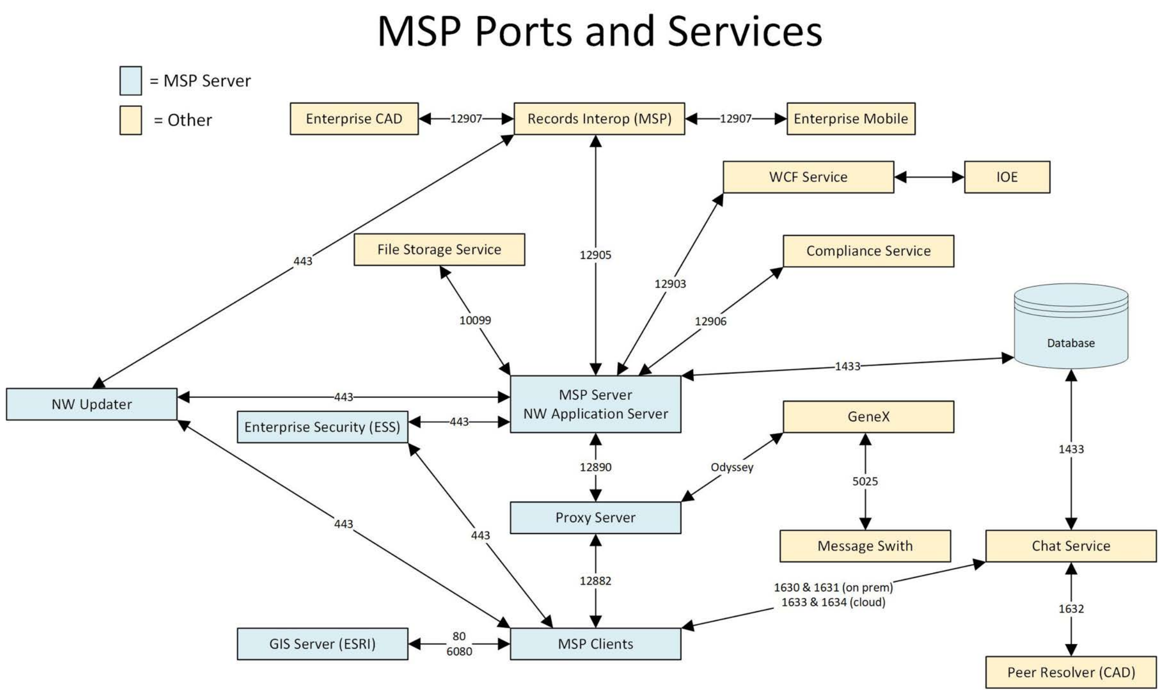
Service	TCP Listening Port	Communication	Purpose
ArcGIS Server or Public Safety GIS Tools	6080 6443	Client to server, server to client, server to server	Tools for managing GIS data and providing advanced CAD Functionality.
Map Maintenance	80	ArcGIS server	Is used to maintain Map Related data and settings for all products Must be open from all MSP, Enterprise Mobile, and Enterprise CAD clients.
DB	1433-TCP	Server to server	Outbound to DB Server (MSSQL)

MSP Ports and Services

Service	TCP Listening Port	Communication	Purpose
New World MSP Communication Framework	61616	Server to server	Message bus for processing inbound messages from New World Integration Service.
New World Integration Service	7000	Server to server	Exposes port 7000 for hosting APIs. This port needs to be accessible to the New World Records Interop. This port needs to be externally accessible to the Enterprise Records Integration Service Instance.
New World Chat (on prem)	1630	Client to server	
New World Chat (cloud)	1633	Client to server	
New World Chat Maintenance (on prem)	1631	Client to server	
New World Chat Maintenance (cloud)	1634	Client to server	
New World Peer Resolver	1632	Server to server	Optional service, only installed if Enterprise CAD is not used.
NW Application Server	12890 12903 12905	New World WCF Services, New World Records Interop Service	Is the primary server for the MSP Client Applications.
New World File Storage	10099	Server to server	Provides access to all documents needed by the MSP Applications.
New World WCF Services (Reporting)	12903 12904	Client to server	NW Remoting Service New World Windows Sync Service New World File Storage.
New World WCF	12903	Server to server	Provides data access services to the MSP DB.

Service	TCP Listening Port	Communication	Purpose
New World Records Interop	12882 12905 12886 12897 12898 12899	NWS Application Server, New World File Storage, client to server	Provides access to the Records system for Enterprise CAD, Enterprise Mobile, and the iPad applications. Additionally MSP applications connect to it for running reports. Server for the New World Sync Service, Access point for interfaces to interact with the NW Application Server.
New World Compliance Service	12906	Client to server	
New World Records Interop REST Service	12907	New World Mobile Server	Brazos Integration.
New World Automatic Updater	80	IIS (Website where the updates are hosted)	Using the Background Intelligent Transfer Service to download updates of software.
New World Windows Sync	12886 12897 12898 12899	NW Remoting Service	Provides a local cache of Validation Sets and Master Files.
New World Data Access Services	80 (hosted in IIS)		Provides data access services to the MSP DB for the LERMS.NET client and some interfaces.
NWS Proxy Server	12882	Client to server	Configurable in MSP System Settings. Provides buffered asynchronous communication from the MSP Client Applications and the NWS Application Server. **NOTE:** This is not a system service, but rather a process launched by the NW Application Server.
NW GENEX Engine	Depends on configured interfaces	NW Application Server to Message Switch	Hosts interfaces for NCIC, E911, Enterprise Mobile (10x), and other custom interfaces for working with the NW Application Server.
Master Data Service	443 (hosted in IIS)	Records Interop, Enterprise CAD	Synchronization of validation sets and master files between remote systems.
Enterprise Security	443	Server to server Client to server	

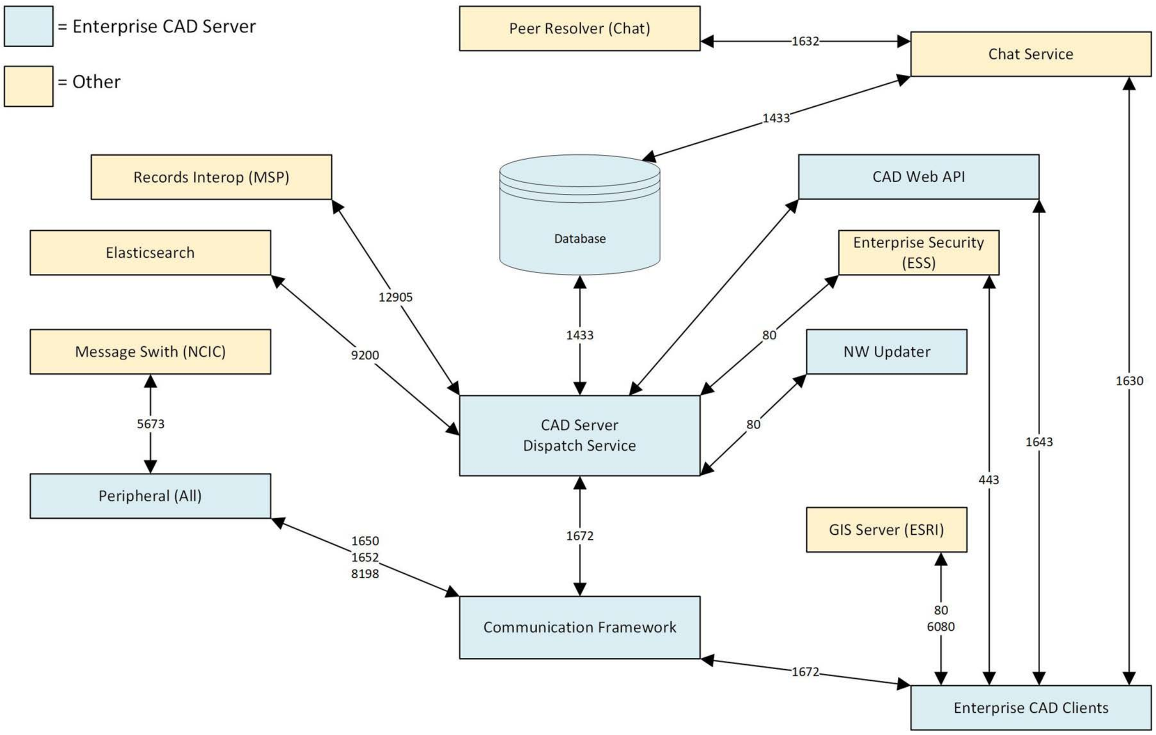
Service	TCP Listening Port	Communication	Purpose
Chat services between Enterprise Mobile, Enterprise CAD, and MSP	Dynamic Ports 49512-65535	Server to server	Server to Server Chat Communication. Ports are relevant when Enterprise Mobile and/or MSP server are in a different network than the Enterprise CAD Server.
DB	1433-TCP	Server to server	Outbound to DB Server (MSSQL)



Enterprise CAD Ports and Services

Service	TCP Listening Port	Communication	Purpose
Enterprise CAD Communication Framework	1670 -TCP	Internal communications	Public Safety suite communication framework service used to message requests and data across application layers.
Enterprise CAD Communication Framework	1671-TCP	External communication	Enterprise CAD to CAD Interfaces.
Enterprise CAD Dispatch	1671 1672	Client to server	Is the primary server for Enterprise CAD clients.
OpenSearch	9200 - HTTP or HTTPS (requires Xpack)	Server to server	OpenSearch
Enterprise CAD Peripheral Services	1650 1652 8198	CAD Dispatch Service	Hosts interfaces such as E911, Paging, Telestaff, toning, etc.
Enterprise Chat	1630 1631	Client to server	Chat server.
Enterprise Peer Resolver	1632		Provides communication services for chat.
Enterprise Automatic Updater		Client to server Server to server	Uses Inter-Process Communication (IPC) channel and Background Intelligent Transfer Service (BITS) to download updates of software and GIS Data.
Enterprise CAD Web API	1643	Server to server	Allows Mobile to CAD communication.
Enterprise Security	443	Server to server Client to server	
Chat services between Enterprise Mobile, Enterprise CAD, and MSP	Dynamic Ports 49512-65535	Server to server	Server to Server Chat Communication. Ports are relevant when Enterprise Mobile and/or MSP server are in a different network than the Enterprise CAD Server.
DB	1433-TCP	Server to server	Outbound to DB Server (MSSQL)

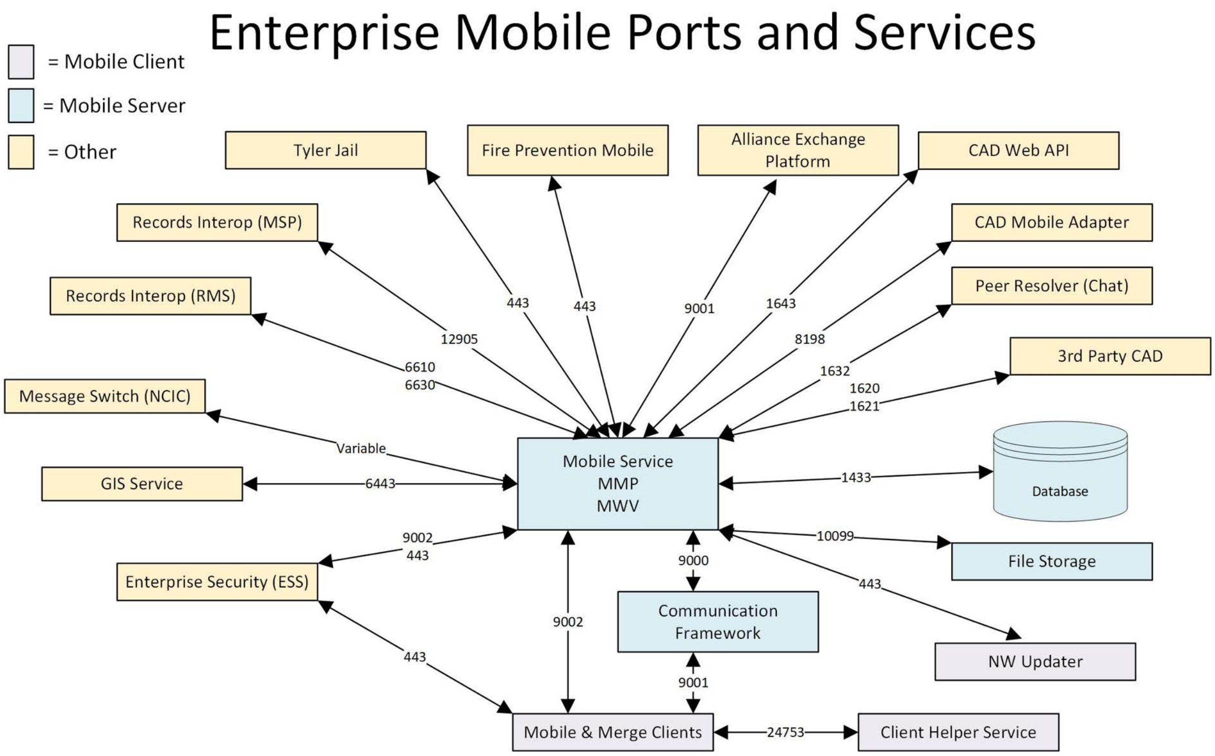
Enterprise CAD Ports and Services



Enterprise Mobile Ports and Services

Service	Listening Port	Communication	Purpose
Message Switch	Variable	Server to server	Provides access to NCIC Data. TLS encrypted communications supported. **NOTE:** This runs on the AIX box.
Enterprise Communication Framework	9001 - SSL	Enterprise- Mobile Services	Enterprise suite communication infrastructure service used to message requests and data across application layers.
New World File Storage	10099	Server to services	Storage of field reports. Firewall exception may not be required since this runs on same box as the Enterprise Mobile server.
Enterprise- Mobile Services	9001 9002		Provides services for Enterprise Mobile Clients.
Enterprise Security	443	Server to server Client to server	
GIS Server	6443	Server to client	To derive nearest intersection when using Create Call.
Enterprise CAD Web API	1643	Server to server	Allows Mobile to CAD communication.
Chat services between Enterprise Mobile, Enterprise CAD, and MSP	Dynamic Ports 49512-65535	Server to server	Server to Server Chat Communication. Ports are relevant when Enterprise Mobile and/or MSP server are in a different network than the Enterprise CAD Server.
Database	1433-TCP	Server to server	Outbound to DB Server (MSSQL)

Note: For Virtual Message Switch ports and services information, refer to the *New World Public Safety Technical Services Implementation Reference Guide* on Tyler Community.

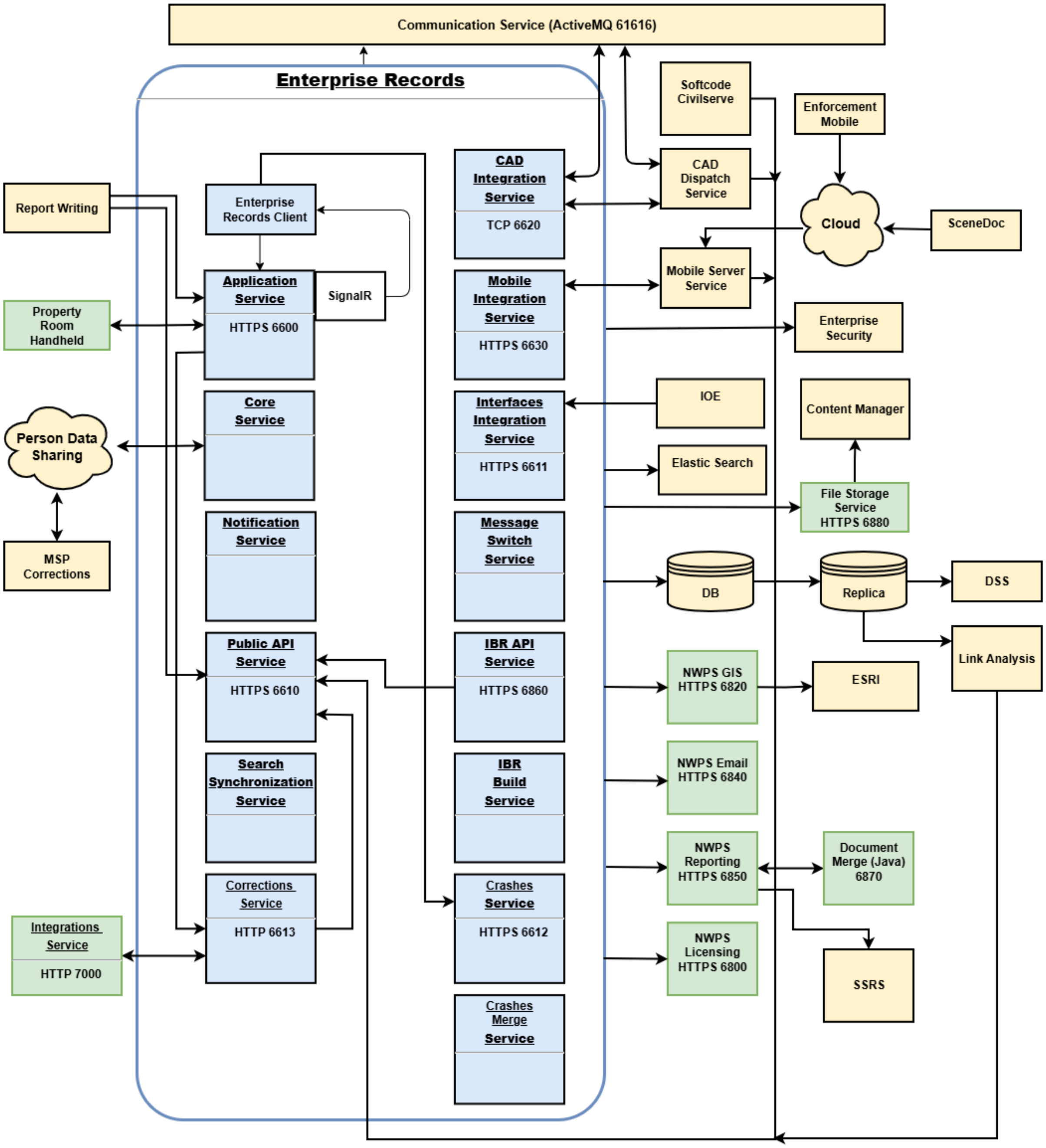


Enterprise Records Ports and Services

If the port is listed as HTTPS it is secure. HTTP is not secure.

Service	Listening Port	Communication	Purpose
DB	1433 -TCP	Server to server	Outbound to DB Server (MSSQL)
CAD Server	1643 -HTTPS	Server to server	Allows Mobile to CAD and Records to CAD communication
Communication Server	61616 - TCP	Server to server	Outbound to Communication Service
OpenSearch	9200 - HTTP or HTTPS (requires Xpack)	Server to server	Outbound to OpenSearch
ESS Identity Service	443 - HTTPS, WSS	Client to server	User Authentication to Enterprise Records
RMS Application Service	6600 - HTTPS, WSS	Inbound port to host site, APIs, and web socket SignalR connections	Exposes port 6600 for hosting web content and APIs. This port needs to be accessible to end-users wishing to access the RMS web application.
RMS CAD Service	6620 - HTTPS	Server to server	Exposes port 6620 for hosting APIs. This port needs to be accessible by internal RMS services.
RMS Compliance Service	6860 - HTTPS	Server to server	Exposes port 6860 for hosting APIs. This port needs to be accessible by internal RMS services.
RMS Corrections Service	6613 - HTTPS	Server to server	Exposes port 6613 to for hosting APIs for consumption by RMS Application Service.
RMS Crash Service	6612 - HTTPS	Inbound port to host site, APIs, and web socket SignalR connections	Exposes port 6612 for hosting web content and APIs. This port needs to be accessible to end-users wishing to access the Crash module.
RMS Email Service	6840 - HTTPS	Server to server	Exposes port 6840 for hosting APIs, currently hosted as a sub-service of the Core Service. This port needs to be accessible by internal RMS services.
RMS GIS Service	6820- HTTPS	Server to server	Expose 6820 for hosting APIs .This port needs to be accessible to end-users wishing to access the RMS web application. This port needs to be accessible by internal RMS services.
RMS GIS Service	6443 -HTTPS	Server to server	Communication to GIS server

Service	Listening Port	Communication	Purpose
RMS Integration Service	7000 - HTTPS	Server to server	Exposes port 7000 for hosting APIs. This port needs to be accessible to the RMS Corrections Service. This port needs to be externally accessible to the MSP Integration Service Instance.
RMS License Service	6800 - HTTPS	Server to server	Exposes port 6800 for hosting APIs. This port needs to be accessible by internal RMS services.
RMS Message Switch Service	Variable	Server to server	Outbound connection to a Message Switch
RMS Mobile Field Reporting Service	6630 - HTTPS	Server to server	Exposes port 6630 for hosting APIs. This port needs to be accessible by internal RMS services
RMS Reporting Service	6850 - HTTP	Server to server	Exposes port 6850 for hosting web content and APIS. This port needs to be accessible to end-users wishing to access the RMS web application. This port needs to be accessible by internal RMS services
SceneDoc	443 - HTTPS	Server to server	
File Storage Service	6880 - HTTPS	Server to server	For connecting to Content Manager.
TCM	6811 - HTTPS	Server to server Client to server	Manages all flat files associated with records such as mug shots and any other flat files attached to incidents, cases, arrests, etc.



Communication Service (ActiveMQ 61616)
Enterprise Records
Report Writing
Enterprise Records Client
Application Service
HTTPS 6600
SignalR
Property Room Handheld
Person Data Sharing
MSP Corrections
Core Service
Notification Service
Public API Service
HTTPS 6610
Search Synchronization Service
Corrections Service
HTTP 6613
Integrations Service
HTTP 7000
CAD Integration Service
TCP 6620
Mobile Integration Service
HTTPS 6630
Interfaces Integration Service
HTTPS 6611
Message Switch Service
IBR API Service
HTTPS 6860
IBR Build Service
Crashes Service
HTTPS 6612
Crashes Merge Service
Softcode Civilserve
CAD Dispatch Service
Enforcement Mobile
Cloud
SceneDoc
Mobile Server Service
Enterprise Security
IOE
Content Manager
Elastic Search
File Storage Service
HTTPS 6880
DB
Replica
DSS
Link Analysis
NWPS GIS
HTTPS 6820
ESRI
NWPS Email
HTTPS 6840
NWPS Reporting
HTTPS 6850
Document Merge (Java)
6870
SSRS
NWPS Licensing
HTTPS 6800

Decision Support Software Ports and Services

Service	Listening Port	Communication	Purpose
Analysis Services **(For Default Instance)**	2383	Inbound Connections on the DSS/Report Server	Allows connectivity between the DSS cubes (SQL Analysis Services) and client tools.
Analysis Services **(For Name Instance)**	2382	Inbound Connections on the DSS/Report Server	Allows connectivity between the DSS cubes (SQL Analysis Services) and client tools.
SQL Server Browser **(For Default Instance)**	1433	Inbound Connections on the DSS/Report Server	Allows connectivity between the DSS data warehouse and client tools. This port is necessary for direct database connections to the data warehouse via Excel, Power BI, Crystal Reports, etc.
SQL Server Browser **(for Name Instance)**	1434	Inbound Connections on the DSS/Report Server	Allows connectivity between the DSS data warehouse and client tools. This port is necessary for direct database connections to the data warehouse via Excel, Power BI, Crystal Reports, etc.

What's New in Enterprise Public Safety 2026.3

Product Enhancement Guide

Last revised on 8-26-26

Empowering people who serve the public®

Table of Contents

Chapter 6

Introduction

What's New in Enterprise Public Safety 2026.3

This *Product Enhancement Guide* describes the changes made in the **2026.3** version of the *Enterprise Public Safety* suite of applications. Some enhancements are application-specific, some involve multiple applications, and some are suite-wide.

MSP Enhancements in What's New Guide Only

MSP enhancements are only documented in the *What's New Guides*, as was announced in the *2025.1 What's New Guide*. PDF guides and in-app *Online Help* will no longer be updated. The last available version of any of the *MSP* guides posted on the *Documentation* page of *Tyler Community - Public Safety* is **2024.2**.

MSP Prerequisites Changes

In **2026.3**, the following changes have been made to *MSP*.

- *Microsoft Edge WebView2* is required on client machines. This is included with *Windows 11* and recent updates of *Windows 10*. For older machines that have not been updated to a recent version of *Windows*, *Microsoft Edge WebView2* needs to be downloaded and installed.
- *MSP* servers no longer require *Microsoft Office*.

Organization of this Update Guide

Chapters within this *Product Enhancement Guide* are organized by application. Enhancements that affect multiple *MSP/Enterprise* applications, such as various *MSP Maintenance* modules and other suite components, appear in standalone chapter titled *Public Safety Suite*.

Enhancements in each chapter are organized by module. For every form, tab, task, or other software component described in this guide, the following information is provided:

- An indication of how the component is accessed within the software
- If available, a description of what prompted the enhancement
- A summary of the change(s)

Additional Documentation Resources

Use the following links to access additional release documentation:

- Release Notes

Documentation Style Conventions

Below are the formatting conventions used within this document:

Formatting Convention	Type of Information Represented
Bold	Buttons, menus, list selections, menu selections.
Bold and Italic	Check boxes, text boxes, options, lists, columns that can be edited.
<bold in brackets>	Keyboard buttons. For example, **<shift>**.
Initial Caps Only	Icons, grids, columns that cannot be edited.
Italic	Windows, pages, tabs, sub-tabs, vertical tabs, dialogs, sections, frames.

Icon Legend

Below is a list of icons that may be used in this document.

Icon	Type
	Note
	Tip
	Best Practice
	Warning

Chapter 1
Enterprise CAD

Introduction

This chapter describes enhancements made in the **2026.3** version of *Enterprise CAD*. It includes any enhancements made to the suite of applications included with *Enterprise CAD*.

Click the links below for more detailed information about the *Enterprise CAD* enhancements included in this release:

❖ ❖ ❖ ❖ ❖

Maintenance Client Enhancements

The *Enterprise CAD Maintenance Client* application allows *Enterprise CAD* system administrators to set up critical functionality for the *Enterprise CAD Dispatch Client* application. By having the maintenance functionality separate from the dispatch and mapping functionality, system administrators can perform setup steps without having the other applications open or even loaded on the same machine.

See the following sections for details about *Maintenance Client* enhancements in **2026.3**:

New Mileage tracking

- "Call Export — Include Mileage Tracking" on page 7
- "ASAP Maintenance — Added AWS Connection Settings" on page 8
- "Call Maintenance — Audible Alerts for Critical Global & Phone Alert Desktop Notifications" on page 9
- "Call Maintenance— Custom View Editor— Save Restricted Narrative Option" on page 12
- "Call Types — Automatically Transfer CAD to CAD Calls when Require Ready for Dispatch Selected" on page 21

❖ ❖ ❖ ❖ ❖

Call Export — Include Mileage Tracking

In **2026.3**, the Call Export XSD file now includes mileage tracking. It includes the beginning and ending mileage entered in the *Unit Log* in the *Enterprise CAD Dispatch Client*.

New mileage tracking

Below is an example of the XML export file including the mileage tracking:

```
-<UnitLog>
<Action>Mileage Tracking</Action>
<DateTime>2025-09-12 17:21:40Z</DateTime>
<Description>Mileage: 0.00, Unit: 1B4</Description>
<Location i:nil="true"/>
<Status>Transport</Status>
</UnitLog>
-<UnitLog>
<Action>Unit Location</Action>
<DateTime>2025-09-12 17:22:08Z</DateTime>
<Description>15600 NE 8TH ST, BE</Description>
<Location>15600 NE 8TH ST, BE</Location>
<Status>Arrived</Status>
</UnitLog>
-<UnitLog>
<Action>Unit Status Change</Action>
<DateTime>2025-09-12 17:22:08Z</DateTime>
<Description>Arrived</Description>
<Location i:nil="true"/>
<Status>Arrived</Status>
</UnitLog>
-<UnitLog>
<Action>Unit Location</Action>
<DateTime>2025-09-12 17:22:08Z</DateTime>
<Description>@Jail</Description>
<Location>@Jail</Location>
<Status>Arrived</Status>
</UnitLog>
-<UnitLog>
```

```
<Action>Mileage Tracking</Action>
<DateTime>2025-09-12 17:22:08Z</DateTime>
<Description>Mileage: 2.30, Unit: 1B4</Description>
<Location i:nil="true"/>
<Status>Arrived</Status>
```

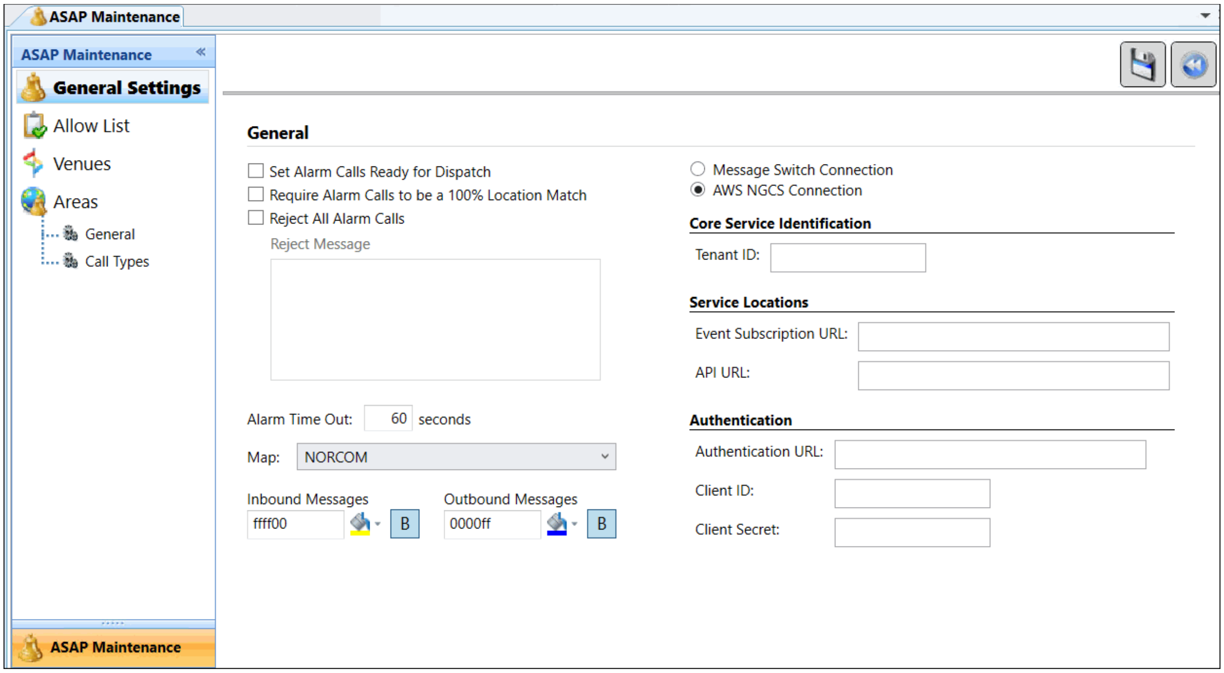
ASAP Maintenance — Added AWS Connection Settings

ASAP Maintenance allows system administrators to designate general ASAP settings; an allow list of cities, counties, and states from which the PSAP accepts alarm locations; and ASAP venues, areas and their associated mapped call types.

The *General Settings* window allows system administrators to set up general ASAP settings such as message switch connection settings, only accepting ASAP calls with a 100% location match, designating when to reject all alarm calls and the message that would accompany those rejections, an alarm timeout duration, the map being used, inbound and outbound message characteristics.

When configuring connections for the ASAP feature, users want to select either the Message switch connection or the AWS NGCS connection settings, allowing them to manage connections effectively.

In **2026.3**, a new ***AWS NGCS Connection*** option has been added to the *General Settings* window of *ASAP Maintenance*. This change introduces another option for the state ***Message Switch Connections***. These options toggle the fields associated with them. Only one option can be selected.



The Connection sub-section contains ***Tenant ID***, ***Event Subscription URL***, ***API URL***, ***Authentication URL***, ***Client ID***, and ***Client Secret*** that are set up by *Tyler Technologies* implementation professionals during configuration and customer registration with *AWS* and ASAP.

Call Maintenance — Audible Alerts for Critical Global & Phone Alert Desktop Notifications

The *Call Maintenance* module contains functionality related to setting up call defaults, jurisdictional settings, call types, EMD devices and related settings, EMD codes, toning devices, scheduled tones, global and phone alert settings, call priorities, custom user interface views and defaults, call export settings, service vehicle rotations, dispatch positions and area assignments, radio channels, questionnaires, paging, and ASAP settings.

In **2026.3**, enhancements have been made to the *Global Alerts* and *Phone Alerts* windows of *Call Maintenance* such that dispatchers managing active calls for service can now receive audible alerts alongside desktop notifications for critical global alerts and phone alerts. Previously, critical alert desktop notifications were only visual, which could be easily overlooked during high-activity periods.

This enhancement ensures dispatchers are immediately aware of critical alerts through a distinct audio cue, improving situational awareness and response times.

See the following sections for more detailed information about these enhancements:

- "Global Alerts" on page 10
- "Phone Alerts" on page 11

Global Alerts

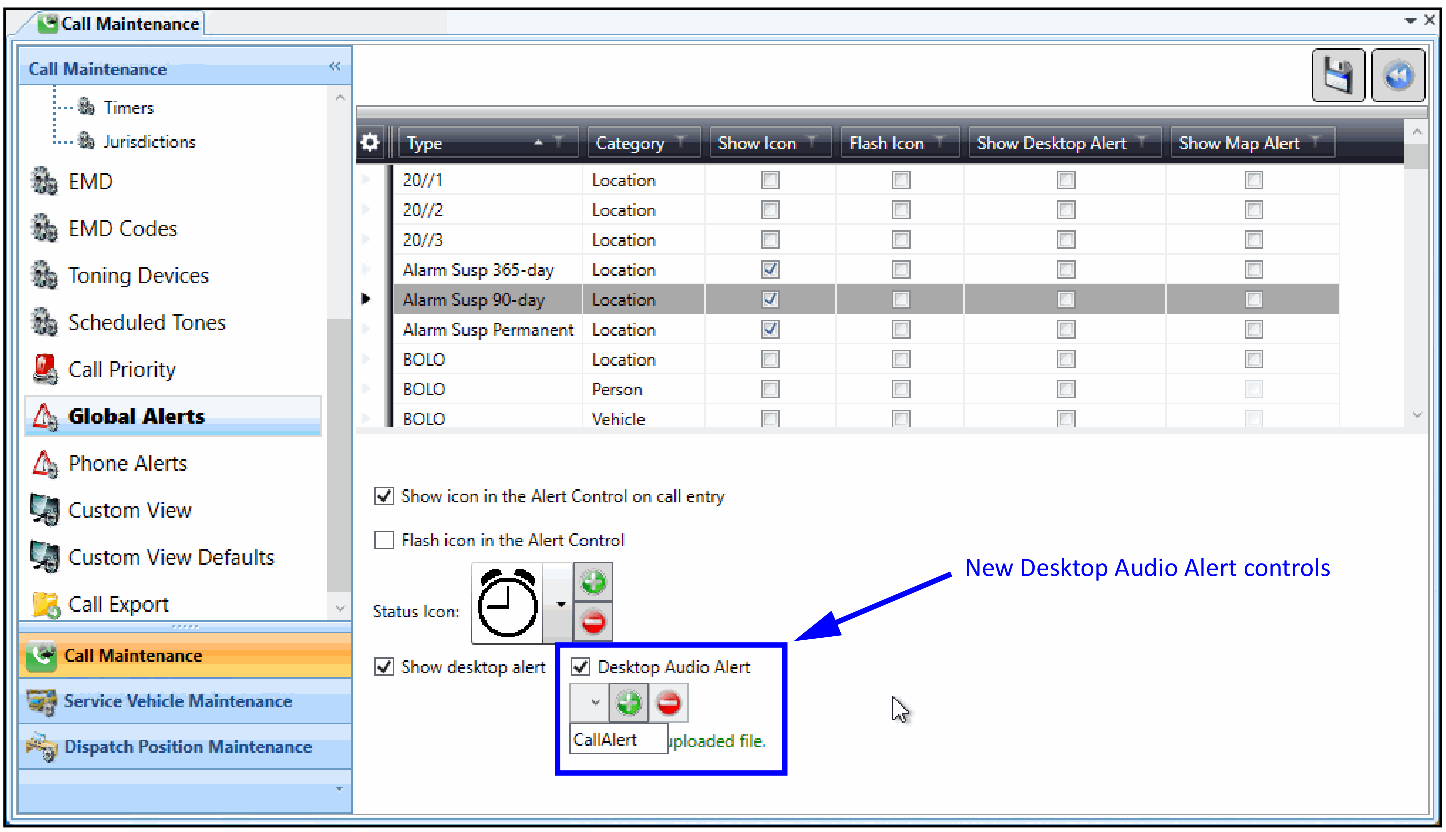
The *Global Alerts* window, accessed by clicking the **Global Alerts** button on the *Call Maintenance* window, allows system administrators to designate alert icons for specific alert types as well as set whether specific alert types display a desktop alert and/or appear in the optional ***Alert Control*** field on a custom *CFS Entry* window.

New ***Desktop Audio Alert*** controls have been added, allowing CAD administrators to upload and assign a custom audio file that sounds in the *Dispatch Client* for critical global alerts.

When a desktop alert is triggered for a critical global alert on a CFS, the selected sound file plays automatically, alerting the dispatcher.

These controls are only available when the ***Show Desktop Alert*** check box is selected.

As with other audio controls in the software, administrators click the **Add** button to browse to and select an audio file or the **Delete** button to delete any existing audio files. If this check box is selected and users try to **Save** without selecting a file, a You *must specify an audio alert file if audio alert is enabled* error message displays.



Phone Alerts

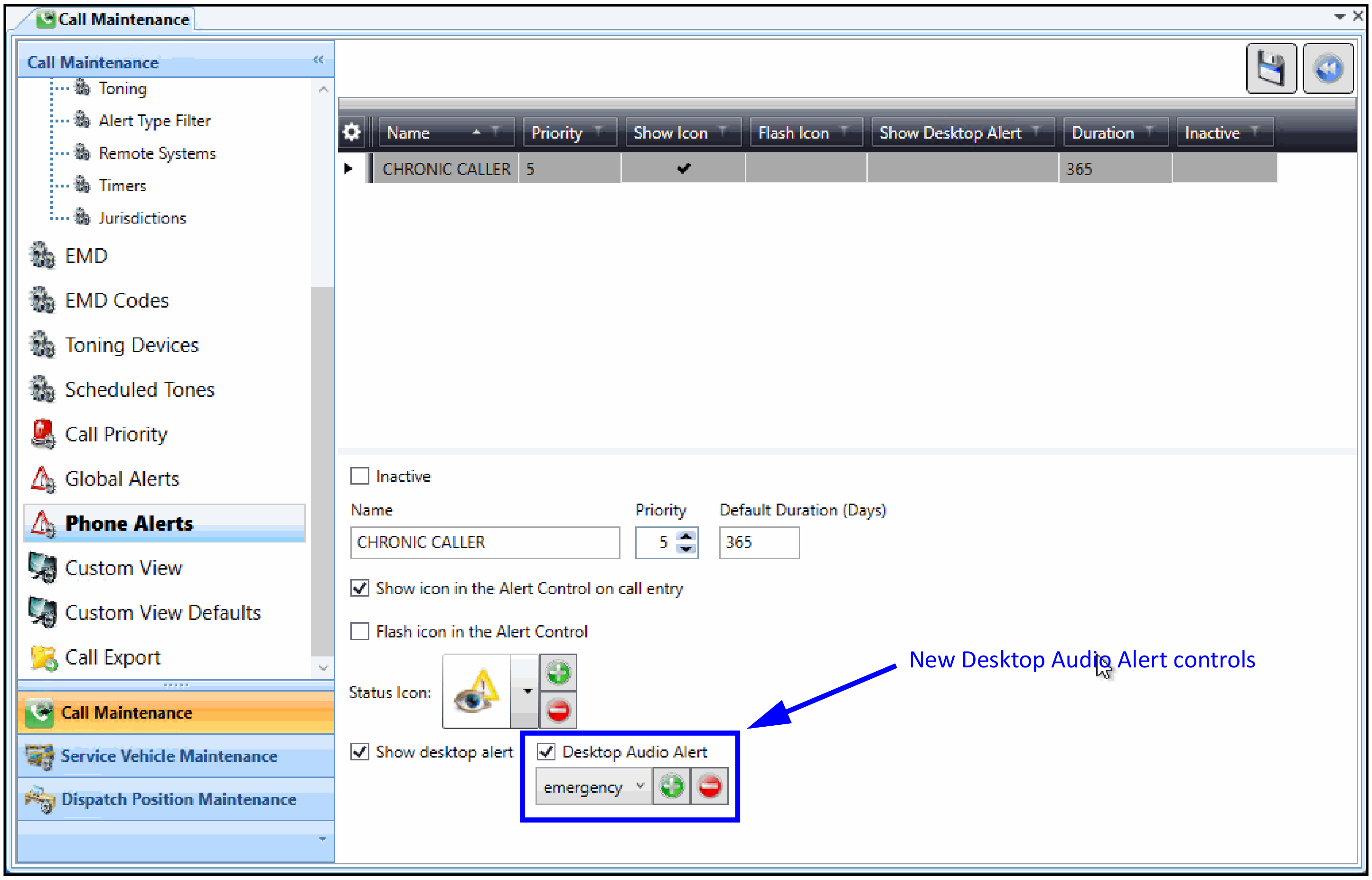
The *Phone Alerts* window, accessed by clicking the **Phone Alerts** button on the *Call Maintenance* window, allows system administrators to enter and maintain alerts for phone numbers. While several of the controls are identical to ones found on the *Global Alerts* window, there are several controls specific to phone alerts.

New ***Desktop Audio Alert*** controls have been added, allowing CAD administrators to upload and assign a custom audio file that will sound in the *Dispatch Client* for critical phone alerts.

When a desktop alert is triggered for a critical phone alert on a CFS, the selected sound file plays automatically, alerting the dispatcher.

These controls are only available when the ***Show Desktop Alert*** check box is selected.

As with other audio controls in the software, administrators click the **Add** button to browse to and select an audio file or the **Delete** button to delete any existing audio files. If this check box is selected and users try to **Save** without selecting a file, a You *must specify an audio alert file if audio alert is enabled* error message displays.



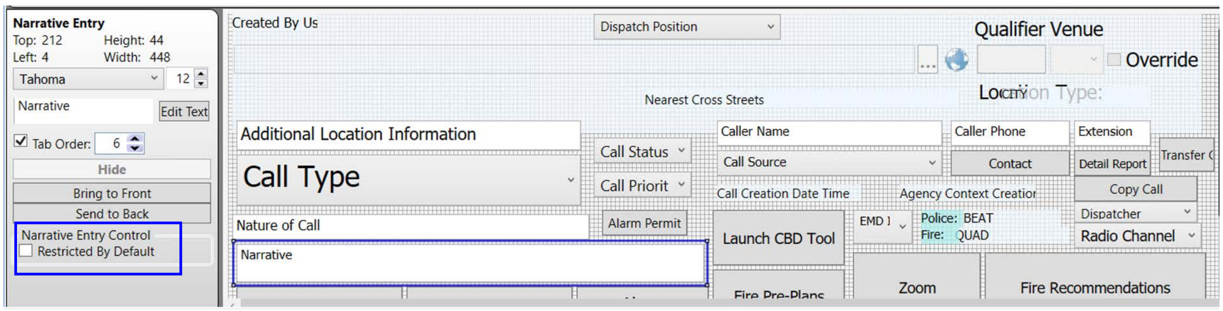
Call Maintenance— Custom View Editor— Save Restricted Narrative Option

The **Calls** toolbar group contains functionality related to setting up call defaults, jurisdictional settings, call types, EMD devices and related settings, EMD codes, toning devices, scheduled tones, global and phone alert settings, call priorities, custom user interface views and defaults, call export settings, service vehicle rotations, dispatch positions and area assignments, radio channels, questionnaires, paging, and ASAP settings.

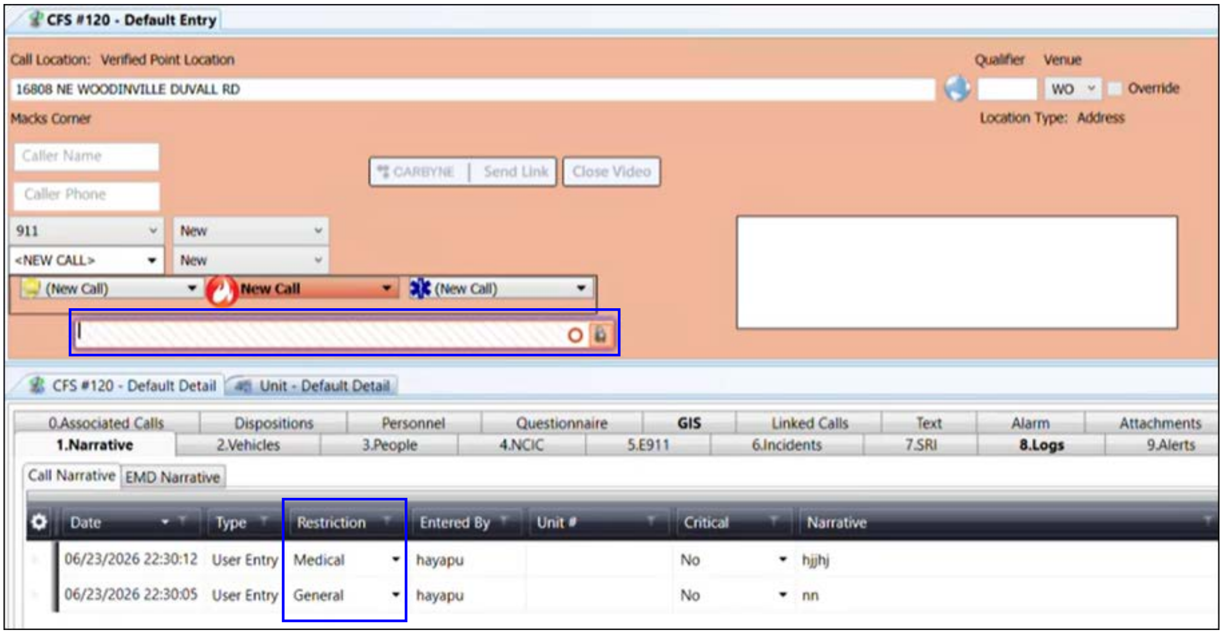
The *Custom View Editor*, accessed by clicking the **Custom View** button on the *Call Maintenance* window, allows system administrators to define a custom design for the *CFS Entry* window or *Quick Call Entry* window. The *Custom View Editor* is a drag-and-drop design and resizing tool, allowing users to customize the upper area of the *CFS Entry* window or *Quick Call Entry* window. A customized window may use a different order for the entry fields, or add or remove fields altogether.

In previous releases, users had to manually restrict narratives in the *CFS Details* window. This created an extra step for the user and made it easy to miss a restriction.

Tyler Technologies strives to ensure sensitive data is not arbitrarily shared with unauthorized personnel. In **2026.3**, the restricted narrative option is saved to ensure sensitive data is restricted by Call Type. A new *Narrative Entry Control* with a ***Restricted by Default*** option has been added to the *Custom View Editor*.



When selected, Narratives are automatically restricted by Call Type in a Call for Service in the *CAD Dispatch Client*. For example, if the Call Type is medical, the ***Narrative*** field automatically is marked restricted. When using the layout, as narratives are added to the call, they are labeled in the *Narrative* grid according to the Call Type, such as Medical or Law.



Another example is that police dispatchers could use the Police Dispatch CFS Layout that has the ***Restricted Narrative*** enabled, resulting in every call created by a dispatch client using that layout defaulting to a restricted narrative labeled Law.

Units — Response Plan Maintenance — Improved Design and Controls

The **Units** toolbar group contains all functions used to set up unit default settings, units, unit types, unit mileage types, unit toning, unit contacts, unit statuses, stations, cross-staffing groups, auxiliary unit types, TeleStaff™ settings, and response plans. The *Unit Maintenance* window contains links to all the windows that are used to set up a unit within an agency. Having all the setup options located in one location allows system administrators to quickly enter, update, or cross staff units in their agency.

The *Response Plan Maintenance* window, accessed by clicking the **Response Plan Maintenance** button from the *Unit Maintenance* window, allows system administrators to designate their recommendation defaults, set up response plans, response plan assignments, beat backups, station order, response groups, replace a unit in the system, define capabilities, assign capabilities, define modes of operation, set up area groups, set up mutual aid requests/responses, designate resource depletion settings, and request remote assistance. When the units of a beat are already deployed to a call for service and another call is received, the dispatcher would then dispatch units from the backup beat. Alternatively, if units from a specific station are already deployed to a call, subsequent calls would be dispatched to the backup station. When a unit is replaced in the system, response plans that utilized the replaced unit is automatically updated with the replacing unit. Administrators can also limit the use of station resources on the *Station Order* window to ensure stations have resources available for incoming incidents.

Response Plan Maintenance can be complex and confusing. In previous releases, the controls were not intuitive.

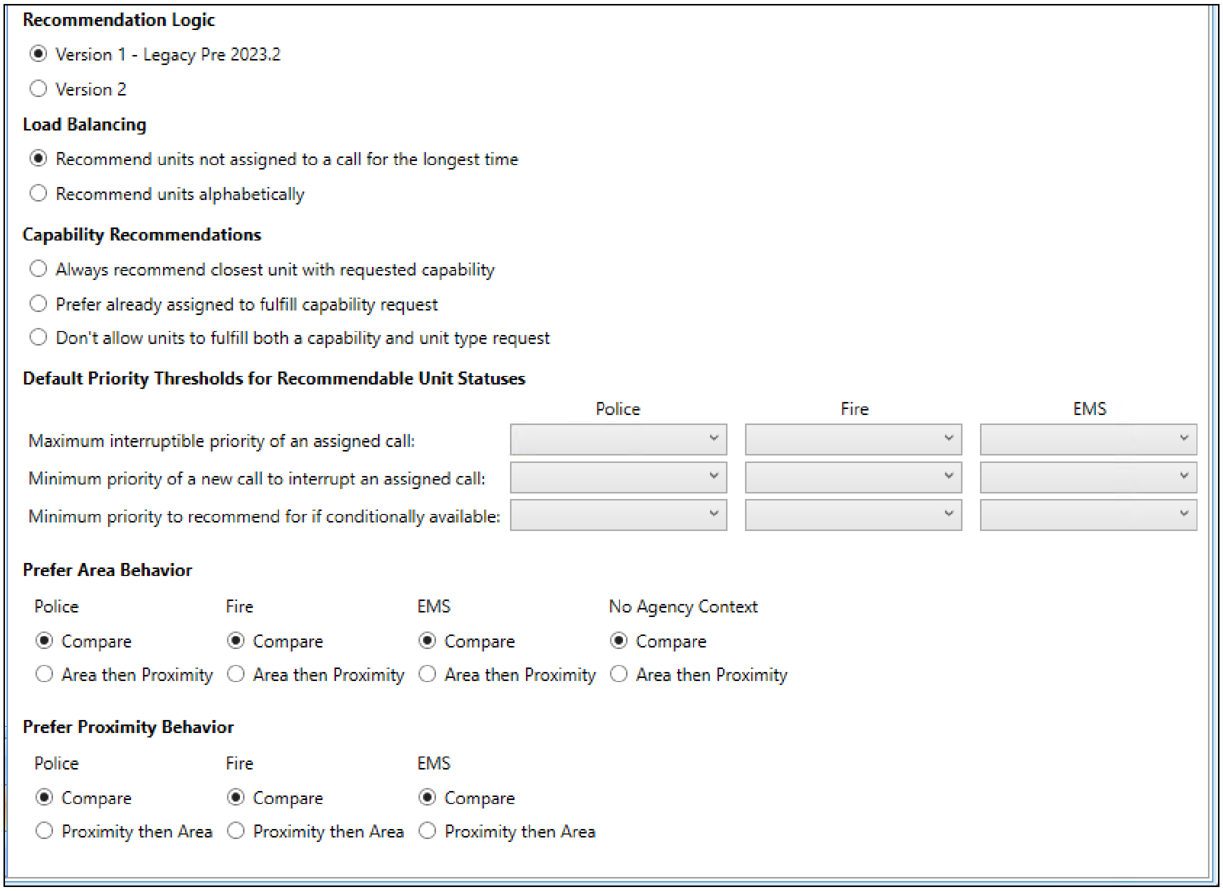
In **2026.3**, improvements were made to the controls and design of the *Response Plan Maintenance* window to assist users in creating effective response plans. This enables users to fulfill their needs for unit recommendations in the *Dispatch Client*.

See the following:

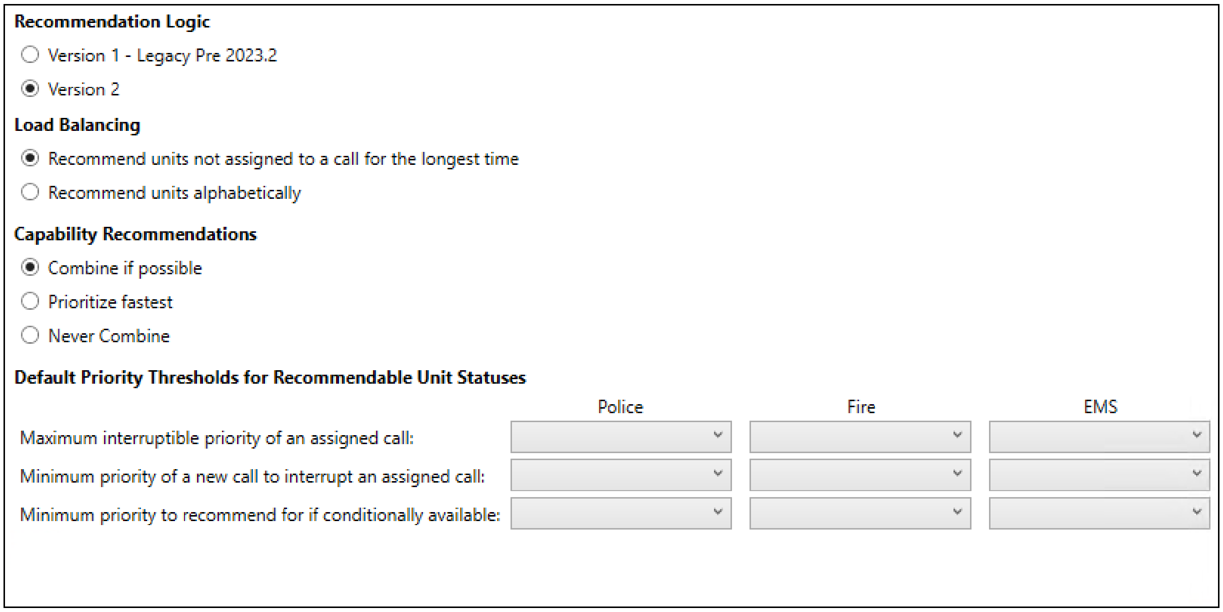
- "Recommendation Defaults — Only Version Controls and Options Display when Version is Selected" on page 15
- "Response Plans— Plan Logic Column Removed From Recommendation Logic Version 1" on page 17
- "Response Plans— Made Response Plan Order Arrow Buttons Larger" on page 18
- "Response Plans— Numbers Added to Plan Resources when Strict Ordering is Enabled" on page 19
- "Response Plan — Added Tool Tips to Complex Controls" on page 20

Recommendation Defaults — Only Version Controls and Options Display when Version is Selected

In previous versions, all controls displayed regardless of the selected *Recommendation Logic* version. This caused confusion about the options available and how each version behaves.



In **2026.3**, when selecting a Recommendation Engine version from the *Recommendation Logic* section in *Recommendations Defaults*, only the selected version's controls and options display. For example, when creating Response Plans with the logic set to ***Version 2***, administrators no longer see the options related to *Prefer Proximity Behavior* and *Prefer Area Behavior*.



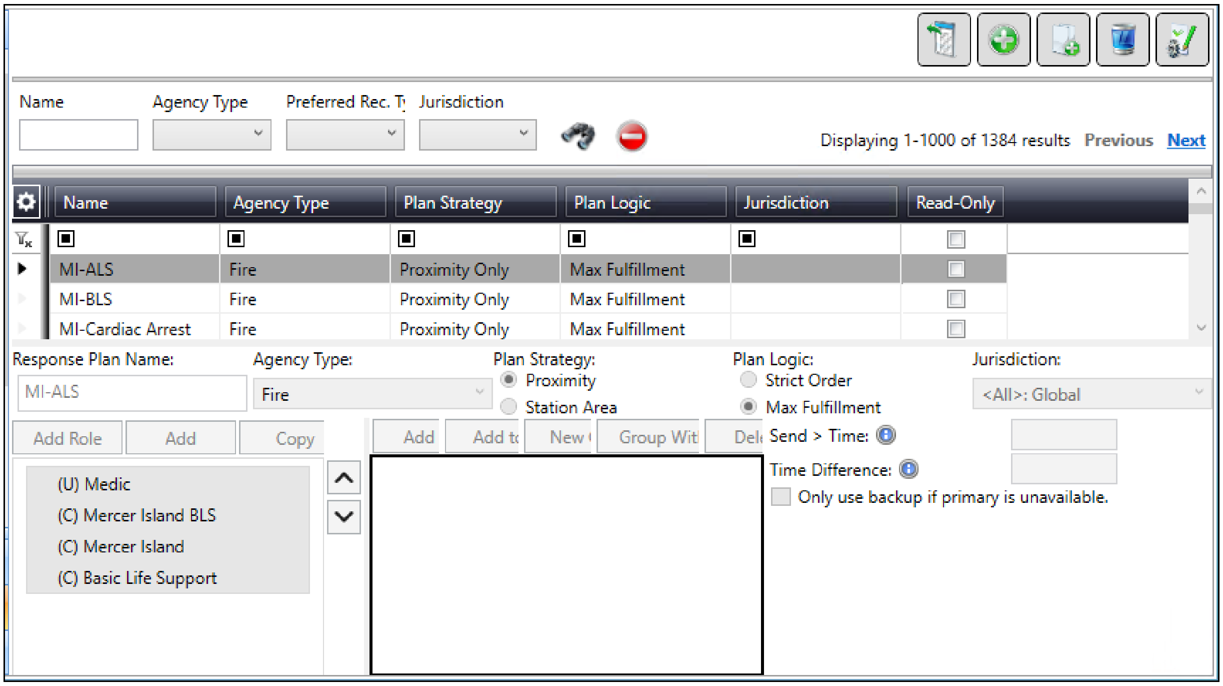
This guides administrators when creating Response Plans and reduces cluttering the page with unnecessary controls. Administrators are no longer confused by choices that are not valid for the Recommendation Logic they selected.

Additionally, the *Recommendation Logic* section has changed from a list to options. Since there are only two *Recommendation Logic* options, administrators are presented with a control that offers either one or the other option. The options are clearly displayed up front, allowing them to see their options at a glance, instead of forcing an administrator to activate a list.

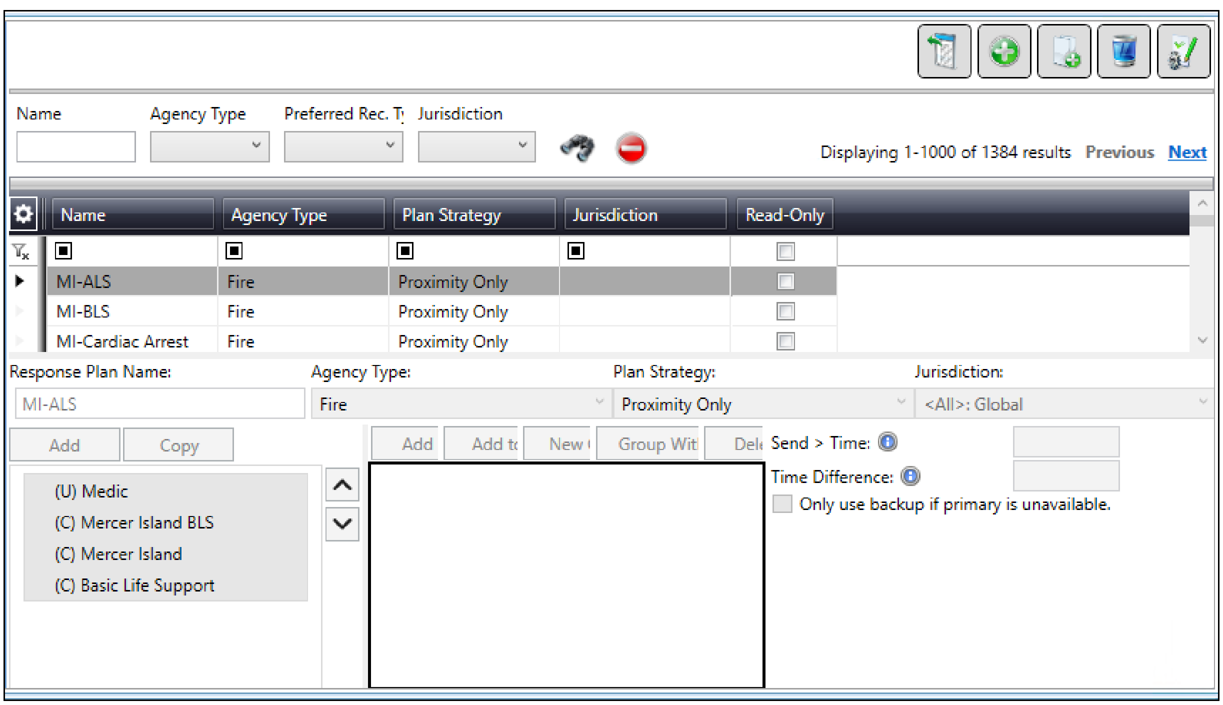
Response Plans— Plan Logic Column Removed From Recommendation Logic Version 1

When selecting ***Version 1*** from the *Recommendation Logic* section on *Recommendation Defaults*, the *Plan Logic* column does not display on the *Response Plans* window in *Response Plan Maintenance*.

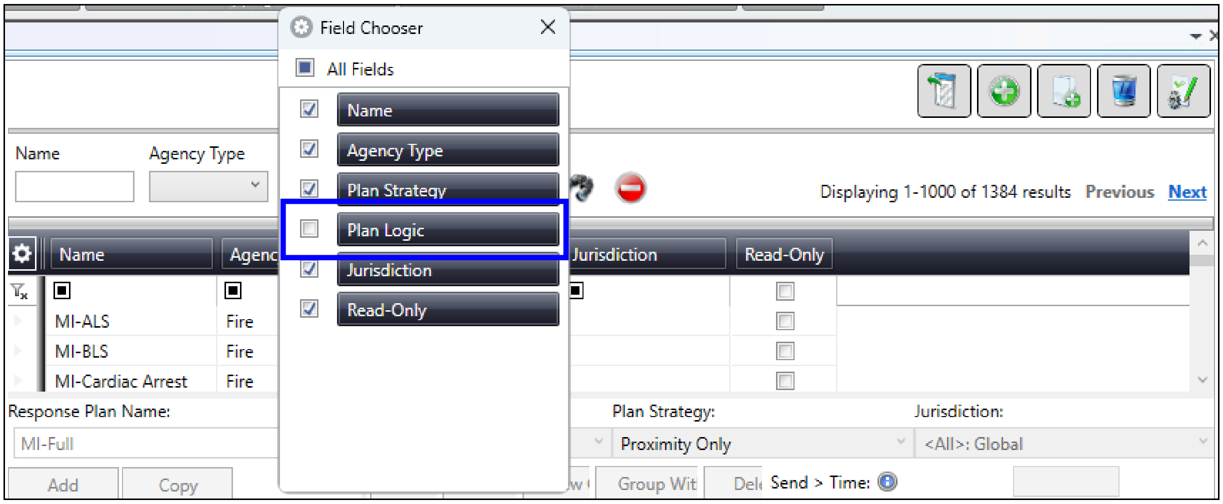
When ***Version 2*** is selected, the *Plan Logic* column displays as shown below:



When ***Version 1*** is selected, the *Plan Logic* column no longer displays as shown below:



Additionally, ***Plan Logic*** is cleared by default from the *Field Chooser* dialog of the grid column options when using ***Version 1***.



Response Plans— Made Response Plan Order Arrow Buttons Larger

When editing a Response Plan in previous versions, it was difficult to use the arrows to reorder resources in the list. The icons were too thin to easily select with a mouse.

Old Ordering Arrow buttons

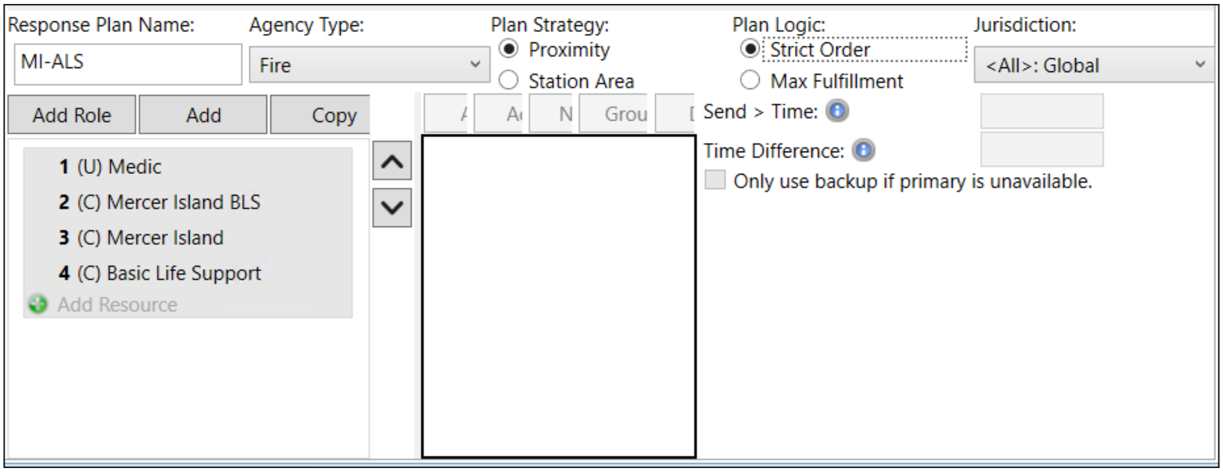
In **2026.3**, the arrows have been made larger and modernized with a larger clickable area and square borders.

New Ordering Arrow Buttons

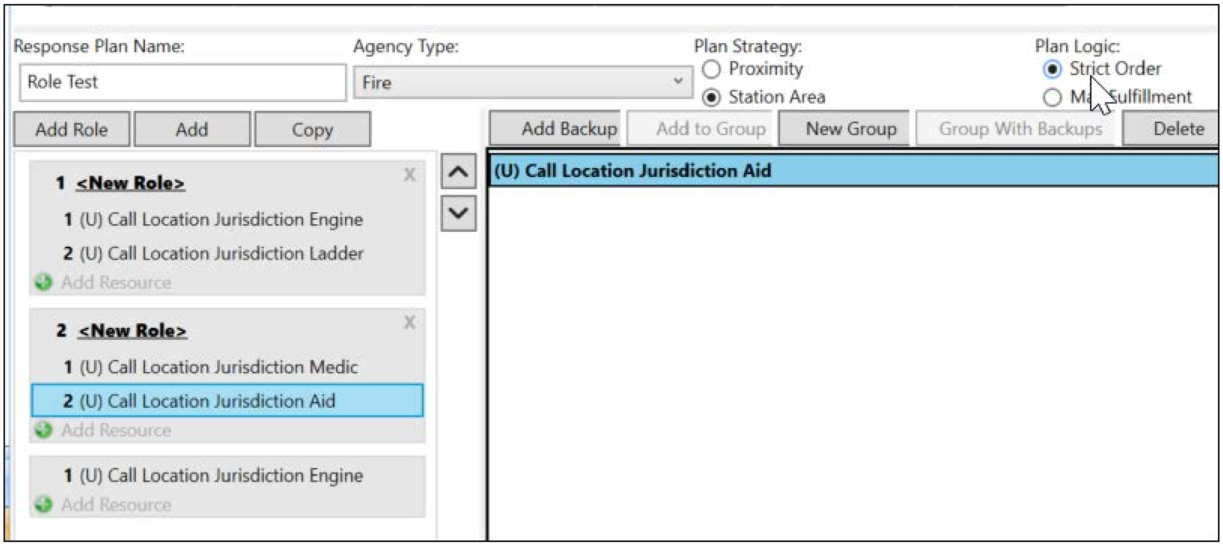
Response Plans— Numbers Added to Plan Resources when Strict Ordering is Enabled

In previous releases of Recommendation Engine version 2, when administrators selected ***Strict Ordering*** on the *Response Plan* window, there were no indicators to confirm their ordering of Response Plan resources.

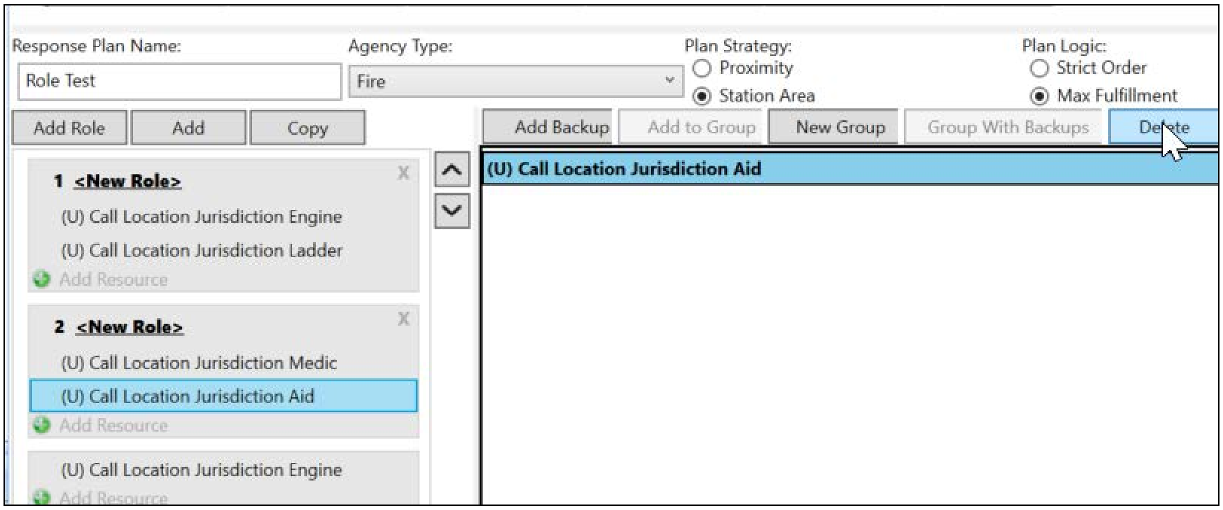
In **2026.3**, administrators can see numeric values next to each resource so that they can confirm the expected ordering in the resource list when selecting ***Strict Ordering*** for Response Plan resources. This enables at-a-glance confirmation that resources are in the needed order. Administrators can quickly verify their ordering, reducing time and mistakes.



When roles are used and ***Strict Ordering*** is enabled, the numeric order restarts under each role. For example, Role A is assigned a number 1. Then, each resource is numbered 1,2,3, etc. Role B, when inserted below, is assigned a number 2. Then, each resource under Role B is numbered 1,2,3, etc.



However, when roles are used and ***Max Fulfillment*** is enabled, the resources under each role do not receive order numbering.



Response Plan — Added Tool Tips to Complex Controls

Tyler Technologies always provides online help, user guides, and administrator guides, as well as other supplemental documentation to ensure clients can successfully use applications. Access the PDF versions of the guides on ***Tyler Community***. Access help from within each client for the specific window by pressing **<F1>**, or click the **Help** menu and choose **CAD Help** to access the entire online help system.

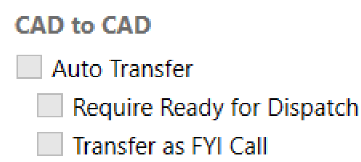
In an effort to continue to aid users with information to make using the application easier, tool tips have been added to some of the more confusing settings in the *Response Plan* window. The controls with tool tips have an icon next to them. Hover the mouse over the icon to access the tool tip for that control.

Call Types — Automatically Transfer CAD to CAD Calls when Require Ready for Dispatch Selected

Tyler Technologies has streamlined communication between two or more *Enterprise CAD* systems. These systems can be within the same agency but on different servers or from remote agencies that have been configured for inter-agency communication. Either way, the communication is seamless and allows for mutual sharing of critical information such as BOLOs or assistance requests through unit recommendations, amongst others.

When processing a call, dispatchers want to ensure all necessary fields are filled before the call is transferred to another agency. This avoids incomplete information being sent. Dispatchers accustomed to using the Ready for Dispatch workflow to process calls and mark them ready to be dispatched want to be able to use the same workflow when sending calls via CAD to CAD. They also want to ensure the call is fully ready first, as the current auto-transfer behavior immediately triggers when an applicable call type is selected. This is primarily because once a call is sent via CAD to CAD, fields other than narrative can no longer be updated.

In **2026.3**, a new ***Require Ready for Dispatch*** check box has been added to the *Call Types General* tab in *Call Maintenance* in the *Maintenance Client*. The controls have been reorganized to reside under a *CAD to CAD* section and in a sub-group under the ***Auto Transfer*** check box, making it easier to recognize the connection between options.



The ***Require Ready for Dispatch*** check box is disabled until the ***Auto Transfer*** option is selected.

When the ***Require Ready for Dispatch*** option is selected, calls do not auto transfer from the *Dispatch Client* until the **Ready for Dispatch** button is clicked.

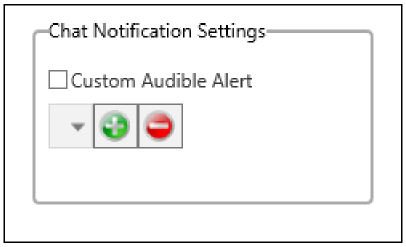
When a dispatcher clicks the **Ready for Dispatch** button, if the call type is configured for auto transfer, the call transfers to all configured default remote systems.

Administration Ribbon — System Settings — General — Add Audible Alert Options for Chat Notifications

Telecommunicators want a customizable audible alert so they do not miss important notifications when receiving new chat messages.

In past releases, the notification system for new chat messages relied on a simple ding notification. This sound is easily missed and does not effectively alert users.

In **2026.3**, administrators can set a custom audible alert for better notification using the controls that have been added for chat notifications. The new controls are located on the *Administrator* ribbon, on the **System Settings** tab, **General** sub-tab. The controls behave the same as any other audible notification setting in *CAD Maintenance*. The alert sounds when new messages are received and have not been seen.



The system checks if the *Messaging* window is not open or if it is tabbed and hidden before triggering the alert.

Improve EMD Code Management

This release delivers significant improvements to how *CAD* administrators manage and maintain Emergency Medical Dispatch (EMD) codes within *Call Type Maintenance*. These changes reduce manual effort, improve data accuracy, and provide more flexibility for Response Plan configuration.

See the following:

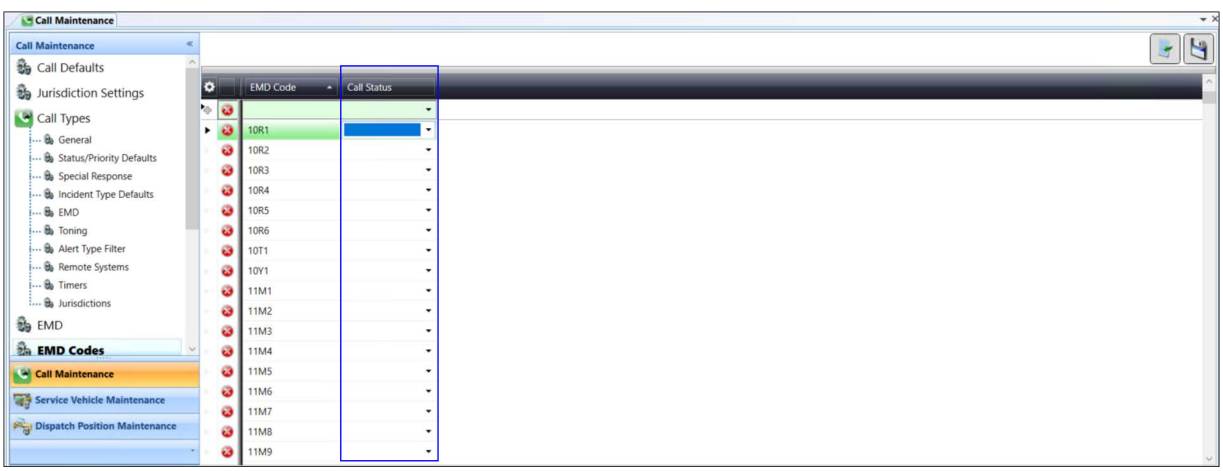
- “Map EMD Codes to Call Status” on page 23
- “Bulk Import of EMD Codes via CSV” on page 23
- “Improved EMD-to-Call-Type Mapping Interface” on page 24
- “Prevent Duplicate EMD Code Assignment” on page 25

Map EMD Codes to Call Status

EMD codes can now be mapped to a Call Status in addition to, or instead of, a Call Type. When an EMD code is received from the questionnaire software, the system can update the Call Type, the Call Status, or both on the Call for Service. This means:

- Administrators no longer need to create thousands of individual Call Types to achieve unique Response Plan assignments for each EMD determinate code.
- A single Call Type with multiple status or priority combinations can now activate different Response Plan assignments based on the status set by EMD.
- Call Status mapping is optional. Existing Call Type only mappings continue to work as they have in previous releases.

To enable the new mapping, a new column has been added to the *EMD Codes* sub-tab on the *Call Types* tab in *Call Maintenance*.



Select the ***Call Status*** from the list to map it to the ***EMD Code***.

Bulk Import of EMD Codes via CSV

A new Import feature allows administrators to add and update EMD codes in bulk using a CSV file. The import supports the following data:

- EMD Codes
- Call Status (optional)

During the import process, duplicate codes in the CSV are ignored and only new codes are added.

Additionally, existing codes can have their Call Status mapping added or updated using the import feature, saving time and removing the tediousness of individual mapping and updates.

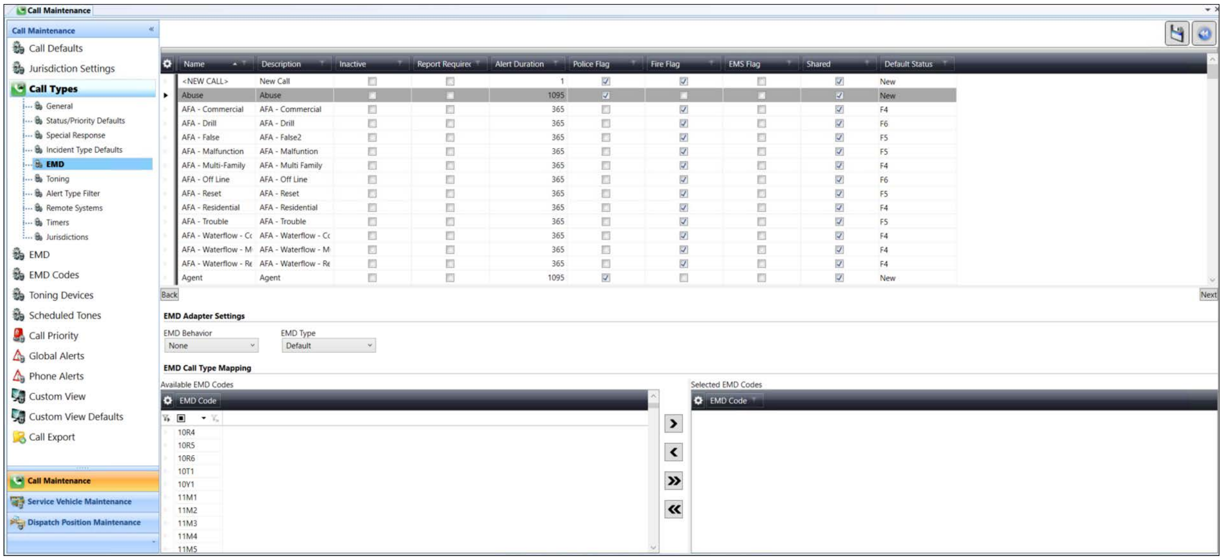
Codes that exist in *CAD* but are not in the CSV file are not removed. Administrators must manually delete codes.

To import a CSV file to map EMD codes:

1. In the *CAD Maintenance Client*, click the **Call** button on the *Maintenance* ribbon.
2. Click the **EMD Codes** tab top open the *EMD Codes* window.
3. Click the **Import** button. The *Open* dialog displays.
4. Navigate to the CSV file to import.
5. Click **Open**. A notification displays when the import process completes.

Improved EMD-to-Call-Type Mapping Interface

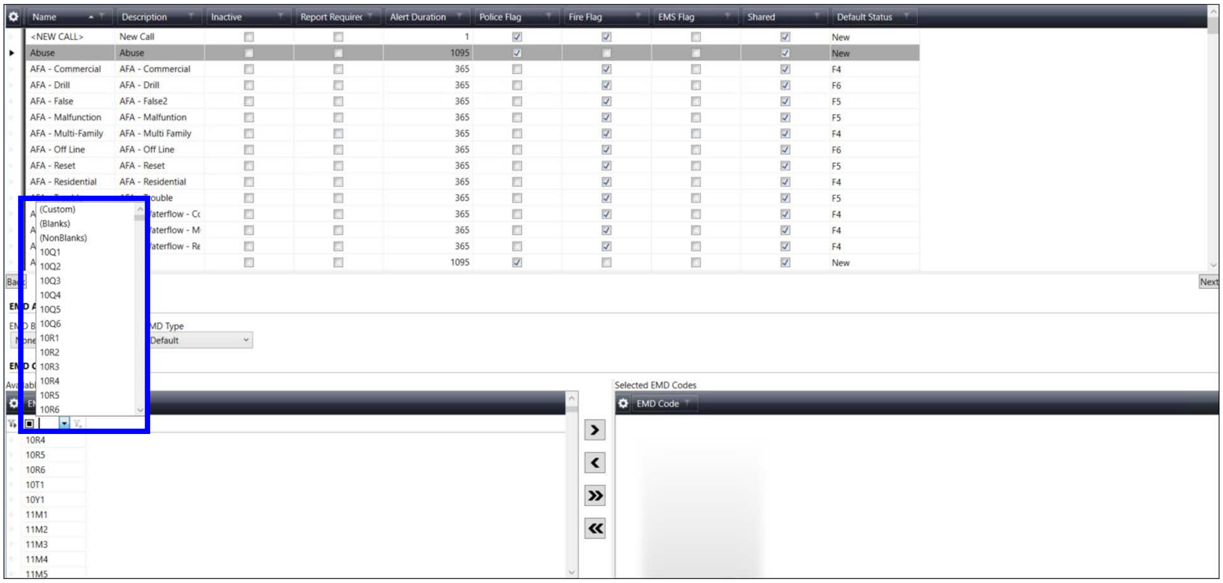
The EMD code mapping interface within *Call Type Maintenance* has been updated from the single-entry batch edit grid to a select or multi-select and move with advanced filtering. This makes it significantly easier to sort through and assign large volumes of EMD codes to Call Types.



To map Call Types to EMD codes:

1. Select a Call Type from the grid.
2. Click the **Edit** button.
3. Filter or navigate the to EMD code.

To filter, click into the filter field to activate it and type the code, or click the arrow next to the filter field to select the code from a list.



4. Select the code or click, press **<Shift>**, and click the last code of the group selection to select a group of codes.
5. Click the **Move** > button to move the code(s) to the *Selected EMD Codes* list. Note that the **>>** button moves all the codes in the list.
6. Click the **Save** button.

Prevent Duplicate EMD Code Assignment

The system now checks for duplicate assignments when mapping EMD codes to Call Types. If an administrator attempts to assign an EMD code that is already mapped to a different Call Type, a confirmation dialog displays about the conflict. Within this dialog, administrators can choose whether to reassign the code or cancel the action. This prevents unintended behavior where multiple Call Types reference the same EMD code.

Dispatch Client Enhancements

The *Enterprise CAD Dispatch Client* application allows CAD dispatch centers to function more efficiently while offering dispatchers all the tools necessary to quickly take calls and dispatch the appropriate agency personnel.

See the following sections for details about *Dispatch Client* enhancements in **2026.3**:

❖ ❖ ❖ ❖ ❖

CFS Window — Separated FPM Alerts from Other Alerts

The *CFS Entry* window, along with the associated *CFS Detail* window and its associated tabs, is the main tool used by dispatchers to document the details of a CFS as it is being reported. Dispatchers can use the standard *CFS Entry* window or a custom *CFS Entry* window that is based on agency call-taking preferences. Using a custom *CFS Entry* window offers agencies a way in which to add additional functionality for dispatchers to access from their *CFS Entry* window.

In **2026.3**, the following changes have been made to separate FPM alerts from Local Records alerts expedite alert notifications, as they may contain pertinent prior incident and responder safety information.

See the following for more details:

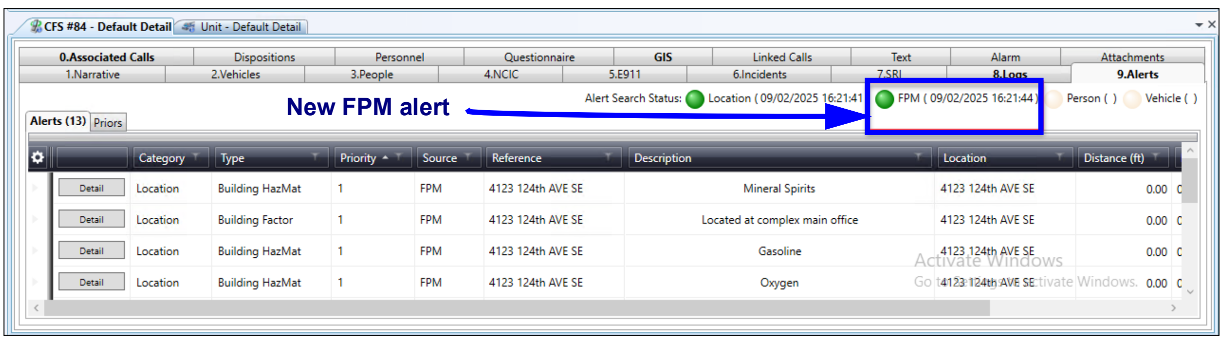
- "Alerts Tab — Separated FPM Alerts from Other Alerts" on page 27
- "Logs Tab — Separated FPM Alerts from Other Alerts" on page 27
- "Added Time Zone Field to Scheduled Calls Window" on page 30

❖ ❖ ❖ ❖ ❖

Alerts Tab — Separated FPM Alerts from Other Alerts

The *Alerts* tab allows users to view information pertaining to any alerts associated with the current CFS. Alert information included on this tab includes the category of alert, type, priority, source (records or FPM) description, alert location, distance, effective date, and expiration date. The status of alert searches appear along the top of the tab with colored indicators denoting their success.

In this release, *FPM* alerts have been separated from local record alerts. A new alert indicator appears above the grid on the *Alerts* tab.

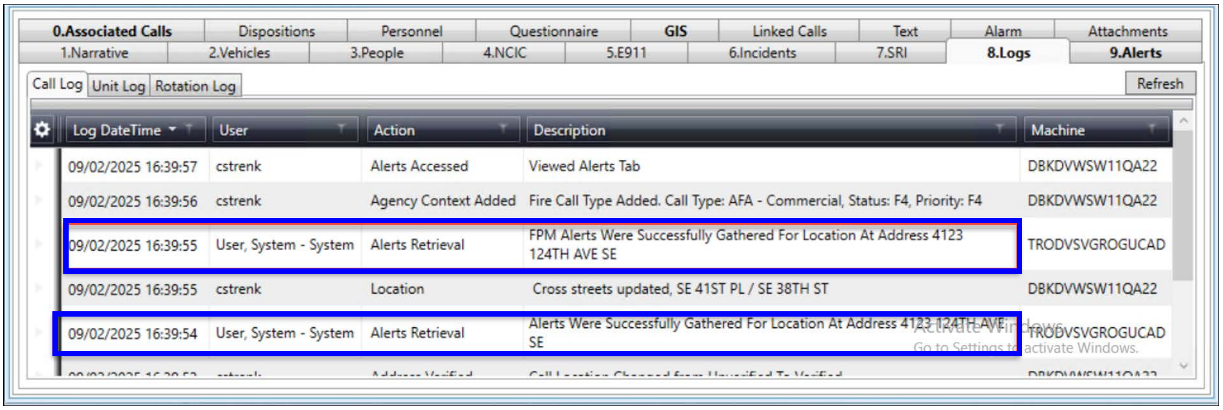


Logs Tab — Separated FPM Alerts from Other Alerts

The *Logs* tab tracks action taken on the call including call creation, changes, clearance, units assigned via a run card or unit recommendation, unit involvement, manual pages, which dispatchers opened up a particular CFS, or service vehicle rotation actions. This information is contained in three sub-tabs.

The *Call Log* sub-tab allows users to view a listing of call activity, additions, or updates associated with the current CFS, such as the call creation date/time, call timer expiration date and time, vehicle and person additions, etc.

In this release, a separate *Call Log* entry displays for *FPM* status upon retrieving alerts. The *Description* indicates if the *FPM* alerts were or were not successfully gathered for the location at the specified address.

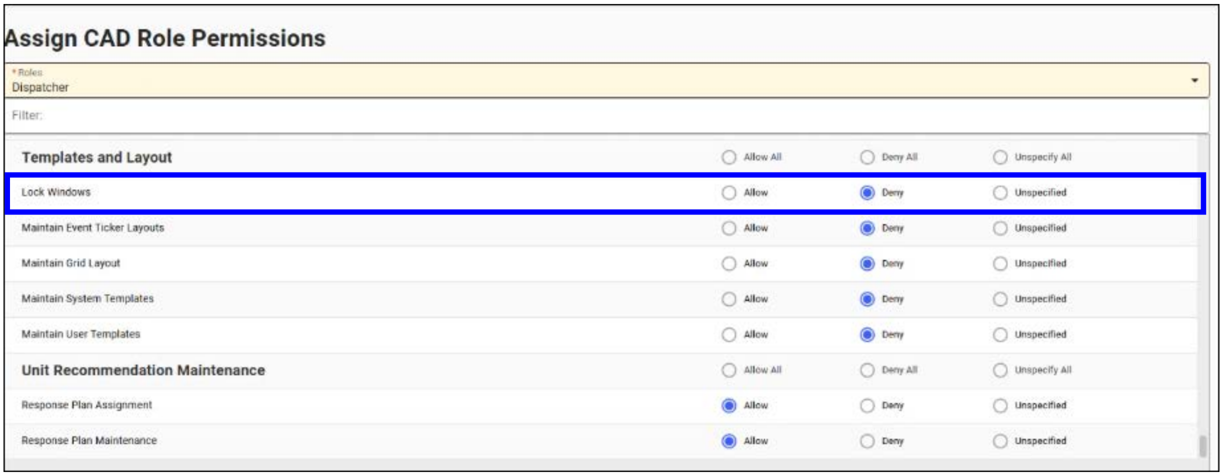


Added the Ability to Lock Templates

In previous releases, windows and templates were not locked. Occasionally, users would accidentally move a window out of position. To reset the windows, they would reload the template, which could take up to 60 seconds to refresh.

Because every minute counts when taking an emergency call, the ability to lock templates has been added in **2026.3**.

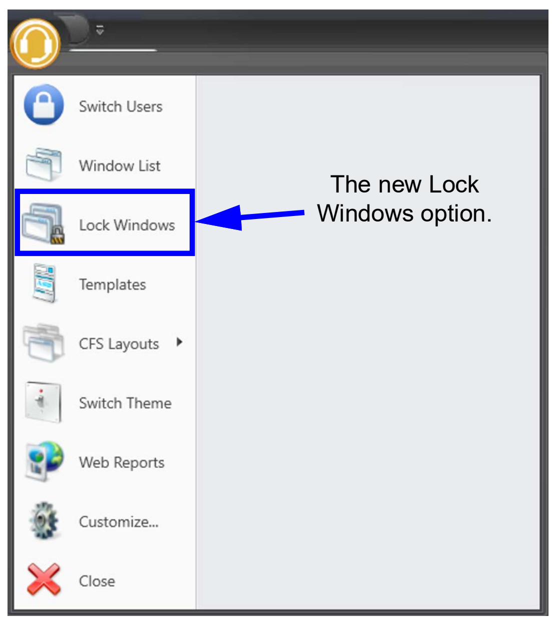
A new **Lock Windows** permission has been added to *ESS* under the **Templates and Layout** permission to allow or deny window locking for any assigned *CAD* position. This permission is set to ***Allow*** by default.



Roles that have this permission can lock templates, layouts, and windows from the **CAD Application** button.

This option is disabled if the role permission is set to ***Deny***.

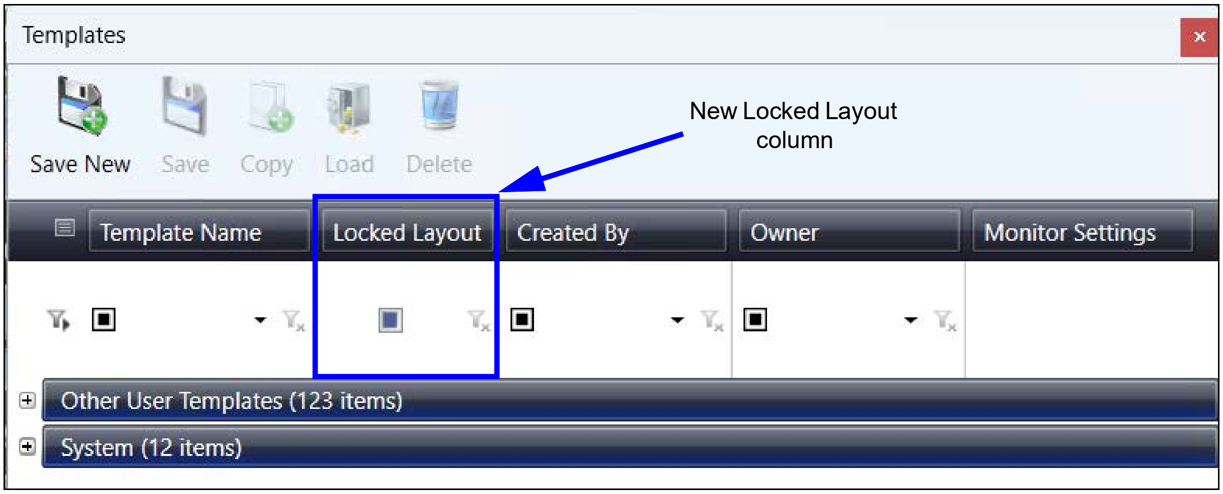
When the **Lock Windows** option is enabled from the **Application** button menu in the *CAD Dispatch Client* by a user with **Lock Windows** permission, the current layout or template is locked into place. All docked windows remain as they are displayed and cannot be moved, reorganized, or undocked.



After Lock Windows is selected, the **Application** button menu option changes to **Unlock Windows**, where, if selected, the user can then unlock the windows and rearrange their layout.

Additionally, when opening new windows and selecting **Lock Windows**, the new windows also lock with the template or current layout. If opening new windows while the current layout is locked, the new windows are not locked unless the user unlocks and re-locks the windows from the **Application** button menu.

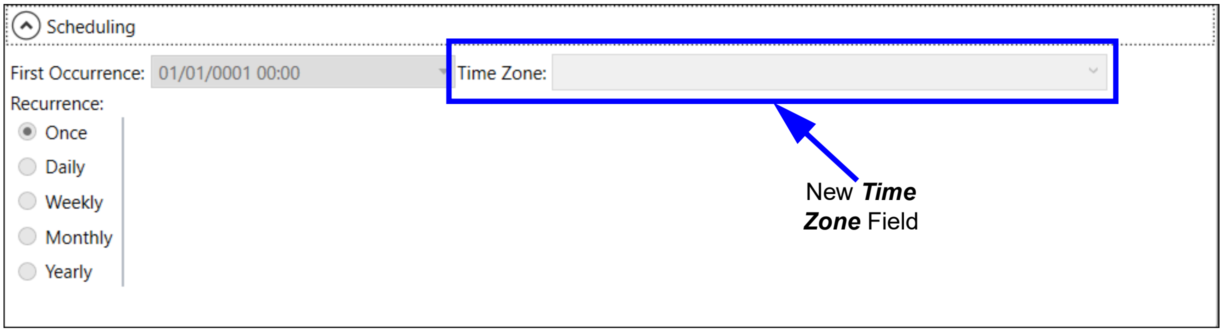
A *CAD* Administrator can create a locked template using the **Lock Windows** option, then selecting **Templates** from the **Application** button menu, and creating a new template while the lock is enabled. A new Locked Layout column indicates if the templates are locked or unlocked.



Added Time Zone Field to Scheduled Calls Window

At times, it is necessary to schedule calls for service that have yet to occur but are planned, such as funeral processions, street closures for events, or transportation of defendants to/from court proceedings. The *Scheduled Calls* window, accessed by clicking the **Scheduled Calls** button on the *Dispatch* tab's ribbon, allows dispatchers to enter information pertaining to scheduled calls so that they appear in the *Call List* with units already assigned.

In previous releases, scheduled calls automatically use local time. This may cause a discrepancy with the scheduled events in the *Mapping Client*. In **2026.3**, a ***Time Zone*** field has been added to the *Scheduled Calls* window under the *Scheduling* tab.



With the new ***Time Zone*** field, the scheduler handles both scheduled calls and map events. Map events has that time zone ability in the code, resolving the issue in the *Call Scheduler* stored procedures as there was a conflict for how scheduled calls were handled versus map events. The ***Time Zone*** field added to *Scheduled Calls* resolves the issue.

For example, a dispatcher who is based in Dallas, Texas (Central Time), is working for a company managing infrastructure maintenance across several states. A road repair crew is in Denver, Colorado (Mountain Time), and the state traffic control center overseeing highway notifications operates from Atlanta, Georgia (Eastern Time). Using the Time Zone field ensures that the integrity of the scheduled event matches the various time zones across the *Dispatch Client* and the *Mapping Client*.

If **Deny** is selected for the Lock Windows role permission in *ESS*, the user does not have the ability to lock or unlock windows from the Application button menu in the *Enterprise CAD Dispatch Client*. Additionally, the X on the docked windows is disabled so the user cannot close them. Windows can be resized, but they cannot be closed, moved, docked or undocked. New windows can be opened, but they cannot be docked to the original layout template. New windows can, however, be docked and tabbed to each other. New windows also can be closed because they are not part of the original locked template and the user does not have locking permissions.

Command Maintenance — Multiple Enhancements

CAD commands are the underlying components that users enter in order to accomplish tasks such as changing unit status, ending a CFS, and dispatching units to a CFS.

The *Command Line* is intended to support a narrow set of dispatch commands deemed time critical or frequently occurring (at least once per hour).

The *Command Maintenance* window, accessed by clicking the **Commands** button on the *Maintenance* tab's ribbon, allows users to enter and maintain commands that are then entered on the *Command Line* to perform a function.

In **2026.3**, the *Command Maintenance* window now supports copying commands. In addition, new parameters have been added to the **NewQuickCall**, **UpdateUnitTimer**, and **RerouteUnits** mapped commands, and a new **CheckInAllUnits** mapped command has been introduced.

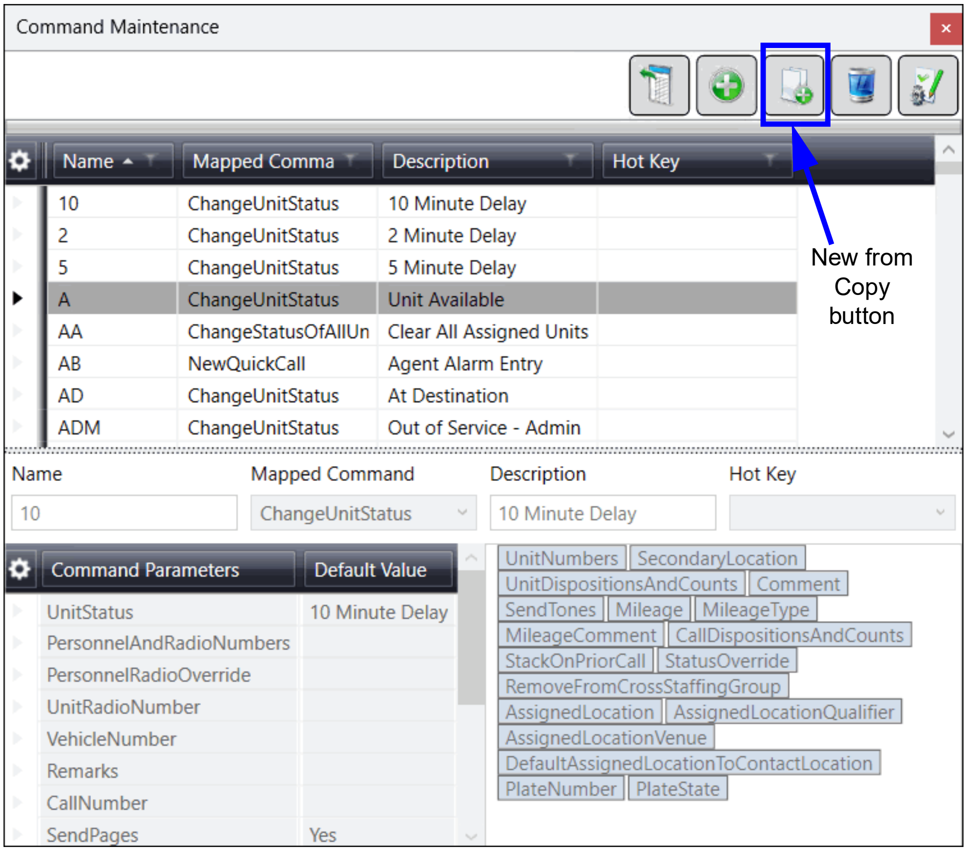
Refer to the following sections for more details on these enhancements:

- "Added the Ability to Copy Commands" on page 32
- "UpdateUnitTimer Mapped Command — Added Narrative Parameter" on page 32
- "RerouteUnits Mapped Command — Added SendTones, SendPages, and SendRipAndRun Parameters" on page 33
- "NewQuickCall Mapped Command — Added ViewCall and UnitAVLocation Parameters" on page 34
- "Added New CheckInAllUnits Mapped Command" on page 36

Added the Ability to Copy Commands

Currently, each command must be created from the ground up, making users configure all command parameters. This process is time-consuming, especially when making command aliases for unit statuses.

In **2026.3**, a new **New from Copy** button allows users to easily modify a single field such as unit status without reconfiguring all command parameters. This simplifies the process of creating commands, such as, creating a command alias for a unit status.



To create a new command from an existing command:

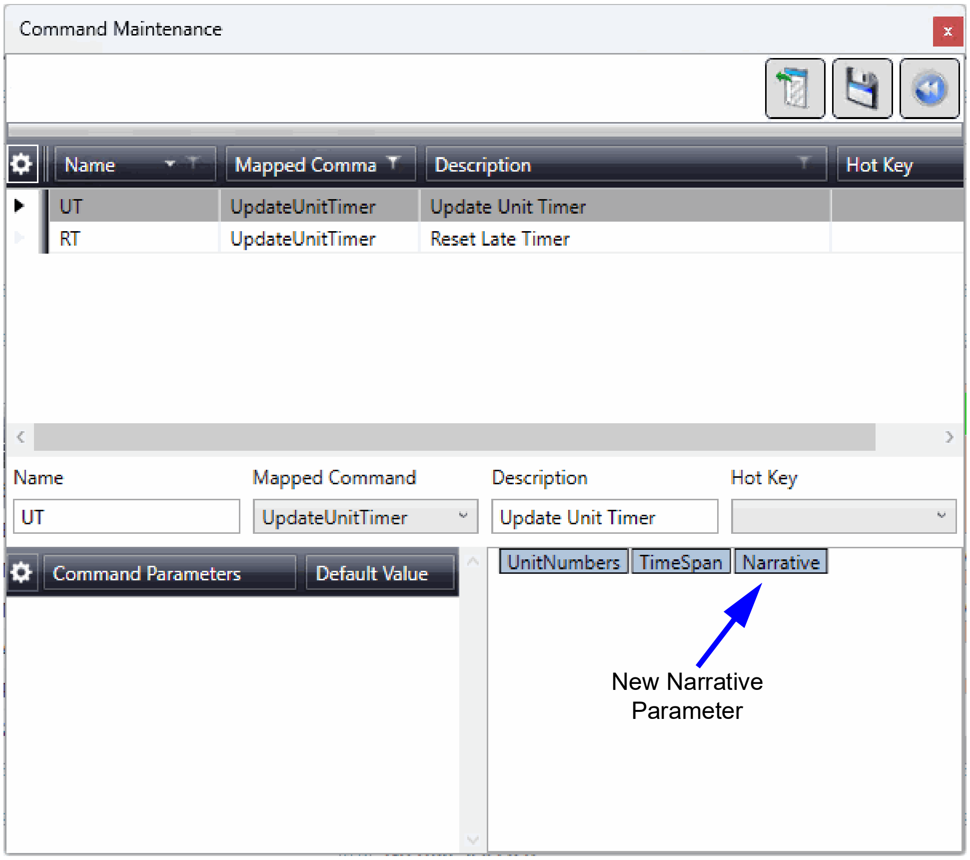
1. On the *Command Maintenance* window, select the command to copy in the *Command* list.
2. Click the **New from Copy** button. A new command is created with all the parameters configured to match the original command.
3. Change the name of the new command.
4. Make any additional field or parameters changes to the new command.
5. Click **Save**.

UpdateUnitTimer Mapped Command — Added Narrative Parameter

The **UpdateUnitTimer** mapped command updates the time span on the timer for the specified unit or units.

Dispatchers want to capture updates when they reset their unit timer so that they can maintain accurate records as units give narrative updates during a status check.

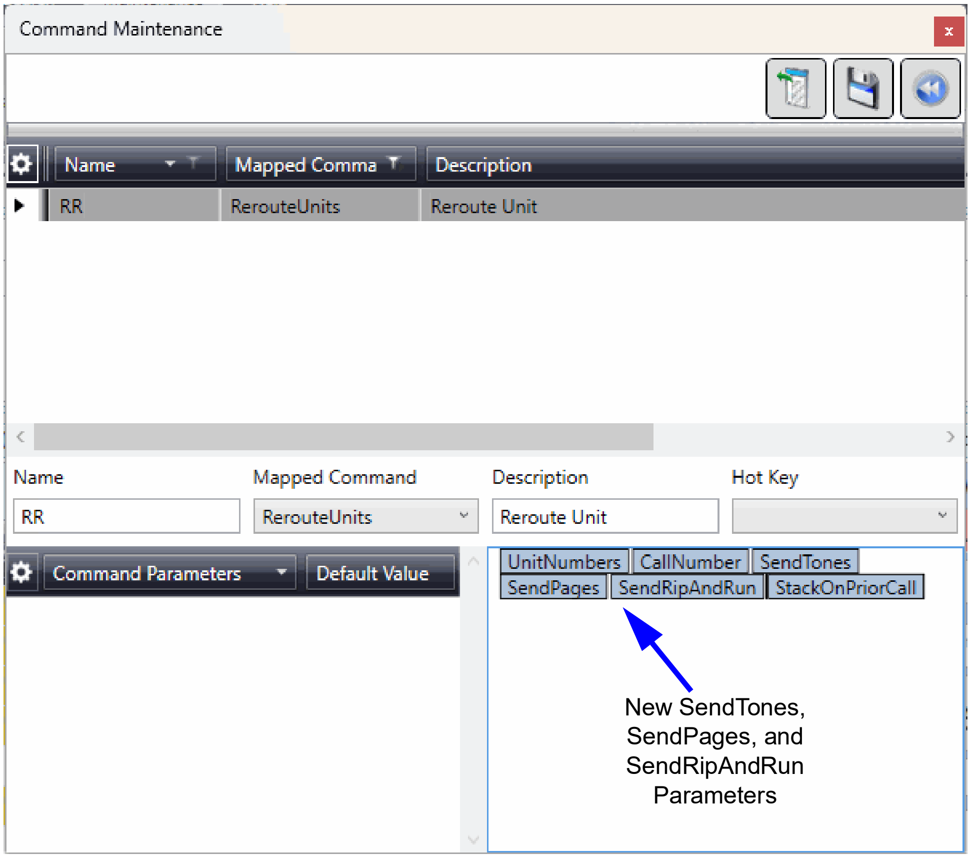
In **2026.3**, dispatchers can now document narrative updates provided by units during status checks. They can capture these updates through the command line when updating the unit timer with the **UpdateUnitTimer** mapped command, using the new ***Narrative*** parameter.



RerouteUnits Mapped Command — Added SendTones, SendPages, and SendRipAndRun Parameters

The **RerouteUnits** mapped command reroutes the specified unit(s) to the designated CFS. In daily operations, units frequently reroute or swap calls and typically do not require notifications when doing so.

In **2026.3**, new ***SendTones***, ***SendPages***, and ***SendRipAndRun*** parameters have been added to the **RerouteUnits** mapped command. These parameters give dispatchers the ability to suppress notifications that would otherwise be triggered when the command is executed, providing greater control over communication workflows. When a parameter is set to **NO**, the corresponding notification is not sent when the mapped command is executed. When it is set to **YES**, that notification is sent upon execution of the mapped command.



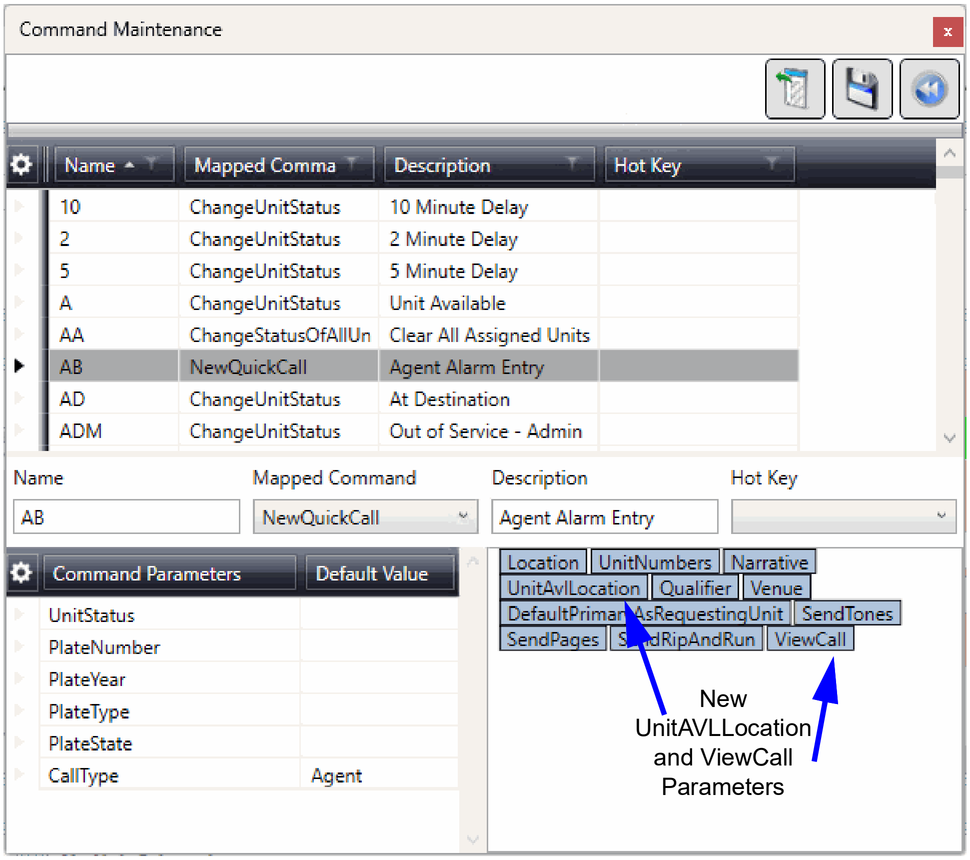
Each parameter can be added to the default editor by selecting it and pressing the **< Delete >** key. Once added, its default value can be set to either **YES** or **NO**.

NewQuickCall Mapped Command — Added ViewCall and UnitAVLocation Parameters

Dispatchers use shortcuts to enter quick calls in the *Command Line* because radio traffic from the unit moves quickly. To better accommodate these needs, the ability to immediately open the CFS to clean up the details and addresses, as well as create calls from officer-initiated activities, have been added to the **NewQuickCall** command in **2026.3**.

The **NewQuickCall** mapped command creates a new quick call. When ***Default Primary As Requesting Unit*** is set to **Y**, the primary unit, which is the unit that is typed in the command first, is set as the ***Requesting Unit*** in the new quick call. If the primary unit is not a police unit, then the first police unit is used. If a police unit is not provided, the ***Requesting Unit*** field remains blank.

The default ***UnitStatus*** for a **NewQuickCall**, if not set using this parameter, is **At Scene**.



A new ***ViewCall*** parameter has been added to the **NewQuickCall** mapped command, offering dispatchers the ability to immediately open the CFS to clean up the details and addresses of a CFS. It has the following options:

- **Yes**: If selected, CAD opens the CFS in a floating window after the call is created, or the user can select the call in the *Call List* if the filters are not set to null.
- **No**: If selected, the CFS does not open after the call is created. This is the default setting.

Also, the ***UnitAvlLocation*** parameter has been added to the **NewQuickCall** mapped command. This new parameter streamlines the process of creating calls from officer-initiated activities that are communicated via radio.

When creating the quick call, and ***UnitAvlLocation*** is set to **Yes**, the address values populate using the latitude and longitude coordinates of the AVL location.

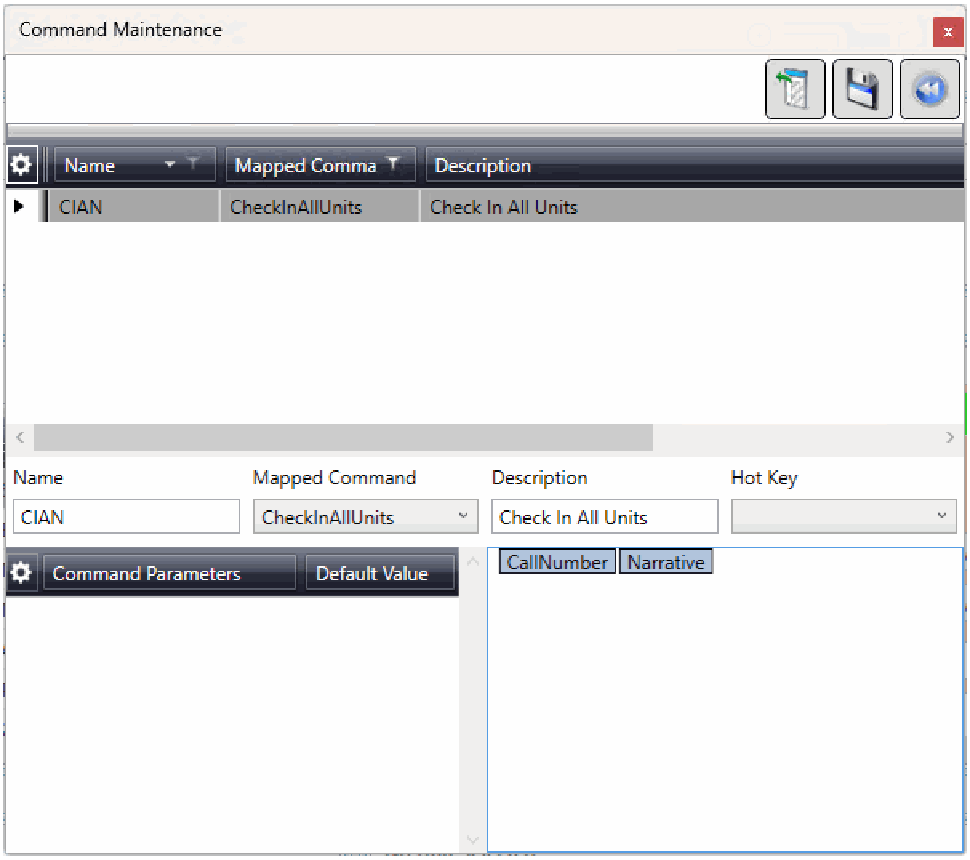
If the user selects **Yes**, but valid AVL data is not available, the system create the new CFS with an empty overridden address value and displays an error message.

If the user types location data into the ***Location*** parameter and the ***UnitAvlLocation*** is set to **Yes**, the data the user typed is used for the CFS address.

Added New CheckInAllUnits Mapped Command

In previous versions, users must type all units assigned to a call using the **UpdateUnitCheckIn** mapped command to check in units. This requires the user to look at the call and identify all the units they need to type in the command to effectively execute the command.

In **2026.3**, a new **CheckInallUnits** mapped command has been added. This mapped command allows dispatchers to mark their check-in time easily and keep accurate records when they check in all units on a CFS. Additionally, when units respond to the status check on the radio, dispatchers can add narrative updates so that all information is documented.



The new **CheckInallUnits** mapped command streamlines marking check-in times and documenting updates. This command behaves similarly to the **UpdateUnitCheckIn**, but works for all units assigned to the CFS that have an **At Scene** status.

The **CheckInAllUnits** command contains ***CallNumber*** and ***Narrative*** parameters.

Automate Call For Service from Third-Party Applications

In previous releases, clients using third-party solutions had to copy and paste their information into *Enterprise CAD* to manually create a CFS. This process is time consuming and prone to errors.

In **2026.3**, third-party applications can now connect to *Enterprise CAD* to automate CFS creation. The new API acts as a template for third-party applications to follow *Enterprise CAD* specifications. This removes the need for expensive interface configuration for each third-party application. Now, third-party providers can use the *Enterprise CAD* API to design and configure their applications to follow *Enterprise CAD* CFS standards, creating a seamless and easy integration and workflow for call takers and dispatchers. This API also enables a smooth partnership between applications and agencies.

The third-party application sends the information to *Enterprise CAD*, where *Enterprise CAD* validates the data, then creates a CFS.

The following will appear in the newly created call after Enterprise CAD validates the information:

- "New Narrative Type and Source Labels on the Narrative Tab" on page 37
- "Call Details on the People Tab" on page 38

New Narrative Type and Source Labels on the Narrative Tab

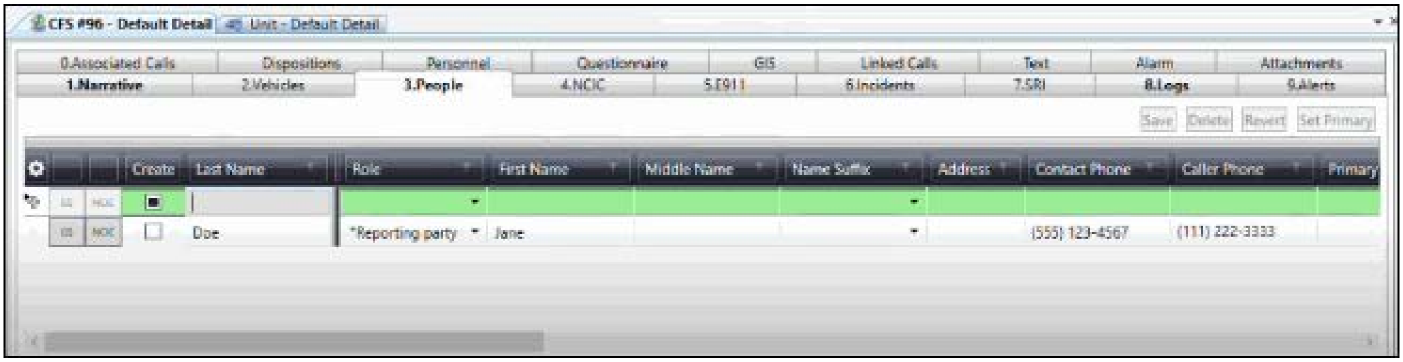
When calls are created through the external API, dispatchers will notice two new values in the *CFS Details Narrative* tab:

- *Type* column: A new **General** narrative type has been added. This replaces the previous unnamed default (value 0) and will appear for narratives entered via the API.
- *Entered By* column: The name of the external narrative source displays for CFS narratives received from the API, allowing dispatchers to quickly identify which narrative entries were created through automated external integrations as opposed to manual user entry.

Call Details on the People Tab

When a third-party application submits caller information with a new call, the data appears in the *CFS Details People* tab.

Caller name (First and Last) and contact phone number display, giving telecommunicators immediate access to accurate caller information for externally created calls.



The formatting from the third-party applications must follow specific rules based on current E*nterprise CAD* entry requirements.

- ***First Name***: Optional
- ***Last Name***: Required
- ***Contact Phone***: Optional
- ***Primary Flag***: Optional
- ***Role***: Required

CFS Detail — Narrative Tab — Added Ability to Copy Narratives

The *CFS Detail* window contains eighteen (18) tabs used to enter and/or display details about the given CFS.

The *Narrative* tab displays narrative information entered in the ***Narrative*** text box on the *CFS Entry* window, Questionnaire Synopses, as well as any Emergency Medical Dispatch (EMD) narratives.

In **2026.3**, the ability to copy narratives has been added. This update makes shift changes easier to pass narratives between telecommunicators and between messaging within *CAD* and *Mobile* responders.

To copy narratives:

1. Click the *Narrative* tab in the *CFS Details* window.
2. Click the tab for the narratives to copy.
3. Select the narrative to copy. To copy more than one, select the first narrative, press <Shift>, and click the last narrative to copy.
4. Right-click the option triangle in the *Options* column next to the narrative(s). The menu opens.Choose **Copy Narrative**.

Use the **<CTL>+<C>** keyboard shortcut to reduce the number of steps to copy the narrative(s).

5. Navigate to the application in which to paste the narrative(s).
6. Press **<CTL>+<V>** or right-click and choose **Paste** from the menu.

Organized Startup Options Dialog Template Selections

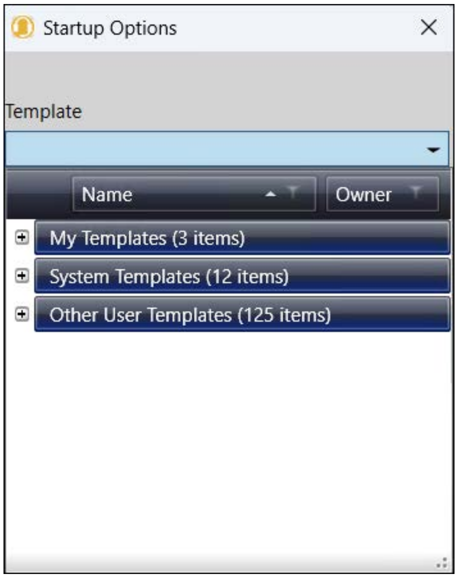
When enabled to display during *CAD* login, the *Startup Options* dialog offers users a way in which to select additional options for use during their dispatch session. These options include selecting a specific workspace template, a dispatch position, and a specific layout for the *CFS Entry* window. When selected, those features are immediately visible upon login.

A layout ***Template*** is a user-saved interface configuration. In previous releases, all templates are shown in an alphabetical list on the *Startup Options* dialog. For agencies that allow user-based templates, this can create a large list.

In **2026.3**, the templates on the *Startup Options* dialog have been organized, allowing telecommunicators to see their user templates at login without scrolling through a large list. This allows them to login quickly and begin their shift sooner.

The list is organized in the following order:

- My Templates
- System Templates
- Other User Templates



After a user has input a valid credential combination, the *Startup Options* dialog opens. Click the ***Templates*** field to open the list of organized templates.

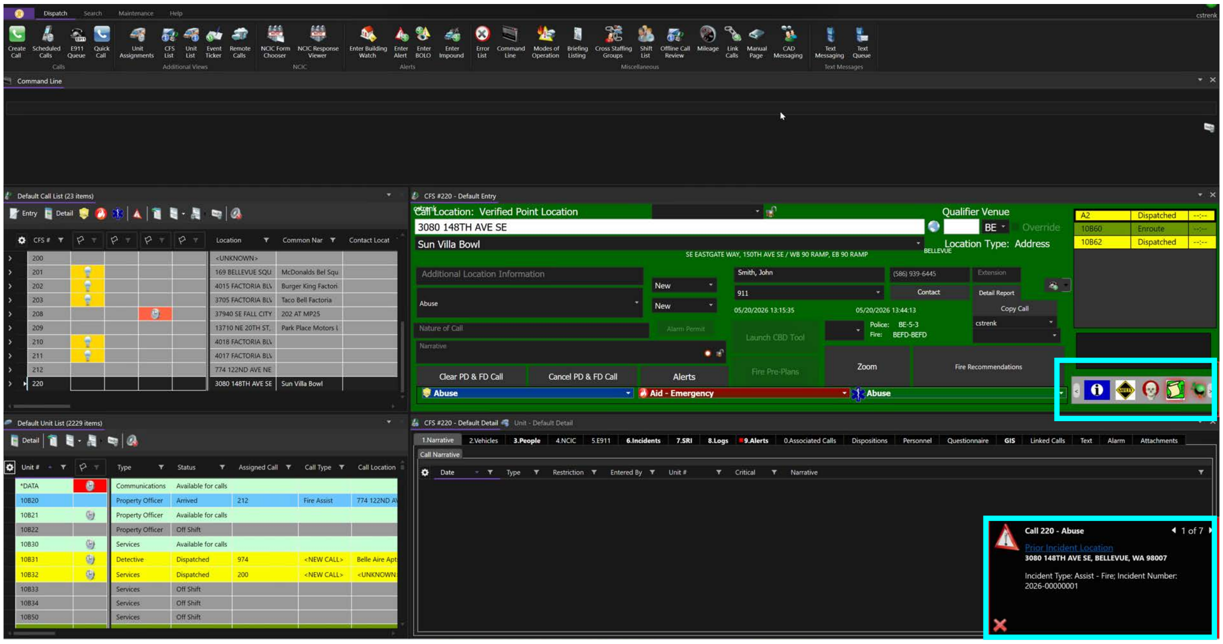
Click the **+** next to the heading to expand the templates.

Select the template to use from the expanded list.

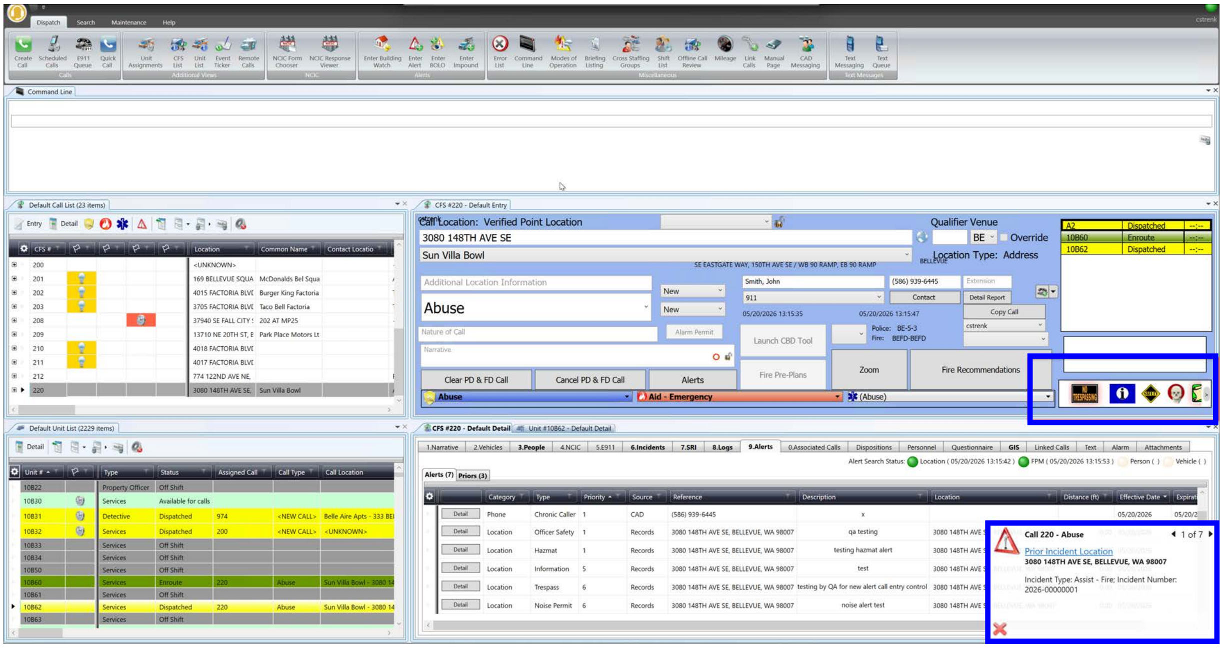
Increased Alert Notification Visibility

In past releases, the Alert Notification has a transparent background. This makes it difficult to read the alert through some backgrounds. Users want to easily identify the Alert Notification so they can quickly understand the alerts as they appear.

In **2026.3**, the Alert Notification background is an opaque color that appropriately corresponds with the background. For example, if in dark mode, the alert follows the dark mode theme with high contrast text and symbols.



Below is an example of the Alert Notification in light mode:



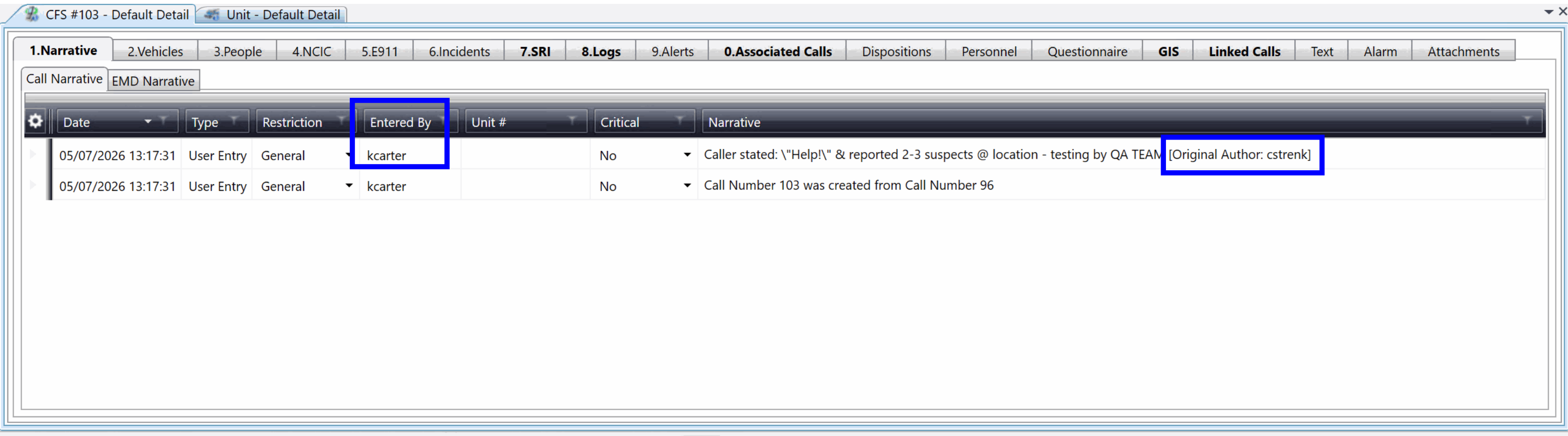
Call Narrative — Copied Narrative References ID of Original Author in New CFS

When an existing CFS is copied into a new call, the narrative entries from the original call are carried forward into the new record. In previous versions of the software, all copied narrative entries were attributed solely to the dispatcher performing the copy action. As a result, the original authorship of individual narrative entries was not preserved, which could lead to confusion regarding who initially authored each entry.

In **2026.3**, enhancements have been introduced to improve narrative traceability when copying a narrative. In high-volume dispatch environments, it is common practice to copy calls to create follow-up or related incidents. With this enhancement, the original author's identity is now preserved and displayed within copied narrative text, providing dispatchers and supervisors with clear visibility into who authored each entry, even after a call has been copied.

Now, when a CFS is copied, each copied narrative entry in the new CFS includes the original author's user alias appended to the narrative text in the format:

< narrative text > [Original Author: User Alias]



The ***Entered By*** field continues to list the user who copied the CFS, maintaining an accurate audit trail of who created the new call record.

Retaining original narrative authorship during the copy process provides several operational benefits:

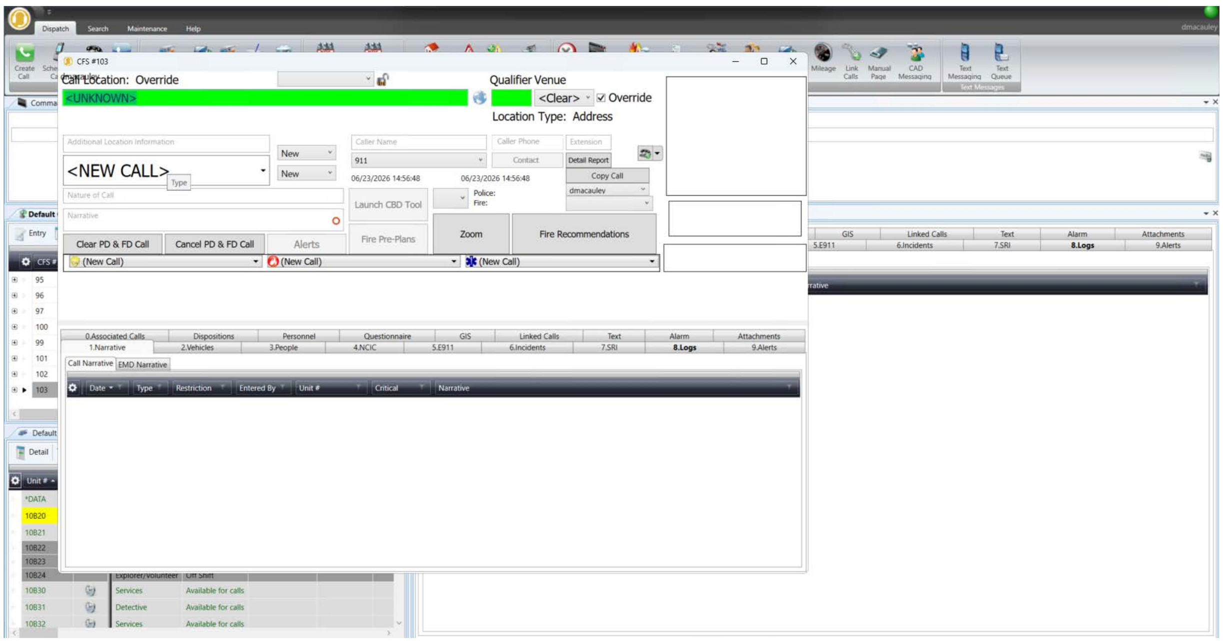
- Accountability: Maintains clear attribution of narrative entries, enabling supervisors to readily identify the original author without requiring reference to the source incident.
- Data Integrity: Preserves the transparency and continuity of the historical record, ensuring narrative content remains traceable even when incidents are copied across shifts, units, or partner agencies.
- Operational Clarity: Allows dispatch personnel to easily differentiate between newly entered information and narrative content carried forward from a prior incident, reducing confusion and improving situational awareness.

CFS Entry — New Calls Open in a Separate Undocked Window

The *CFS Entry* window, along with the associated *CFS Detail* window and its associated tabs, is the main tool used by dispatchers to document the details of a CFS as it is being reported. Dispatchers can use the standard *CFS Entry* window or a custom *CFS Entry* window that is based on agency call-taking preferences. Using a custom *CFS Entry* window offers agencies a way in which to add additional functionality for dispatchers to access from their *CFS Entry* window. For information on setting up and using a custom *CFS Entry* window, refer to the *Custom View Editor* section of the *Maintenance Client User Guide*.

In previous releases, dispatchers had to create a difficult filter on the *Call List* to open new calls in a new window. This created unnecessary limitations.

In **2026.3**, a new window opens by default when creating a new call so that usable space is maximized when a dispatchers is not actively working on a call. Additionally, when there are no docked windows, a new call opens in a new window instead of the docked *CFS Entry* window.



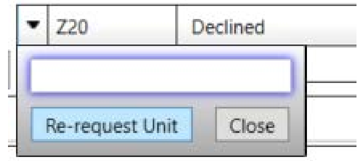
CAD to CAD — Added the Ability to Re-request a Declined Assistance Request

When licensed and set up for *CAD to CAD*, *Enterprise CAD* systems can transfer active calls for service to remote systems in cases when a CFS crosses agency boundaries or assistance from a neighboring agency warrants the sharing of call information.

Previous releases did not have the ability to re-request assistance. When a unit request was declined, the *Remote Unit Request* window in the *CFS Entry* window disabled options. Dispatchers want to request the unit again after a remote unit is declined for assistance so that they can get the help they need if the unit becomes available or if the rejection was accidental.

In **2026.3**, dispatchers can re-request a remote unit after a declined assistance request using the **Re-request Unit** button. Re-requests are available when:

- the unit has become available again
- additional requests on the same remote call are needed
- a dispatcher accidentally rejects the call



To re-request a unit, click the **Re-request Unit** button on the menu on the *Remote Unit Request*.

Users can also re-request the dispatch of the remote unit via the Command Line and accepting unit recommendations.

The narrative updates to reflect the re-request with Unit ## has been re-requested." The *Remote Unit Request* updates after a re-request to allow the remote CAD user to accept or decline the updated request.

The host system CFS notes the re-request in the *CFS Call Log*.

CFS Entry — Call Type Auto-Complete and Enhanced Filtering

In **2026.3**, the ***Call Type*** field on the *CFS Entry* window has been enhanced with a new auto-complete search capability, making call entry faster and more intuitive for dispatch personnel.

Previously, the ***Call Type*** field's selection list only displayed results that began with the characters entered. With this enhancement, dispatchers can now type any portion of a ***Call Type*** name and the *Enterprise CAD* system dynamically filters and displays all matching call types in real time.

This improvement reduces the time spent searching through long ***Call Type*** lists and supports faster, more accurate call classification during active operations.

In public safety communications, speed and accuracy are critical. This enhancement assists dispatchers in the following ways:

- **Locates Call Types Faster**

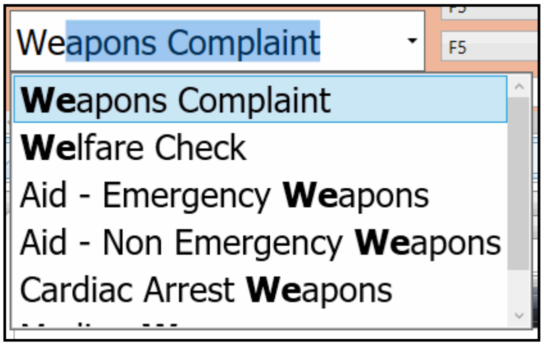
  Dispatchers no longer need to remember the exact name of a call type. Entering any known keyword quickly surfaces the desired option.
- **Reduces Data Entry Errors**

  Selecting from a filtered, *CAD*-generated list minimizes the risk of manual entry mistakes.
- **Improves Focus on the Caller**

  By reducing time spent navigating menus, dispatchers can remain focused on gathering critical information from callers and managing incident details.

New Call Type Filtering Functionality

Following is a list of how the new ***Call Type*** filtering feature works:



- **Flexible Type-Ahead Search**

  The *Call Type* field now supports *free*-text searching. As text is entered, the *CAD* system displays matching call types containing the entered text anywhere within the name—not just at the beginning.

- **Real-Time Filtering**

  The ***Call Type*** field's suggestion list updates instantly with each keystroke, narrowing available options as more characters are entered.

- **Visual Match Highlighting**

  Matching text within each suggested call type is displayed in bold, allowing dispatchers to quickly identify why a result was returned.

- **Clear Selection Highlighting**

  The currently selected suggestion is visually highlighted for easy confirmation before selection.

- **Full Keyboard Navigation**

  To support rapid data entry workflows, dispatchers can:

  - Use the **<Arrow>** keys to move through suggestions.
  - Press the **<Tab>** key to accept the highlighted result and advance to the next field.

  This allows for efficient keyboard-only operation without requiring mouse interaction.

- **Theme Consistency**

  The filtered suggestion list displays consistently across both light and dark system themes for a uniform user experience.

As shown above, entering "we" in the ***Call Type*** field displays matching results such as:

- **We**apons Complaint
- **We**lfare Check
- Aid - Emergency **We**apons
- Aid - Non Emergency **We**apons
- Cardiac Arrest **We**apons

In prior versions of the software, only call types that started with "we" (such as WEAPONS or WELFARE CHECK) would have been shown.

With this enhancement, any call type containing the entered text anywhere in its description is included, with those starting with the entered text list first.

Tips for Dispatchers

Below are some tips to remember when using the new ***Call Type*** filtering:

- **Use Distinctive Keywords**

  If the full call type name isn't immediately known, type a unique word associated with it. For example, entering "fire" may return:
  - Structure Fire
  - Dumpster Fire
  - Vehicle Fire
- **Use the <Tab> key for Faster Entry**

  Once the correct call type is highlighted, press the **<Tab>** key to accept the selection and move directly to the next field, keeping hands on the keyboard and maintaining workflow efficiency.

Zoom to Location on Map for Cleared Calls

In **2026.3**, the **Zoom** button on the *Cleared Call Entry* window is now functional when reviewing cleared Calls for Service (CFS).

In previous versions of the software, the **Zoom** button was disabled once a call was cleared, requiring personnel to manually locate the incident on the map if geographic context was needed. With this enhancement, users can now zoom directly to the location of a cleared call and view a temporary pin marker on the map for quick reference.

This improvement provides immediate location awareness during incident reviews, shift transitions, and supervisory oversight.

Reviewing cleared calls is a routine part of dispatch operations, whether for shift hand-offs, supervisor review, follow-up coordination, or command-level after-action analysis.

Until now, personnel reviewing historical incidents had to manually navigate the map or cross-reference addresses to locate where an incident occurred.

This enhancement helps dispatchers, supervisors, and command staff:

- **Quickly Locate Past Incidents**

  With a single click of the **Zoom** button, the system centers the map on the cleared call's location, eliminating manual searching.
- **Improve Situational Awareness During Reviews**

  Viewing a cleared call geographically allows personnel to better understand nearby activity, incident clustering, and jurisdictional considerations.
- **Support Faster Shift Hand-Offs**

  Incoming personnel can quickly orient to recent activity by visually reviewing where incidents occurred.
- **Enhance Supervisor and Command Review**

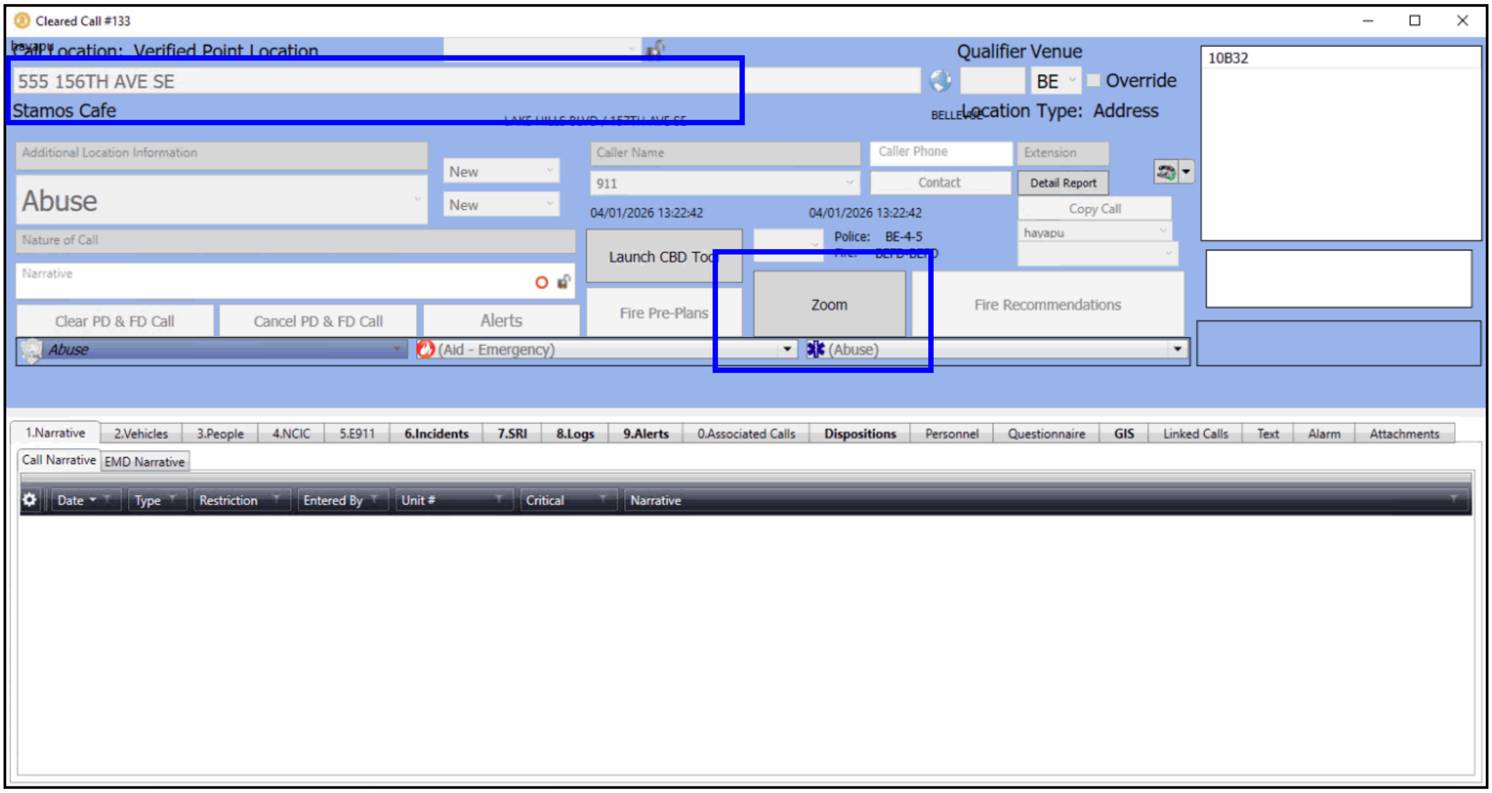
  Supervisors and command staff can rapidly assess incident locations during quality reviews, investigations, or trend analysis without needing to perform separate map searches.

New Cleared Call Zoom Functionality

Following is a list of how the new **Zoom** button functionality on cleared calls works:

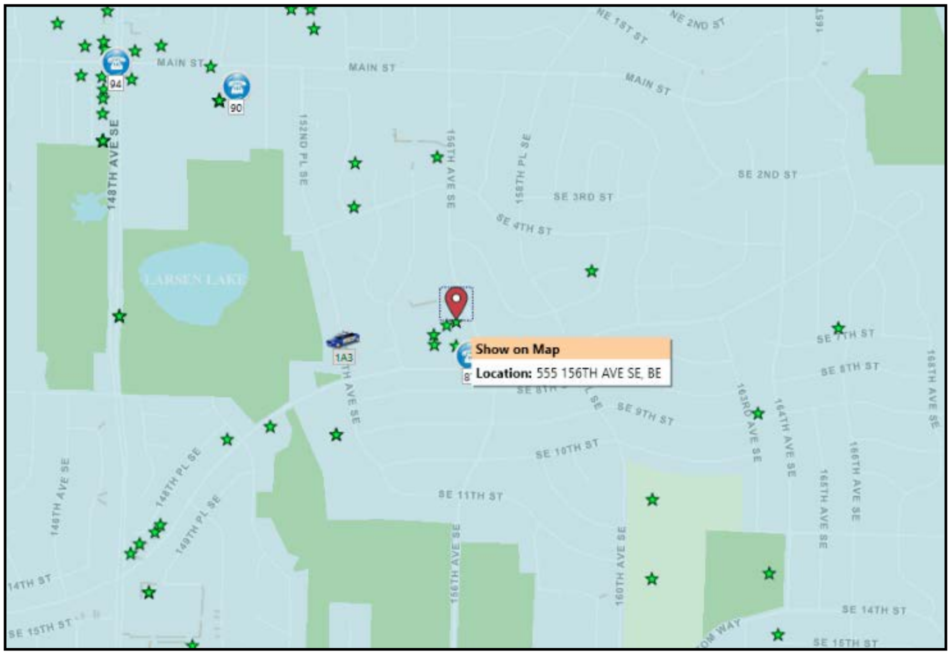
- **Zoom Button Enabled for Cleared Calls**

  The **Zoom** button on the *Cleared Call Entry* window is now active when viewing cleared calls. Selecting it centers and zooms the *Mapping Client* to the incident location at a preset zoom level.



- **Temporary Map Pin Placement**

  When zooming to a cleared call, the system places a temporary pin at the incident location for clear visual identification.



  This behaves consistently with other location pin functions throughout the application.

- **Automatic Pin Removal**

  To prevent map clutter, the temporary pin is automatically removed when another location-based action is performed, such as zooming to a different call or address.

- **Overridden Address Handling**

  If the cleared call has an overridden (non-geoverified) address, the system displays the following message:

  ⚠ Unable to zoom to location. The location is not a geoverified location. Dismiss

  This ensures users understand why the location cannot be displayed on the map.

- ***Mapping Client* Availability Check**

  If the *Mapping Client* is not currently running, the system displays the following error message rather than failing silently:

⚠ The command could not be completed. The mapping client is not running. Dismiss

Below are the steps needed to view a cleared call in the *Mapping Client*:

1. Open a cleared CFS from the *Cleared Call Search* window.
2. Click the **Zoom** button (the same button used for active calls).
3. The open *Mapping Client* centers on the call's location and zooms to a preset level.
4. A temporary pin icon appears at the call location.
5. The pin remains until another location-based search or zoom action is performed.

Dockable Clock Window

In version **2026.3**, a new **Clock** button has been added to the **Miscellaneous** group on the *Dispatch* tab ribbon, allowing dispatchers to add a dockable clock directly to their *Dispatch Client* workspace.

Previously, dispatchers needed to reference an external clock or look away from the *Dispatch Client* when announcing the time or documenting radio traffic. With this enhancement, the current time is available directly within the *Dispatch Client* workspace, helping personnel remain focused on active incidents and dispatch operations.

Dispatchers and command personnel frequently reference the current time during critical operations, particularly when acknowledging radio traffic, documenting events, or coordinating incident response.

This enhancement provides immediate access to the current time without requiring users to shift their attention away from the *Dispatch Client*.

The *Clock* window displays the time in 24-hour format.

This enhancement helps dispatchers, supervisors, and command staff:

- **Maintain Focus on Active Incidents**

  View the current time without looking away from the *Dispatch Client*, helping maintain concentration during high-priority dispatch activities.
- **Improve Efficiency During Radio Communications**

  Quickly reference the current time when acknowledging radio traffic or documenting time-sensitive events.
- **Customize the Dispatch Workspace**

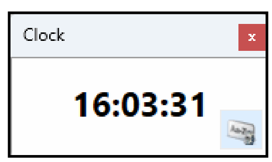
  Add, dock, and position the *Clock* window wherever it best supports the user's workflow and screen layout.

New Clock Window Functionality

Following is a list of how the new *Call* window works

- **Dockable Clock Window**

  A new dockable *Clock* window displays the current time using the workstation's system clock. Like other *Dispatch Client* windows, it supports standard docking, tabbing, and layout templating, and can be used in both locked and unlocked workspace layouts.



- **Clock Button on the Dispatch Ribbon**

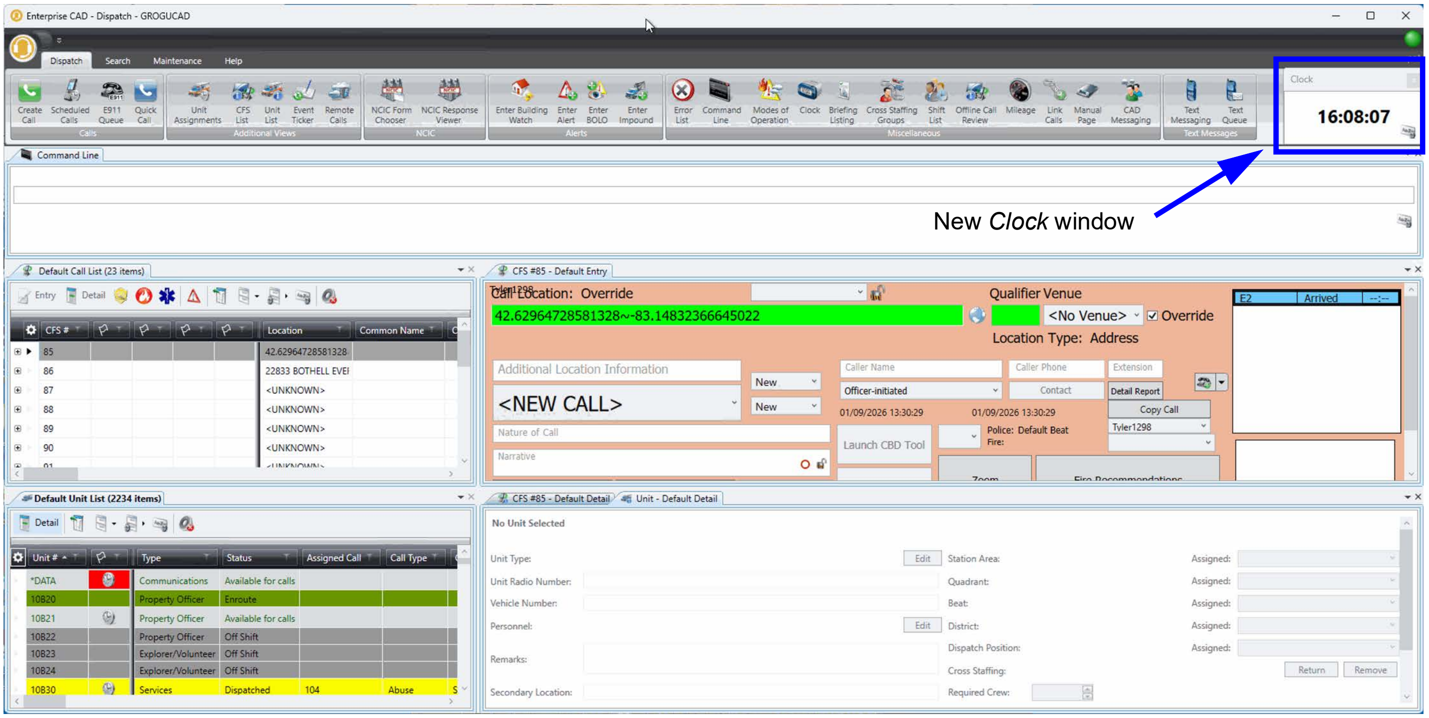
  A new **Clock** button has been added to the **Miscellaneous** toolbar group on the *Dispatch* tab's ribbon, providing quick access to open the *Clock* window.

- **Resizable Window**

  The *Clock* window can be resized to fit the workspace. A minimum width and height are maintained to ensure the displayed time remains readable regardless of layout.

Below are the steps to add the *Clock* window to the *Dispatch Client* workspace:

1. Click the **Clock** button from the **Miscellaneous** toolbar group on *Dispatch* tab's ribbon.
2. The *Clock* window displays. Dock, tab, or position the *Clock* window as desired.



3. Save the workspace template, if applicable, to retain the *Clock* window in future sessions.

Note the following:

- **Workstation System Clock**

  The displayed time is based on the workstation's system clock, and only displays in 24-hour time. If the workstation time is incorrect, the *Clock* window reflects that time.

- **Standard Workspace Features**

  The *Clock* window behaves like other *Dispatch Client* windows and supports docking, tabbing, layout locking, and workspace templates, allowing it to be incorporated into any preferred *Dispatch Client* layout.

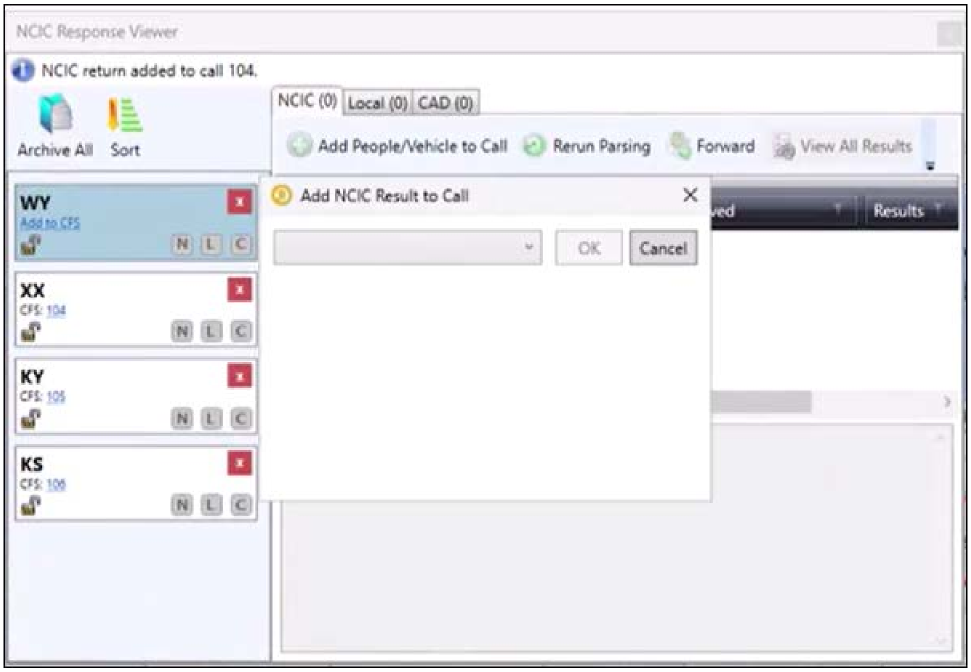
CFS Entry — Added Ability to Add NCIC Results to Any CFS

Police dispatchers want to attach any NCIC result to the CFS when they are handling a call-for-service (CFS), so they can provide relevant information, such as NCIC messages for dangerous felons.

This enhancement allows police dispatchers to attach messages from the NCIC results grid to related CFS. This makes adding important system messages to calls easy, improving communication and response.

To add an NCIC result to a call:

1. Click the **NCIC Response Viewer** button on the *NCIC* toolbar group to open the *NCIC Response Viewer*.
2. Click **Add to CFS** on the NCIC result to add to a call. The *Add NCIC Result to Call* dialog opens.



3. Select a call from the list.
4. Click **OK**. A message displays stating NCIC return added to call XX, where XX is the call number. This confirms the NCIC result was added to the selected call.

Unit Recommendations — Enhanced Dynamic Refresh

The Unit Recommendations dynamic refresh was enhanced to address excessive snapshot creation and performance concerns by limiting the auto refresh to occur after the initial dispatch for up to five minutes in a previous release.

However, it did not appropriately account for when a recommendation should be refreshed initially. This resulted in if a user does not manually refresh an old recommendation that has not been dispatched (i.e. pending call), *CAD* continued to display the initial recommendation, which may be out of date. Furthermore, the Recommendations Updated time updatee when opening the window, despite the fact that the recommendation was never actually re-run. This confuses the user into thinking the recommendation they are viewing is already up to date.

In **2026.3**, two changes were made to improve this experience:

- The recommendation refreshes every time the *Unit Recommendation* window is opened. While this is a departure from how the dynamic recommendation feature has worked, it ensures the latest unit refreshes are no longer running for the life of the call.
- The Recommendations Updated time is only updated when the recommendations are actually refreshed. This reflects the age of the generated recommendations only.

ShowCallInDefaultWindow Mapped Command Removed

In **2026.3**, the **ShowCallInDefaultWindow** command has been removed from the *CAD* system.

User interface improvements introduced in this release changed how default windows are displayed, making this command obsolete. Agencies should now use the **ShowCall** mapped command, which opens a Call for Service (CFS) and navigates directly to a specified tab, providing a more efficient and intentional user experience.

If any agency has **ShowCallInDefaultWindow** mapped to any key, button, or macro, they are alerted to replace it with the **ShowCall** mapped command prior to upgrading to **2026.3**.

Improved Default System Settings for New Enterprise CAD Installations

In **2026.3**, *Enterprise CAD* includes several updated default configuration settings designed to provide a more streamlined experience for new agency implementations.

The updated settings affect online NCIC request processing, local NCIC search results, prior incident alerts, and alert control visibility in the *Call Entry* window.

These enhancements establish recommended out-of-the-box defaults based on proven best practices, helping reduce initial configuration effort while improving usability for dispatch personnel. These changes apply to new *Enterprise CAD* installations only. Existing customer configurations are not affected by these changes unless the settings are manually updated.

Default system settings play an important role in how quickly new users become productive. By applying recommended configuration values during implementation, agencies can spend less time adjusting settings and more time focusing on day-to-day dispatch operations.

This enhancement helps dispatchers, trainers, administrators, and command staff:

- **Simplify New System Implementations**

  Recommended default settings reduce the amount of configuration required during deployment, allowing agencies to begin using *Enterprise CAD* more quickly.
- **Improve Dispatcher Efficiency**

  Several default settings now eliminate unnecessary manual steps during common workflows, helping dispatchers complete tasks more efficiently.
- **Enhance Usability**

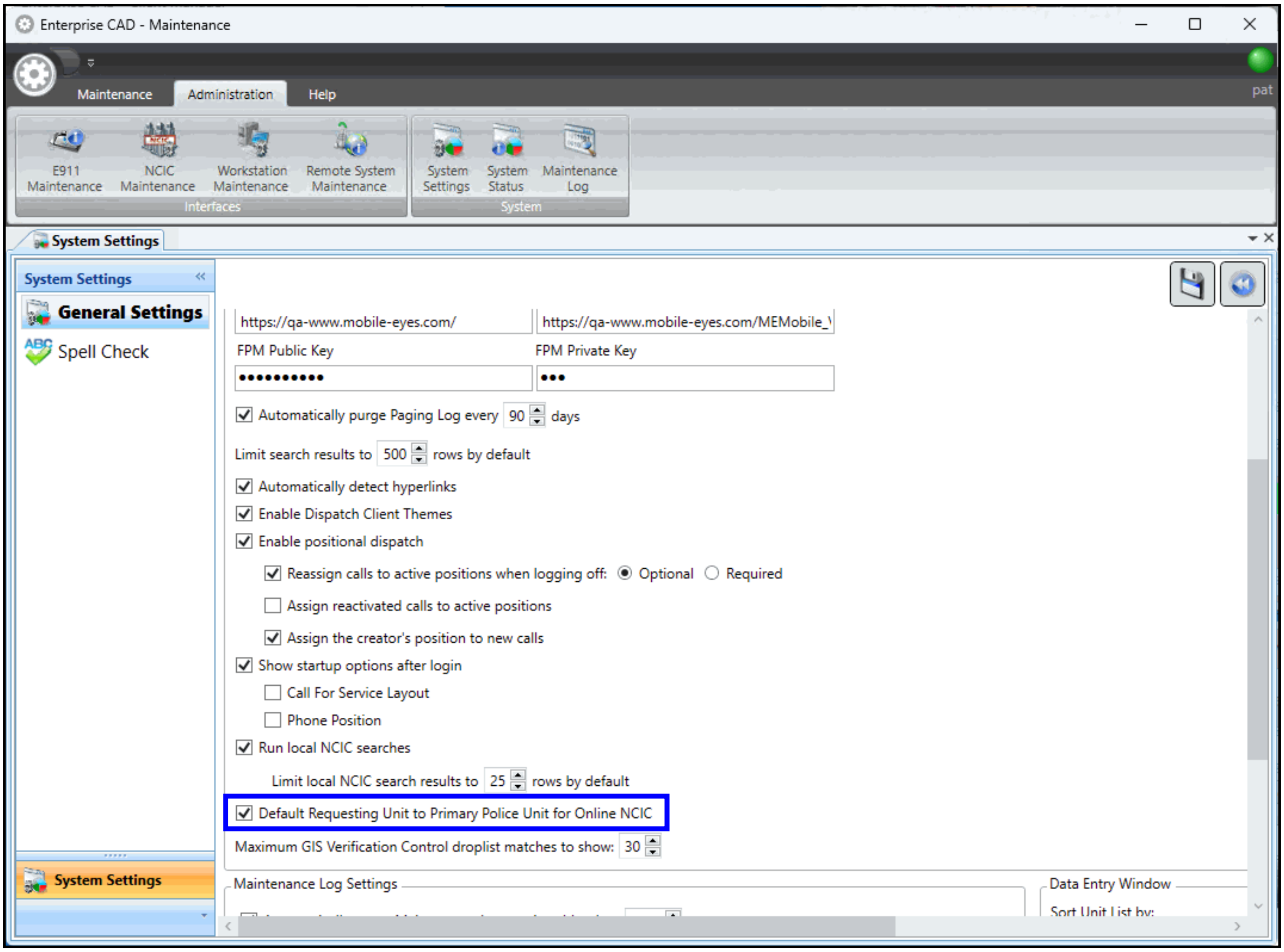
  Improved defaults help reduce information overload and make important information easier to identify during active dispatch operations.

The New Default Settings

Following are details of the new default settings:

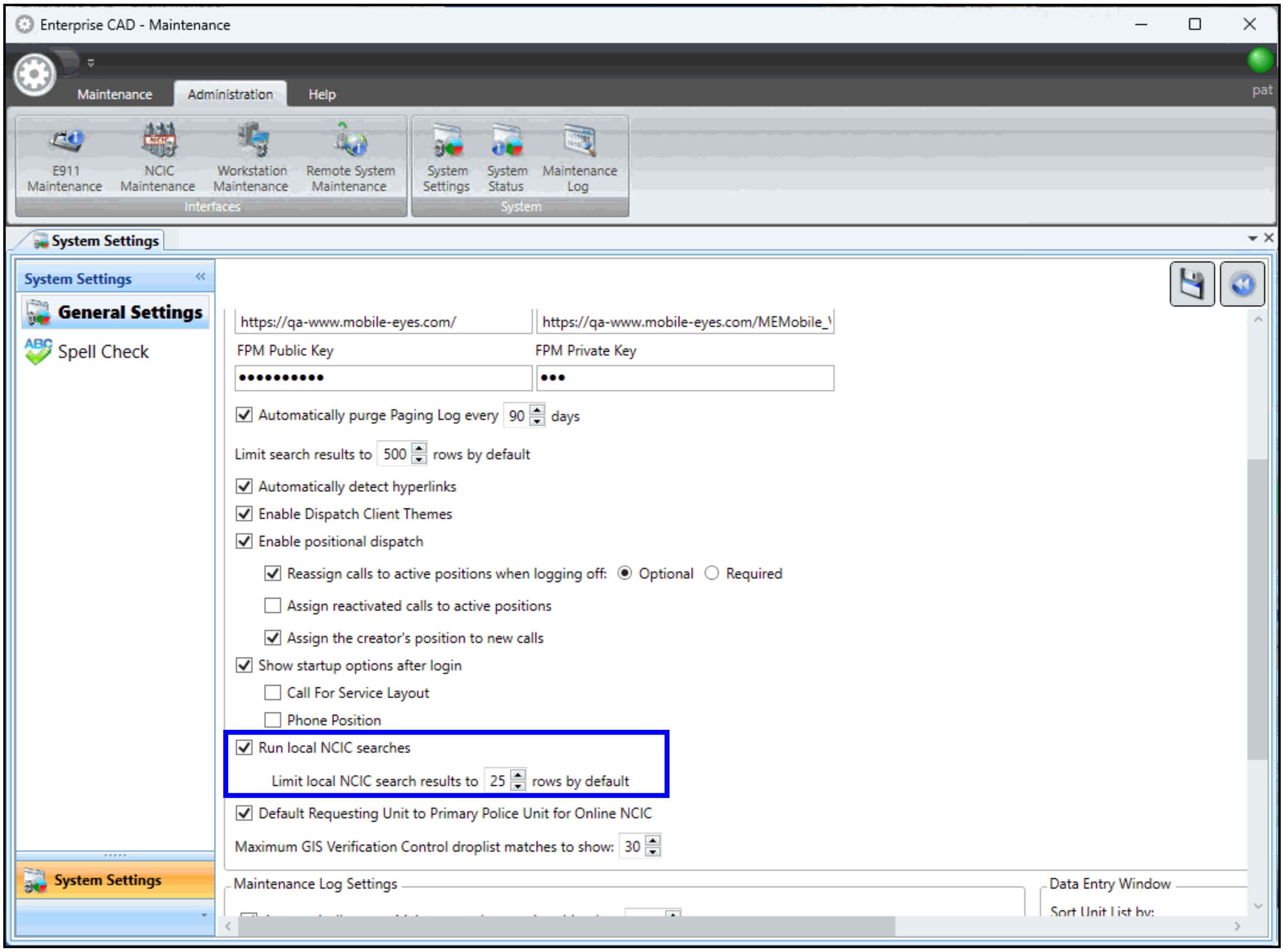
- **Automatic Requesting Unit for Online NCIC Queries**

  The ***Default Requesting Unit to Primary Police Unit for Online NCIC*** setting, accessed under General Settings on the *System Settings* window of the *Maintenance Client*, is now enabled by default for new installations. When conducting online NCIC queries during traffic stops, the requesting unit is automatically populated, eliminating the need for dispatchers to manually enter the unit number for typical single-officer requests.



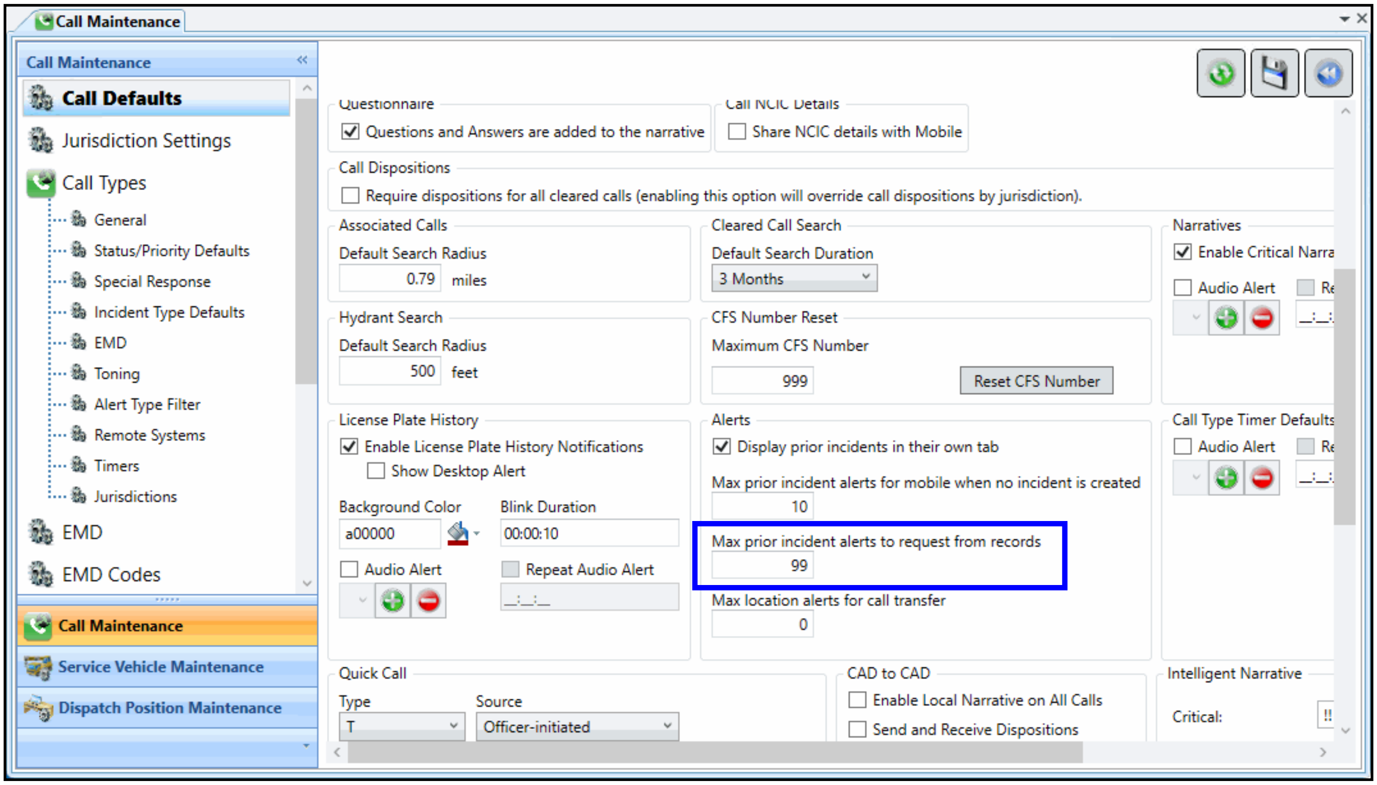
- **Optimized Local NCIC Search Results**

  The default maximum number of local NCIC search results displayed in the *NCIC Response Viewer* window has been reduced to 25 records, or rows. This provides a more manageable results list while maintaining efficient access to relevant information. The setting is located in the General Settings section of *System Settings* in the *Maintenance Client*.



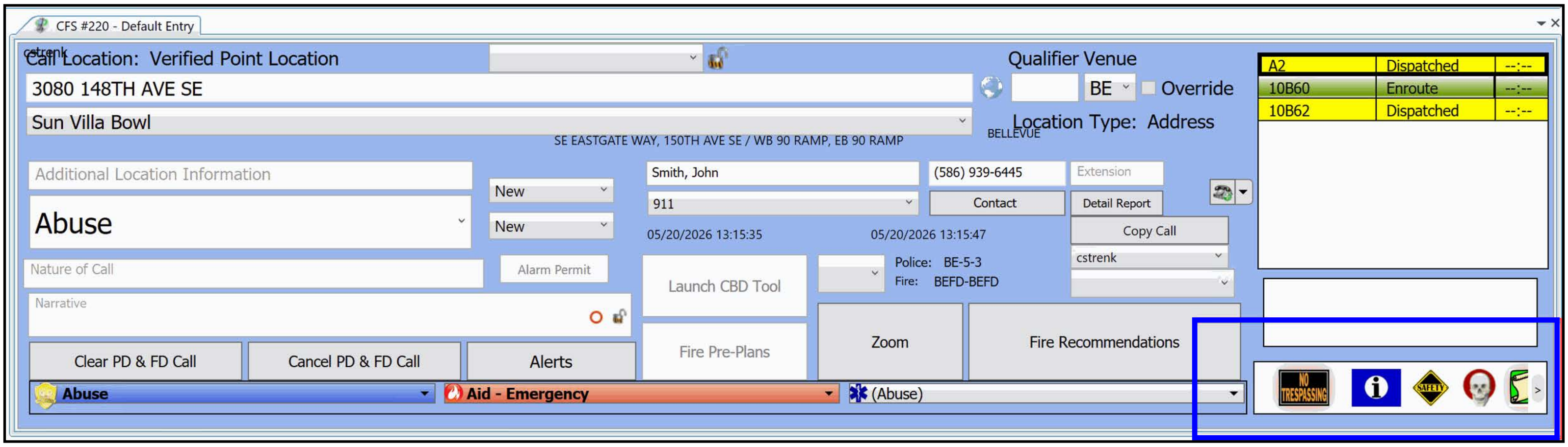
- **Reduced Prior Incident Alert Limit**

  The maximum number of prior incident alerts associated with a Call for Service has been reduced from 1,000 to 99. This helps present a more practical amount of historical information during active call handling while preventing excessively large alert lists.



- **Improved Alert Visibility**

  The alert control panel in the *Call Entry* window now includes a contrasting background color in both light and dark themes, making alert icons easier to distinguish regardless of the selected application theme.



Following are some things to keep in mind for these default setting changes:

- **Applies to New Installations**

  These updated default settings are applied to new *Enterprise CAD* installations beginning with version **2026.3**.
- **Existing Configurations Remain Unchanged**

  Current customer configurations are not automatically modified during an upgrade. Agencies wishing to take advantage of these recommended defaults can review and update the applicable settings as appropriate for their operational needs.
- **Recommended Best Practices**

  These default values reflect recommended configuration settings based on common deployment practices and are intended to improve usability while reducing the need for post-installation adjustments.

RapidSOS Additional Data (RAD) Integration

In **2026.3**, *Enterprise CAD* now integrates RapidSOS Additional Data (RAD) directly into the E911 workflow, giving dispatch personnel immediate access to supplemental caller information without leaving the *Dispatch Client* application.

When available, RapidSOS Additional Data can provide valuable information such as medical profiles, vehicle crash details, alarm information, panic alerts, smart building data, and weapon detection notifications. This information is now available directly on the *E911 Queue* window, making it easier to review, share, and act upon critical incident information during emergency call processing.

In previous versions, dispatchers would have to access the RapidSOS portal to see this additional data.

During emergency calls, every second counts. Having immediate access to supplemental caller information within the *Dispatch Client* helps dispatchers make faster, more informed decisions while reducing the need to switch between applications.

This enhancement helps dispatchers, supervisors, trainers, and command staff:

- **Access Critical Information Faster**

  View available RapidSOS Additional Data directly within the E911 workflow without opening a separate RapidSOS website.
- **Improve Situational Awareness**

  Review supplemental information such as medical details, crash data, alarm information, and smart building data while processing emergency calls.
- **Share Information with First Responders**

  Copy relevant RapidSOS information into the call narrative, additional location information, or chat to help ensure responding personnel receive important incident details.
- **Streamline Emergency Call Handling**

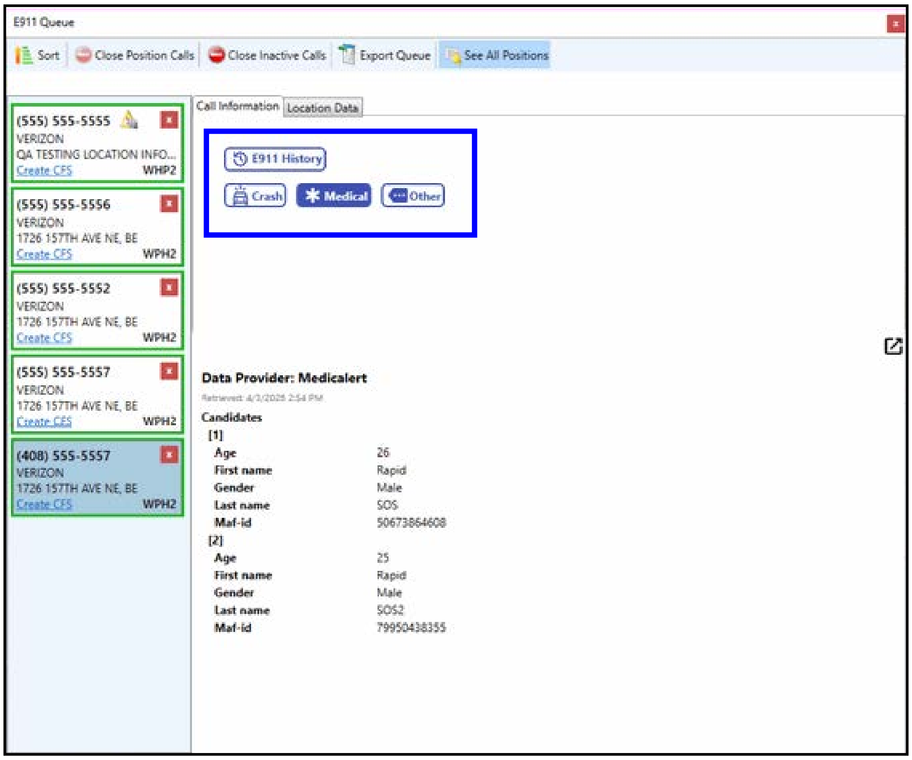
  Keeping supplemental caller information within the *CAD* workflow reduces distractions and allows dispatchers to remain focused on managing the incident.

New RapidSOS Additional Data Integration Functionality

Below are details about the new RapidSOS Additional Data integration:

- **RapidSOS Data Indicators**

  When RapidSOS Additional Data is available for an active 911 call, category buttons appear in the E911 *Call Information* tab, providing immediate visual indication that supplemental information is available.



Additional, or supplemental, data indicators only appear when data is available.

The newly supported additional data categories include:

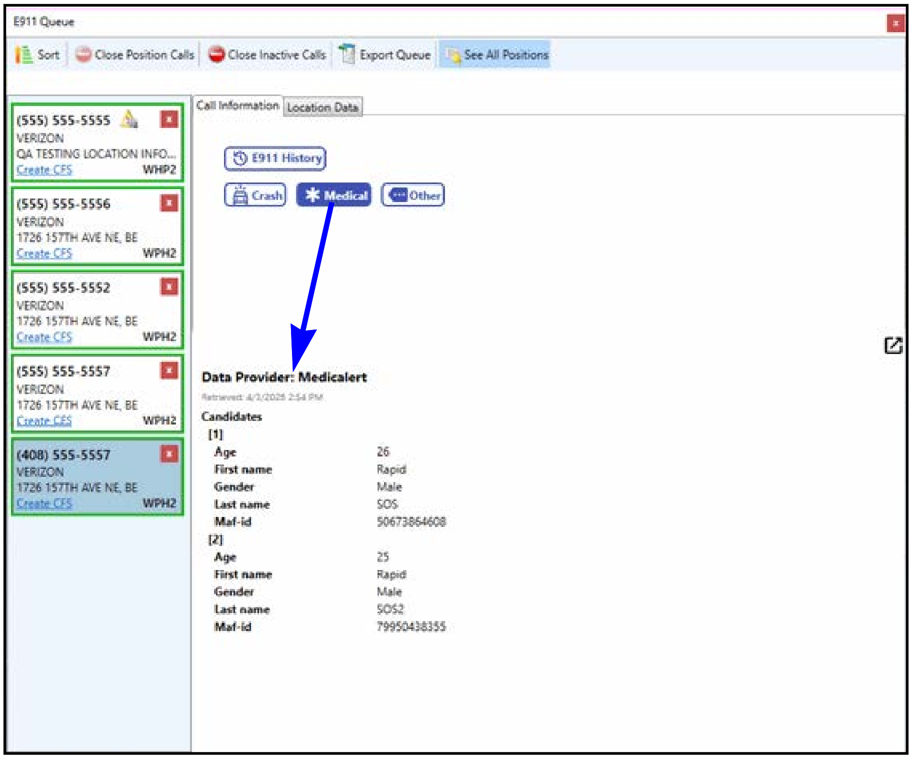
- **Alarm**: Alarm
- **Crash**: Crash
- **Medical**: Medical
- **Panic**: Panic
- **Smart Building**: Smart Building
- **Weapon Detection**: Weapon Detection
- **Other**: Other

- **Improved User Interface**

  The RapidSOS interface has been refined to provide a consistent experience across different screen sizes. Information has been organized for improved readability, and non-essential data has been removed to help focus attention on operationally relevant information.

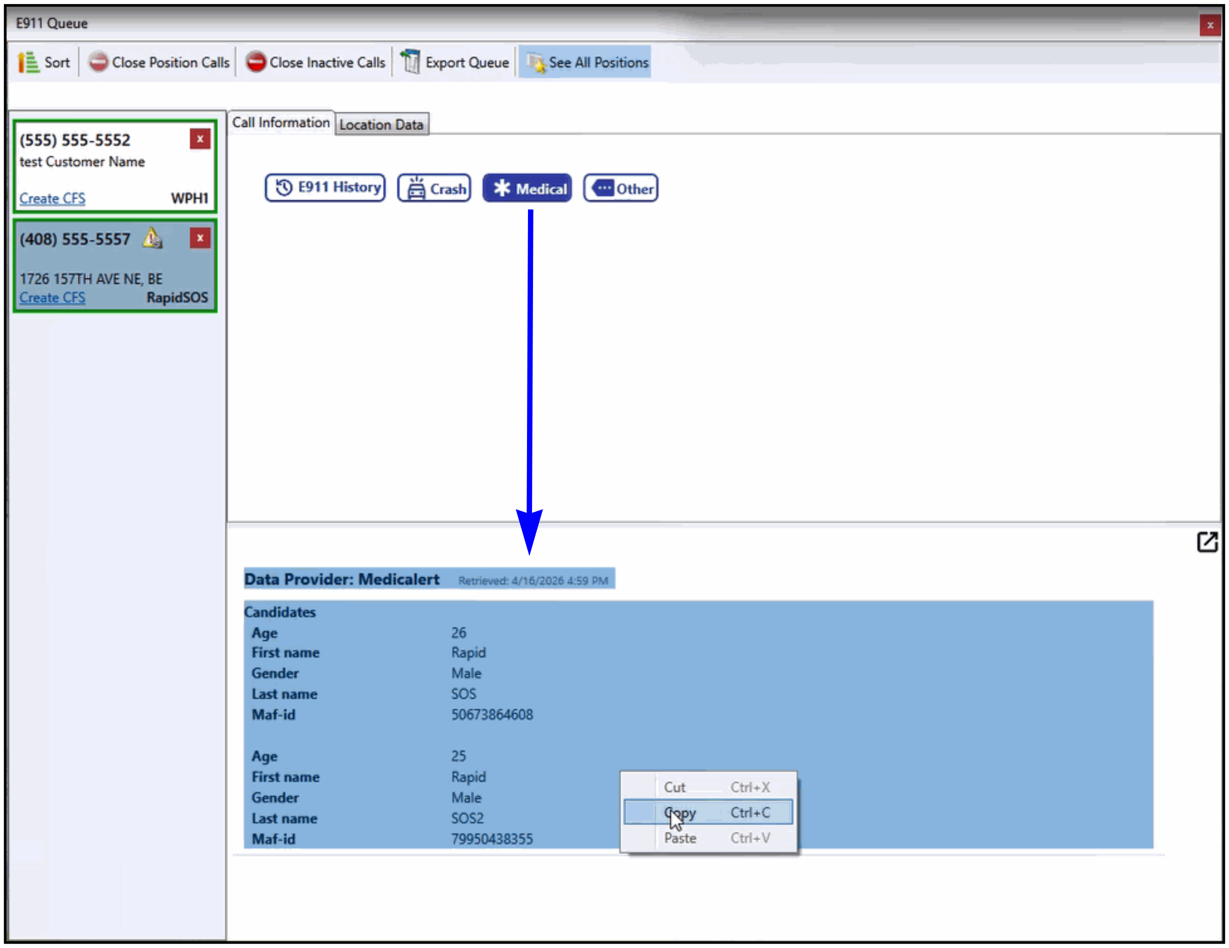
- **View Detailed RapidSOS Information**

  Clicking a RapidSOS category button displays the available information in the *E911 Queue's Details* panel. Information is presented in an easy-to-read format, allowing dispatch personnel to quickly review available caller details without leaving the *Dispatch Client* application.

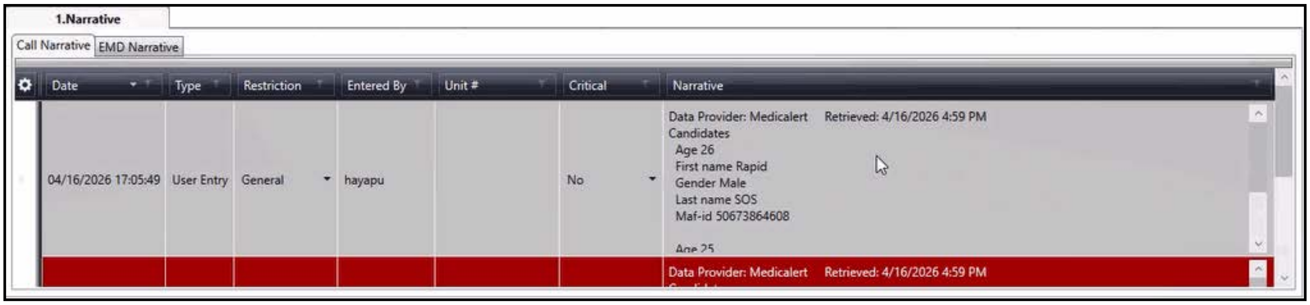


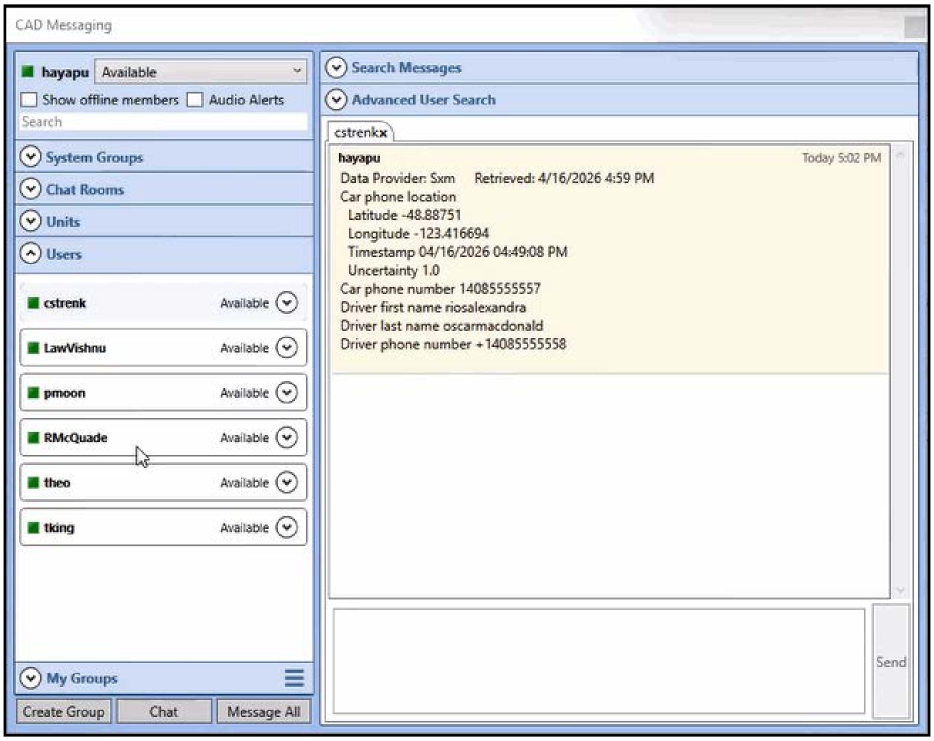
- **Copy Information to a CFS**

  RapidSOS data can be copied and pasted into the ***Narrative*** and ***Additional Location Information*** fields on a CFS, as well as into a *CAD Messaging* chat message, or other appropriate fields, making it easy to share important information with responding personnel. This is accomplished by right-clicking the selected data from the *Call Information* tab on the *E911 Queue* window, and selecting the **Copy** option from the resulting menu.



Dispatchers would then place their cursor in the desired field on the CFS, or in a chat message in *CAD Messaging*, right-click and select **Paste** from the resulting menu.





Following are some things to keep in mind about RapidSOS Additional Data:

- **RapidSOS Data Is Displayed Only When Available**

  RapidSOS Additional Data appears only when supplemental information is available for the active CFS.
- **Supports Improved Information Sharing**

  Relevant RapidSOS information can be copied into the Call for Service, allowing critical details to be shared with responding personnel as part of the normal dispatch workflow.
- **No Agency Configuration Required**

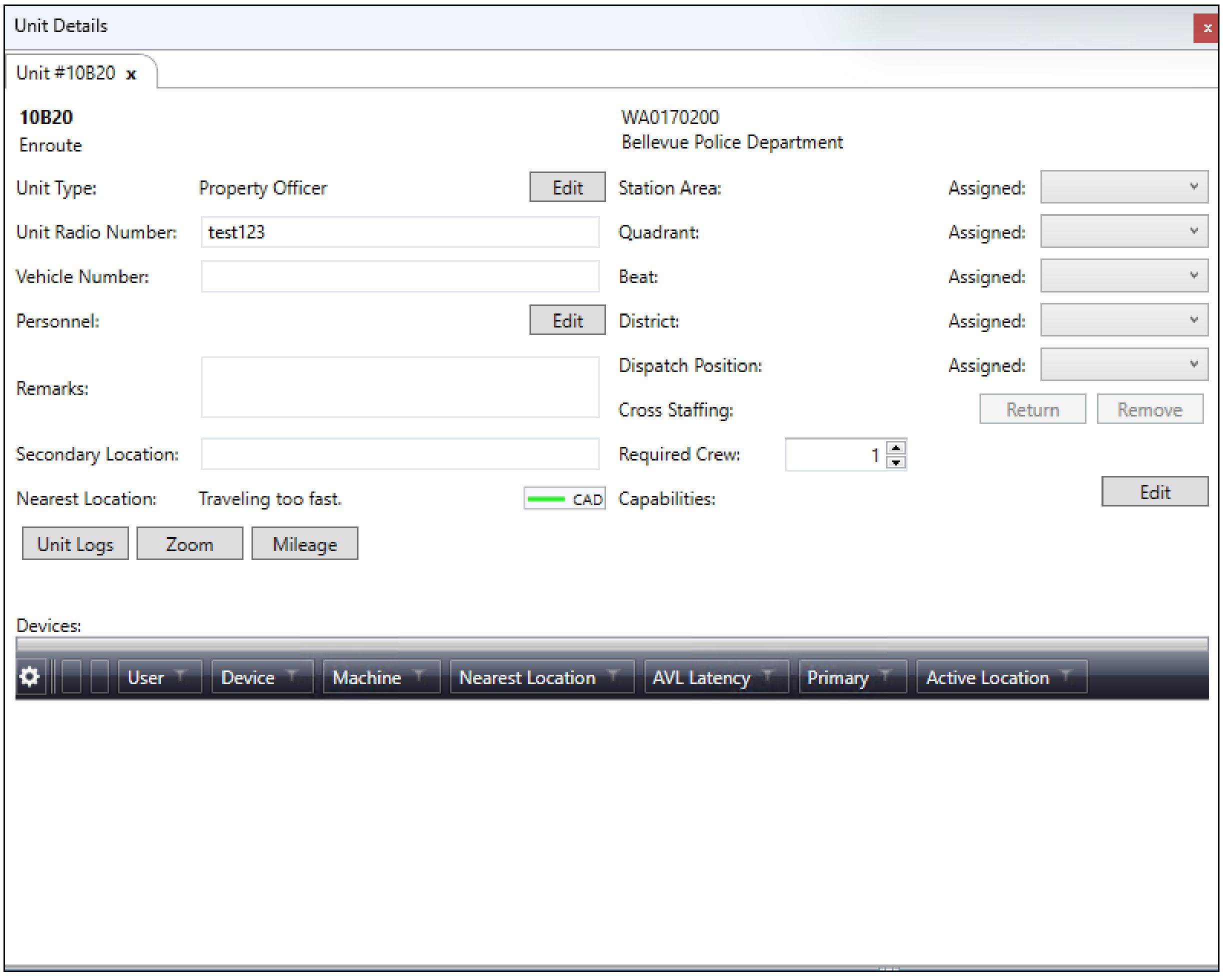
  If RapidSOS is already configured and enabled for an agency, no additional integration is required.

  If not, configuration is done on the *E911 PSAP* page in *E911 Maintenance* in the *Maintenance Client* application.

Unit Details — Added Devices Grid to the Unit Details Window

In previous releases, when the **Devices** button is clicked on the *Unit Details* window, a *Unit Devices* window opens listing the unit number in the window name with a grid that contains information about each device associated to the unit.

Because dispatchers want clear visibility into the unit devices on a unit, devices are now displayed in a grid on the *Unit Details* window in **2026.3**. This gives instant access to unit device information and reduces the number of windows needed to view unit details.



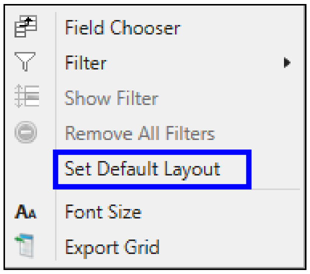
Set Default Layout on Call Details Grids and Call Entry Displays as Call Selected from Call List

Users previously needed to set filters in default lists to enable certain functionality. Additionally, updating templates in *Call Details* required multiple steps, which complicated the process.

In **2026.3**, users no longer need to set filters in lists to enable new call windows to open. When selecting a call from the *Call List*, the *Call Entry* window changes to the selected call in the *Call List*, making it easier to navigate from one call to another.

Additionally, when updating templates in the *Call Details*, users no longer have to perform multiple steps in grid formats and filtering.

Within each *Call Details* windows tab, after arranging the grid, click the **Grid Options** button and choose **Set Default Layout** to retain edits to the layout.



Mapping Client

The *Enterprise CAD Mapping Client*, or *CAD Mapping* window, provides CAD Center users with additional visual information regarding the locations of units and Calls for Service (CFS). The interface provides two-way communication between the *Dispatch Client* application and the *CAD Mapping* window and displays active calls for service and unit locations. Within the *CAD Mapping* window, users can load up to three different map panels in order to display different parts of the map or different map layers.

Sections for details about *Mapping Client* enhancements in **2026.3**:

- "Increased Font Size" on page 64

❖ ❖ ❖ ❖ ❖

Increased Font Size

In previous releases, the font size was difficult to read on high-resolution screens, making it hard to identify important information.

In **2026.3**, font sizes increased for high-resolution screens, making readability accessible for all users. The increased font size for labels on the map makes it easier to identify:

- Unit Numbers, Nearest Address, Latency, Speed
- Unit Devices, Nearest Address, Latency, Speed
- Text Call
- E911
- CFS (Call) Numbers, Address
- Hyperlink Text

GIS generated labels are not affected by this enhancement.

Standard Web Reporting

The *Web Reports* website offers users access to reports that can be run outside of the *Enterprise CAD* suite of applications as the pertinent data from *Enterprise CAD* is replicated and stored on the DSS/Reporting Server. This allows users to run these reports using up-to-date data from *Enterprise CAD*.

sections for details about *Standard Web Reporting* enhancements in **2026.3**:

- "False Burglary Alarm Report — MSP Only" on page 65
- "Enhanced Traffic Stop Reporting in the Officer Activity Report" on page 65

❖ ❖ ❖ ❖ ❖

False Burglary Alarm Report — MSP Only

The **False Burglary Alarm** report provides all alarm calls that were reported as false based on call/unit disposition.

In **2026.3**, The **False Burglary Alarm** report has moved to *Enterprise Records Dynamic Reporting*. This standard web report in *Enterprise CAD* is only available for *MSP* users.

Enhanced Traffic Stop Reporting in the Officer Activity Report

In **2026.3**, the **Officer Activity Report** has been enhanced with a new ***Traffic CFS Types*** multi-select parameter, giving agencies greater control over how traffic stops are identified and counted.

Previously, traffic stop totals were determined using alternate call type values configured behind the scenes. This approach could result in inaccurate counts if alternate values were missing or incorrectly configured. With this enhancement, agencies can explicitly select which Call for Service (CFS) types should be included as traffic stops each time the report is generated.

To improve report transparency, the selected call types are also displayed in the report output, allowing users to easily verify how traffic stop totals were calculated.

Traffic stop data is frequently used for operational reporting, supervisory review, staffing analysis, accreditation, and agency reporting requirements. Accurate and transparent reporting helps ensure confidence in the data used to support operational and administrative decisions.

This enhancement helps dispatchers, supervisors, trainers, and command staff:

- **Improve Reporting Accuracy**

  Traffic stop totals are now based on the call types explicitly selected when the report is generated, reducing the possibility of inaccurate counts caused by missing or incorrect alternate call type configurations.

- **Increase Reporting Flexibility**

  Each agency can define which Call for Service types should be counted as traffic stops without requiring database updates or configuration changes.

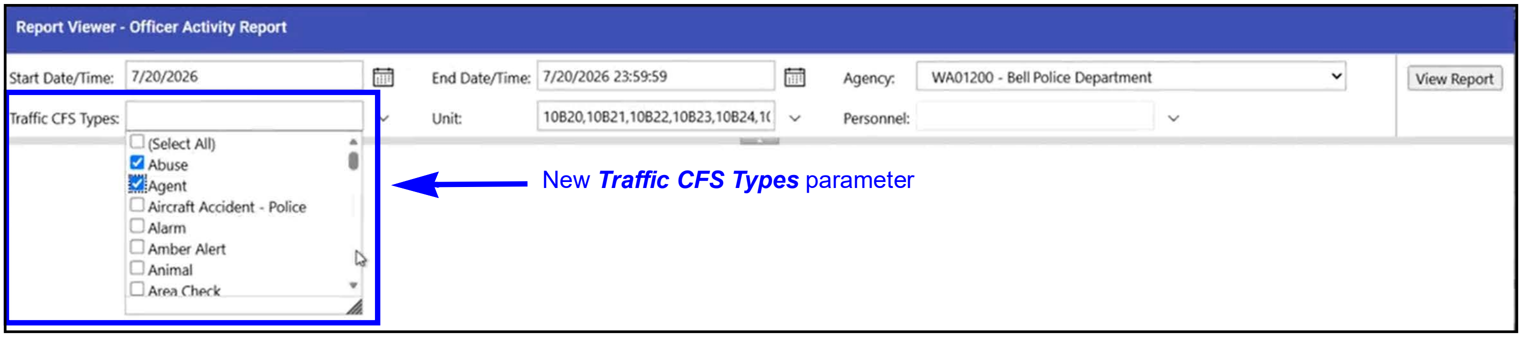
- **Enhance Report Transparency**

  The report clearly identifies which call types were included in the traffic stop count, making report results easier to understand, validate, and audit.

New Traffic CFS Types Functionality

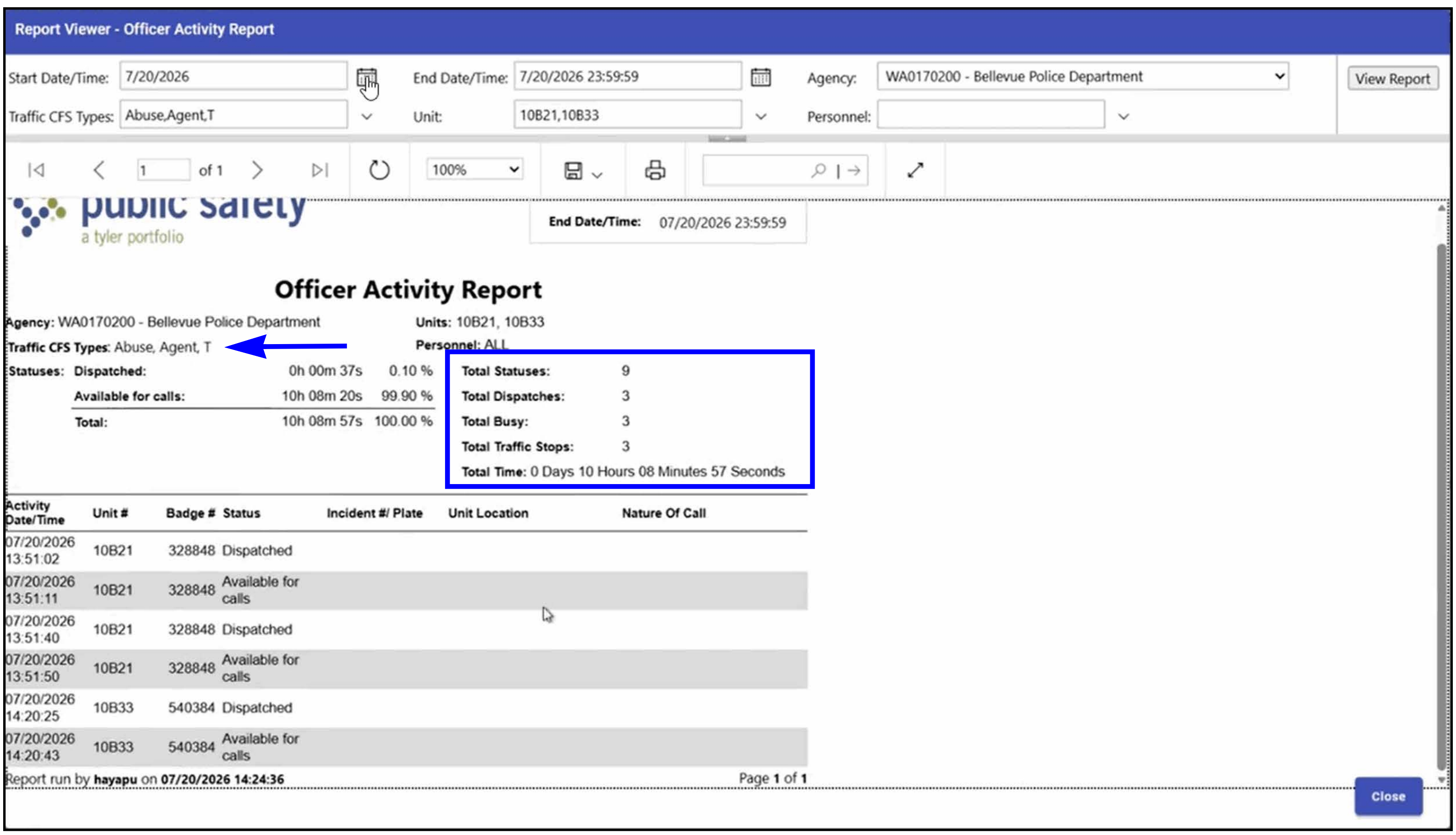
- **Traffic CFS Types Selection**

  A new ***Traffic CFS Types*** multi-select list box has been added to the **Officer Activity Report** parameters. Users can select one or more call types that their agency considers traffic stops to include in the generated report.



- **Traffic Stop Counts Based on Selected Call Types**

  When the report is generated, the traffic stop count includes only calls matching the selected Call for Service types.



- **Traffic CFS Types Output Field**

  A new Traffic CFS Types field has been added to the report output that lists the selected call types, providing a quick reference to the criteria used when generating the report. Hovering over this field displays a tooltip confirming the call types included in the traffic stop count, providing a clear connection between the selected report parameters and the resulting totals.

Things to Remember

Below are some important things to remember when using the new ***Traffic CFS Types*** parameter:

- **Agency Definitions May Differ**

  Each agency determines which Call for Service types should be counted as traffic stops. Select the call types that best match your agency's reporting requirements each time the report is generated.

- **Report Results Reflect Selected Call Types**

  Traffic stop totals are calculated only from the call types selected for that report. Changing the selected call types may produce different totals for the same reporting period.

- **Improved Auditability**

  The report output identifies the call types used to calculate traffic stop totals, making it easier to verify report results and explain how counts were derived.

Recommendation Playback Utility

The *Enterprise CAD Recommendation Playback Utility* allows agency personnel, or *Tyler* personnel, to analyze the recommendations that were used for specific calls for service without having the *Enterprise CAD Dispatch Client* installed. When questions arise as to why one unit was recommended over another, this utility allows for the detailed breakdown of why those units were recommended. From what resources responded and which resources were unfulfilled, to diagnostics and snapshots of the state of the recommendation at the time it was recommended, this utility offers a way to troubleshoot unit recommendations.

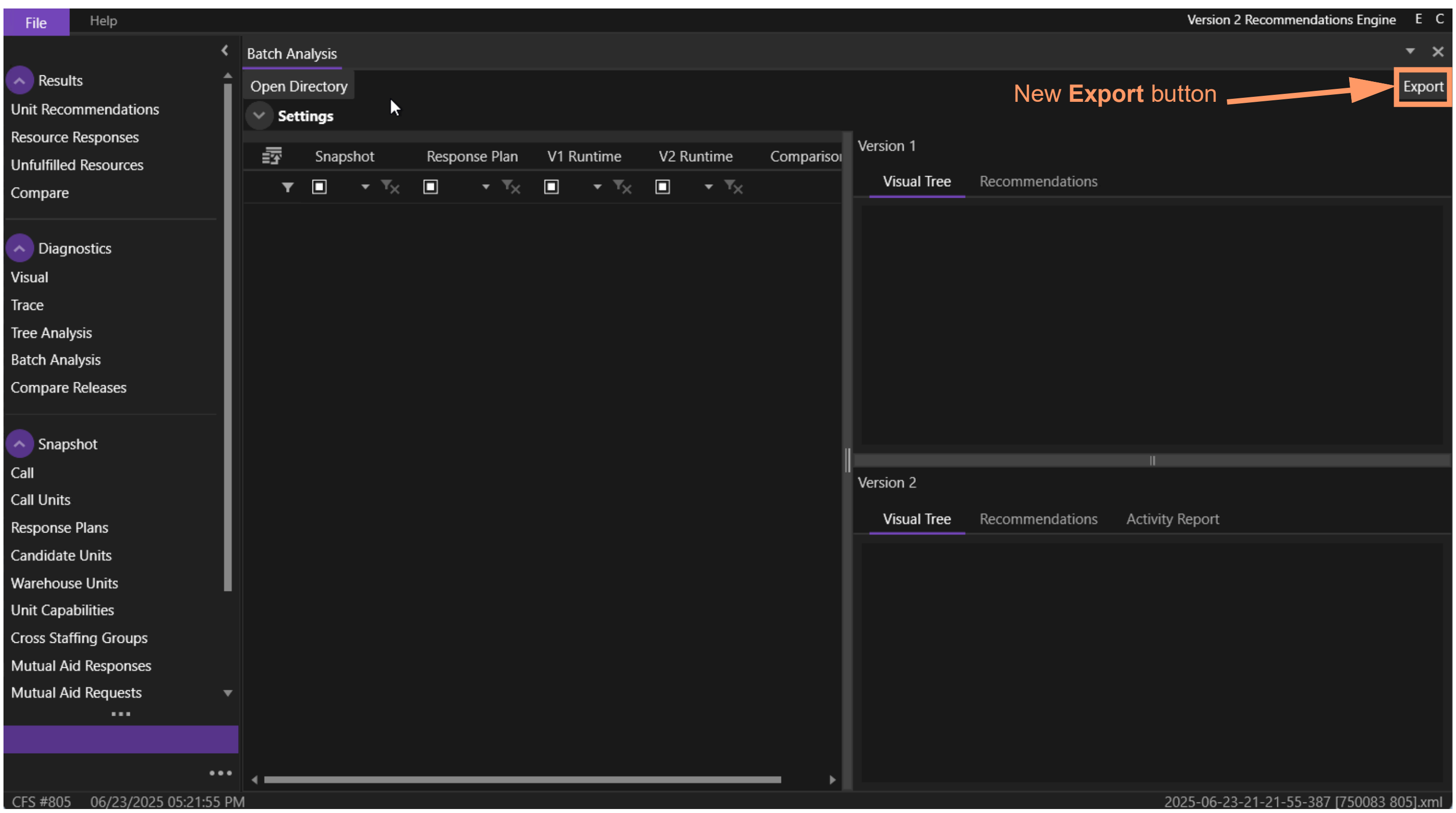
sections for details about *Recommendation Playback Utility* enhancements in **2026.3**:

- "Batch Analysis — Added the Ability to Export Results" on page 68
- "Batch Analysis — Automate Running Batch Analysis" on page 69

Batch Analysis — Added the Ability to Export Results

The *Batch Analysis* tab compares multiple snapshots. Batch analysis is intended to aid an agency's transition to version 2 unit recommendations by providing batch processing of historical snapshot files and notifying users of deviations between the legacy engine and version 2 unit recommendation results. The batch analysis runs the snapshot in both version 1 and version 2 unit recommendations logic and identifies differences in results when they occur. The red x in the list identifies snapshots that may have different results. Selecting that snapshot shows users the differences in the right panes, with version 1 on the top half and version 2 on the bottom.

In **2026.3**, the ability to export results has been added to the *Batch Analysis* tab in the *Recommendation Playback Utility*. A new **Export** button is located in the top right corner of the tab.



The export produces a CSV file that includes:

- Snapshot Name
- Match (true/false)
- Response Plan name

Additionally, the export file indicates which method was used for analysis:

- By Response Plan
- Strict Order
- Maximize Fulfillment

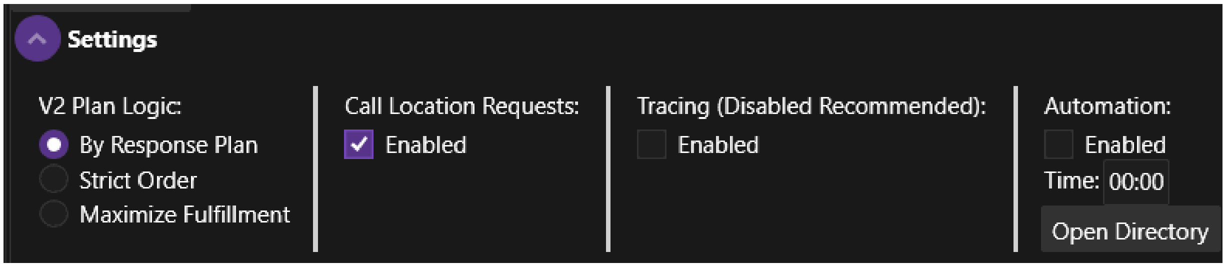
The exported file is saved to the directory the administrator provided in the configuration file. If the *Recommendation Playback Utility* is configured to run automatically, the CSV also automatically exports and saves to the same directory.

Batch Analysis — Automate Running Batch Analysis

The ability to automatically run a batch analysis daily has been added in **2026.3**.

Click the **Settings** button to open the option controls for changing the analysis view or to automate Batch Analysis.

Tip: To change the directory for storing automated exported results, click the **Open Directory** button under the ***Automation*** option and select a directory.



The following options are available in the *Settings* pane:

V2 Plan Logic: Select **By Response Plan**, **Strict Order**, or **Maximize Fulfillment** to see the variation on resource recommendations determined by the three options.

Call Location Requests: When enabled, Call Location Requests are included in the analysis.

Tracing (Disabled Recommended): It is preferred to leave this feature disabled as is slows the analysis process.

Automation: When enabled, users can schedule batch analysis to run daily at the given time.

- ***Enabled***: When selected, users can schedule batch analysis to run daily.
- ***Time***: Enter a time to run the daily batch analysis.
- **Open Directory**: Click this button to select a directory to download the batch analysis files.

Application Cross-over Enhancements

While many enhancements are contained to only one of the *Enterprise CAD* applications, with possible minor setting options in the *Maintenance Client* application, some are related and cross-over to multiple applications. So, for those enhancements that span multiple applications, all of the related information is contained in this section and not split between the application-specific sections of this chapter.

See the following sections for details about enhancements that span multiple *CAD* applications in **2026.3**:

- "Improvements to Enterprise CAD Client Updates" on page 71
- "Enhanced Unit Estimated Time of Arrival (ETA)" on page 74
- "Improved Data Auditing" on page 79

❖ ❖ ❖ ❖ ❖

Improvements to Enterprise CAD Client Updates

Changes have been made in the way that *Enterprise CAD* client updates are delivered, communicated, and applied. This makes updates clearer, safer, and easier for users while reducing disruption during login and ongoing use.

Enterprise CAD has moved toward a version-compatibility model that better manages how clients and services work together. Users can see clearer update messaging, earlier notice when an update is available, stronger warnings when an update becomes mandatory, and a more streamlined update experience when launching and application.

Users now have more visibility into available updates, better warnings before required updates, and a simpler update flow that can return them to the login screen automatically after the update finishes.

This enhancement improves client version management for *Enterprise CAD*. Previously, update behavior could feel inconsistent or require more manual steps. With these changes, the *CAD* communicates update timing, distinguishes between optional and required updates, and automates more of the update process.

These improvements support a broader compatibility strategy designed to let the client and related services evolve with less downtime and fewer surprises, while still ensuring users remain on supported versions when necessary.

The following changes have been made to the update process:

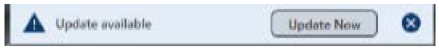
- Better visibility when an update is available so users can act at a convenient time.
- Advance warning before a required update so teams are not caught off guard.
- Clear messaging during application launch when an update must be installed before login.
- More automated update experience that reduces extra clicks and manual relaunch steps.
- Coordinated closing of related *CAD* clients when needed so the update can proceed cleanly.

Optional Update Notifications

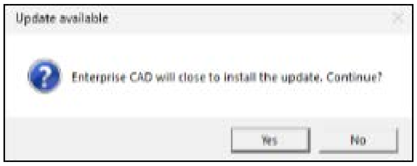
When a new client version is available, users are notified after logging in to the *Dispatch Client*. The notification is visible and actionable without unnecessarily interrupting work.

The notification process is as follows:

- A message appears when the *Dispatch Client* launches after login.
- A message also appears when ***Switch Users*** is used and the view reloads or refreshes.
- The message that displays clearly indicates that an update is available. It appears at the top of the application. click **Update Now** to run the update, or click the **Close** button to install at a later time.



- Users can choose to dismiss the notification or begin the update immediately.
- If the user chooses **Update Now**, another notification displays stating that the application will close.



- If clicking **Yes**, the *Dispatch Client* closes and the update process starts. After the update completes, the login window is displayed again so the user can sign back in.

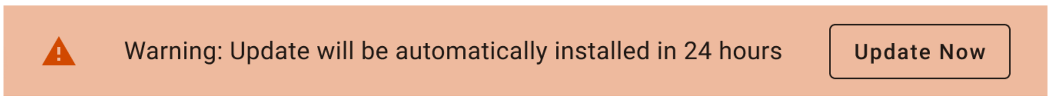
Note: Other related clients are open, such as *Mapping*, *Management*, or *Maintenance*, also close automatically so the update can proceed successfully.

Mandatory Update Warnings

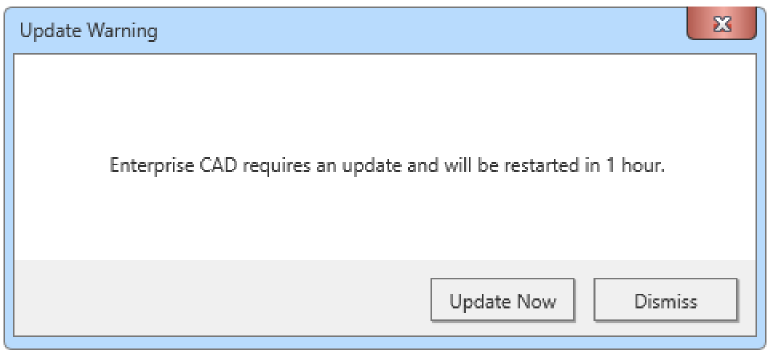
When an update is required, the application warns users ahead of time rather than waiting until users are blocked.

The warning notice stages include:

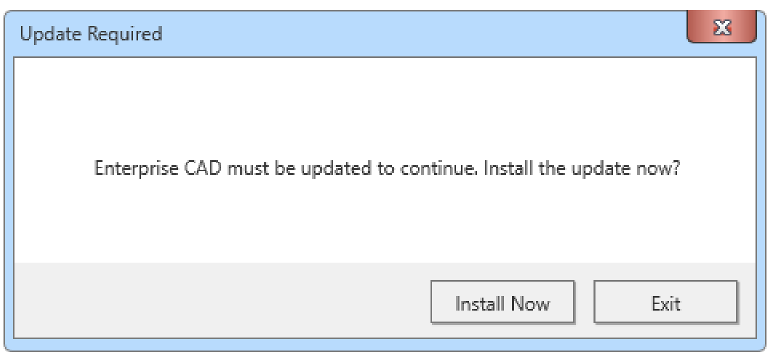
- 24-hour warning before a mandatory update deadline.



- 1-hour warning before the deadline.



- Launch-time warning if the client is started after the mandatory update window has already passed.



These notifications are intended to reduce operational disruption by giving users and agencies time to prepare. Once the update window becomes mandatory, users are informed that action is required to continue using a supported client.

The mandatory workflow is as follows:

- Install closes the *Dispatch Client* and starts the update process.
- If related clients are open, they may also close automatically.
- Exit closes the dialog and closes the *Dispatch Client* without launching the update at that moment.
- If the update is not performed, the process occurs the next time the *Dispatch Client* is launched, based on the launch-time automation described below.

Automated Update Workflow During Application Launch

One of the most important user-facing improvements is the update experience at login. If the client version must be updated before access is allowed, the login screen is intentionally delayed so the update can be addressed first.

Users see messaging explaining that an update is required prior to logging in. The expected choices are straightforward:

- **Install Now** closes the window and begins the update process.
- **Dismiss** or **Exit** cancels the login.

During the process, messaging indicates that the client is being updated. After the update completes, the login window launches automatically so the user can continue without manually reopening the application.

Automatic return to the login window reduces confusion and eliminates an extra manual step after updating.

The update workflow is as follows:

1. A newer version becomes available.
2. The user receives an informational notification while using the *Dispatch Client*.
3. If the update becomes mandatory, the user receives advance warnings before the deadline.
4. If the user launches an out-of-date client after the deadline, the system presents a required update prompt before login.
5. The update process starts and may close related *CAD* clients, if needed.
6. After the update completes, the login window opens automatically.

Operational Considerations:

- **Plan for client restarts**: Updates may close active *CAD* client applications so installation can complete cleanly.
- **Communicate mandatory timeframes internally**: Advance warnings help, but local agencies may still want to notify staff of upcoming required updates.
- **Expect clearer update messaging**: Users will have more direct instructions about what is happening and what action is needed.
- **Expect a more consistent login experience after updates**: The application guides users back to login automatically after the process finishes.

Users will not always be forced to update immediately. The new experience distinguishes between updates that are available and updates that are required. Optional updates can be acknowledged or started by the user, while mandatory updates follow stronger enforcement rules.

Enhanced Unit Estimated Time of Arrival (ETA)

If agency units are equipped with AVL, *Enterprise CAD Mapping Client* and *Dispatch Client* users can see Estimated Time of Arrival (ETA) information for units responding to calls for service. Unit types can also be set up with an ***ETA Alert Threshold*** percentage on the *Unit Types* window which means if the unit deviates from the originally calculated ETA by more than this designated threshold percentage, dispatchers would receive an alert, which is set up in *CAD Maintenance Client*.

The current ETA feature directly relies on the dynamic unit recommendations refresh feature. If the refresh is not being used, users cannot see ETAs. Additionally, the ETA refresh interval is tied to the dynamic recommendations refresh interval. Therefore, ETAs are only calculated during the first 5 minutes of a unit dispatch.

Because ETAs are mainly used to provide an approximate reference to how far a responding unit is from a call, in **2026.3**, ETAs have been redesigned to be independent of unit recommendations. This allows customers to dispatch a unit without using unit recommendations. Additionally, ETAs are available at all times, regardless of the dispatch method for responding units with updated AVL data.

See the following sections for further details about these enhancements:

“Maintenance Client Enhancements”

- “Refined ETA Configuration” on page 75

“Dispatch Client Enhancements”

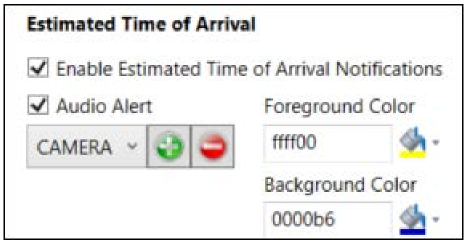
- “ETAs Automatically Refresh Every 30 Seconds” on page 76
- “ETA Display Locations” on page 76
- “How the Redesigned ETAs work” on page 76
- “ETA Deviation Alerts” on page 77
- “Unit Log Updates for ETAs” on page 77
- “Cached ETAs” on page 77

“Mapping Client Enhancements”

- “ETAs Automatically Refresh Every 30 Seconds” on page 78
- “ETA Display Locations” on page 78
- “How the Redesigned ETAs work” on page 78

Maintenance Client Enhancements

Refined ETA Configuration



ETA settings have been updated to reflect the changes to ETA functionality. To access the ETA settings, click Unit on the toolbar to open the *Unit Maintenance* window. Click **Unit Default Settings** button. The *Estimated Time of Arrival* alert settings are located under the *Notification Settings* section.

The ***Display Estimated Time of Arrival Notifications*** check box has been removed because this setting now is always enabled. If a user does not want to see this information, simply hide the ETA information in the *Unit List*, and resize the ETA column in the *Assigned Unit* list in a CFS to hide the ETA. This simplifies maintenance, leaving only the ETA notification settings on this maintenance page.

Additionally, the ***Enable Refresh Frequency___seconds*** has been removed from *Estimated Time of Arrival*. ETAs now automatically refresh every 30 seconds.

Dispatch Client Enhancements

The following enhancements have been made to the *CAD Dispatch Client*:

- "ETAs Automatically Refresh Every 30 Seconds" on page 76
- "ETA Display Locations" on page 76
- "How the Redesigned ETAs work" on page 76
- "ETA Deviation Alerts" on page 77
- "Unit Log Updates for ETAs" on page 77
- "Cached ETAs" on page 77

ETAs Automatically Refresh Every 30 Seconds

In previous releases, ETAs were tied to Unit Recommendations and depended on them being enabled. Additionally, refresh times would be set in the *CAD Maintenance Client*. Each feature has entirely different use cases and purposes. Therefore, in **2026.3**, ETAs have been decoupled from Unit Recommendations and times are automatically refreshed every 30 seconds. This allows dispatchers to use ETAs when sending units to calls without using dynamic Unit Recommendations, allowing them to receive approximate travel times for all units.

ETA Display Locations

ETAs are displayed in the following locations:

- *Unit List*: *ETA* column
- *Call Entry* window (CFS): *Assigned Units ETA* column
- *Mapping Client*: Unit tooltip

How the Redesigned ETAs work

Below describes how the redesigned ETAs work within *Enterprise CAD*:

- When an eligible unit is assigned to a call, its ETA to the call location is immediately calculated and displayed in MM:SS format.
- The ETA continues to update on the 30-second refresh interval until the unit reaches an At Scene status.
- After a unit status reaches At Scene, the ETA displays 00:00.
- If a unit is removed from a call and reassigned, the ETA recalculation begins again.

ETAs are calculated to the geo-verified ***Call Location*** only, not to the assigned location, secondary location, etc.

ETAs require the following conditions. If any are not met, dashes (--:--) are shown instead:

- The unit must be transmitting AVL data.
- The unit must have a valid route to the call.
- The unit must not already be in an At Scene status.

ETA Deviation Alerts

Dispatchers are now alerted when a unit is taking longer than expected to arrive at a call.

If the ETA Alert option is enabled, the system compares the unit's current ETA against the original ETA that was calculated when the unit was first assigned. If the current ETA exceeds the configured threshold percentage for that unit type, an alert displays as follows:

- The ETA column in the Assigned Units area of the Call Entry view will blink using the configured alert color.
- An audible alert sound will play if configured.

Unit Log Updates for ETAs

ETA deviation entries display in the Unit Log. The information included is:

- Original Arrival Time: the initially estimated arrival
- Current Arrival Time: the updated estimate
- Deviation: the difference, displayed in minutes and seconds

For example: Original arrival 14:30:00; Current arrival 14:35:00; Deviation: 5 minutes.

Cached ETAs

To reduce latency on recommendation engine requests, ETAs in **2026.3** are cached for units per call. This reduces the amount of ETA calculation requests made to *GIS*, which increases cost for large volumes of units across long distances. The first request may take time to update, but the subsequent requests should be noticeably faster. Off shifting units or changing unit locations to manipulate the recommended units is also faster than the first request.

If a call location has moved a significant distance, the ETA cache for the call is cleared. Additionally, If a unit's location has moved a significant distance, that unit's ETA is recalculated for that unit. Each entry is issued a new time to location. The recalculation threshhold is 1/4 mile by default. When a call location moves or a recommended unit's locations moves over the recalulation threshhold, the cache clears and the ETAs are recalculated.

Mapping Client Enhancements

The following enhancements have been made to the *Mapping Client*:

- "ETAs Automatically Refresh Every 30 Seconds" on page 78
- "ETA Display Locations" on page 78
- "How the Redesigned ETAs work" on page 78

ETAs Automatically Refresh Every 30 Seconds

In previous releases, ETAs were tied to Unit Recommendations and depended on them being enabled. Additionally, refresh times would be set in the *CAD Maintenance Client*. Each feature has entirely different use cases and purposes. Therefore, in **2026.3**, ETAs have been decoupled from Unit Recommendations and times are automatically refreshed every 30 seconds. This allows dispatchers to use ETAs when sending units to calls without using dynamic Unit Recommendations, allowing them to receive approximate travel times for all units.

ETA Display Locations

ETAs are displayed in the following locations:

- *Unit List*: *ETA* column
- *Call Entry* window (CFS): *Assigned Units ETA* column
- *Mapping Client*: Unit tooltip

How the Redesigned ETAs work

Below describes how the redesigned ETAs work within *Enterprise CAD*:

- When an eligible unit is assigned to a call, its ETA to the call location is immediately calculated and displayed in MM:SS format.
- The ETA continues to update on the 30-second refresh interval until the unit reaches an At Scene status.
- After a unit status reaches At Scene, the ETA displays 00:00.
- If a unit is removed from a call and reassigned, the ETA recalculation begins again.

ETAs are calculated to the geo-verified ***Call Location*** only, not to the assigned location, secondary location, etc.

ETAs require the following conditions. If any are not met, dashes (--:--) are shown instead:

- The unit must be transmitting AVL data.
- The unit must have a valid route to the call.
- The unit must not already be in an At Scene status.

Improved Data Auditing

Enterprise CAD now includes enhanced auditing capabilities for Call for Service (CFS) data. These improvements give supervisors and administrators greater visibility into how users interact with call records, including who viewed sensitive data tabs and when cleared calls were accessed, while keeping audit activity separate from standard operational call logs.

Each audit entry captures the user name, machine name, and a timestamp.

These enhancements help agencies:

- Meet CJIS compliance requirements by maintaining a detailed record of who accessed sensitive call data.
- Support supervisor quality and performance reviews with searchable, filterable access logs.
- Investigate complaints by quickly identifying which users viewed specific calls.
- Keep operational logs clean by separating audit entries from standard call activity.

See the following:

"Dispatch Client Enhancements"

- "CFS Window — Logs Tab — Call Log Sub-Tab — Log NCIC Tab Acess, Alerts Tab Access, and Cleared Call Access" on page 80
- "Search Ribbon — New Call Log Search" on page 81
- "Logs — New Audit Log Categories" on page 82

"Enterprise Security"

- "New Permission in Enterprise Security" on page 83

"Standard Web Reporting"

- "CFS Detail Report — Include Call Log Audits" on page 84

❖ ❖ ❖ ❖ ❖

Dispatch Client Enhancements

The following enhancements have been made to the *CAD Dispatch Client*:

- "CFS Window — Logs Tab — Call Log Sub-Tab — Log NCIC Tab Acess, Alerts Tab Access, and Cleared Call Access" on page 80
- "Search Ribbon — New Call Log Search" on page 81
- "Logs — New Audit Log Categories" on page 82

❖ ❖ ❖ ❖ ❖

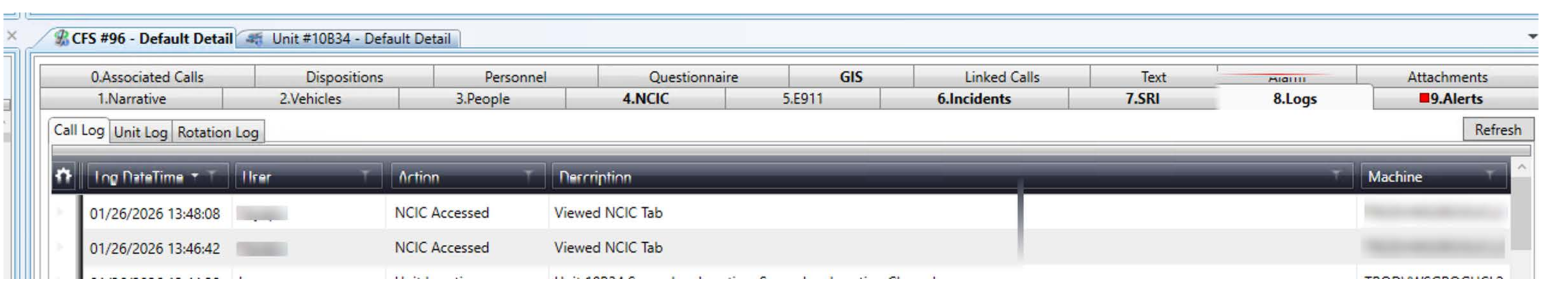
CFS Window — Logs Tab — Call Log Sub-Tab — Log NCIC Tab Acess, Alerts Tab Access, and Cleared Call Access

The *Logs* tab tracks action taken on the call including call creation, changes, clearance, units assigned via a run card or unit recommendation, unit involvement, manual pages, which dispatchers opened up a particular CFS, or service vehicle rotation actions. This information is contained on three sub-tabs: *Call Log*, *Unit Log*, and *Rotation Log*.

The *Call Log* sub-tab allows users to view a listing of call activity, additions, or updates associated with the current CFS, such as the call creation date/time, call timer expiration date and time, vehicle and person additions, etc.

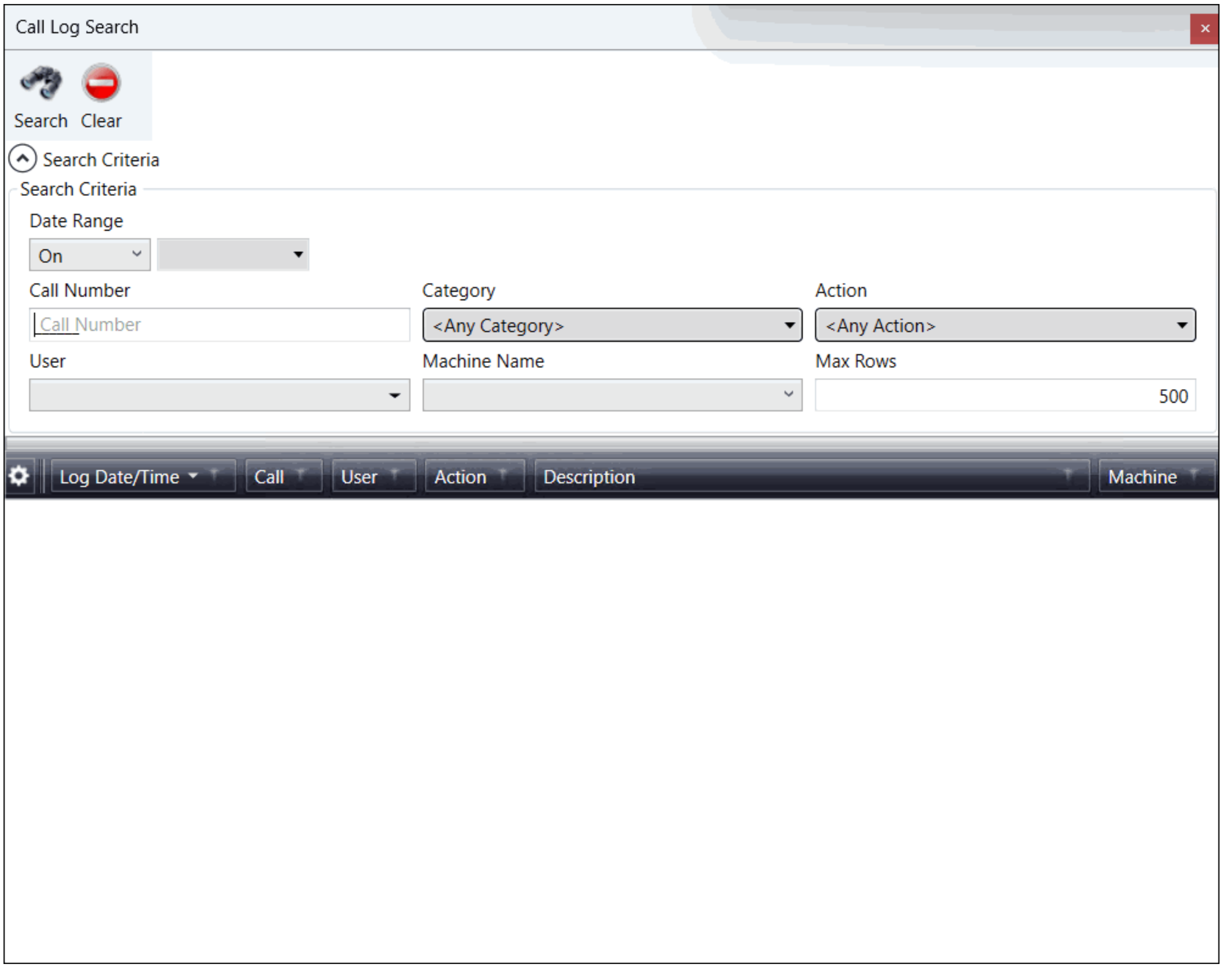
Also, whenever a unit recommendation tab is clicked, the recommended units, including those that are unavailable, are written to the call log. Any time a tab is clicked in recommendations, and new recommendations are returned, the recommendations are logged. Information logged includes the date and time of the recommendation, the user who entered the action, the action (Unit Recommendation) that was taken, a description (includes recommended and unavailable units) of the action, and the MachineID of the person entering the recommendation.

In **2026.3**, the ability to track access to NCIC data, Alerts, and Cleared Calls has been added to the *Call Log* sub-tab. This helps dispatch supervisors to see who has accessed this information, ensuring transparency and compliance with agency policy. Additionally, CJIS auditors can review access logs to identify users who have viewed NCIC data, maintaining compliance with regulations.



Search Ribbon — New Call Log Search

A new Call Log search tool is available in Search in the *Dispatch Client*. Click the **Call Log** button on the *Dispatch Client Search* ribbon to access the *Call Log Search* window.



Supervisors can use this window to search audit activity across all calls using the following filters:

- ***Call Number***: Enter a specific CFS number to search by Call Number.
- ***Date Range***: Select **On**, **Before**, **After**, or **Between** options, then type a date(s) or choose them on the calendar.
- ***Call Number***: Enter a call number to search.
- ***Category***: Select a category from the list, such as **Alarms**, **Call Management**, or **Data Accessed**. Users can make multiple selections. Click **OK** to keep selections.
- ***Action***: Select an action from the list, such as **Address Verified**, **Agency Context Added**, or **Agency Context Canceled**. Users can make multiple selections. Click **OK** to keep selections.
- ***User***: Select a user from the list to search by user name.
- ***Machine Name***: Select a machine from the list to search by workstation name.
- ***Max Rows***: Enter the maximum number of rows to display in search results. The default result limit is 500, with a maximum allowed of 1,000 results.

Results can be exported to *Excel*, with all columns and date values matching the on-screen display.

Logs — New Audit Log Categories

Call log activities are now organized into categories to make searching and filtering more efficient. For example, the *Data Accessed* category groups together NCIC Accessed, Alerts Accessed, and Call Accessed entries, making it easy to isolate data-access activity from operational log entries.

Enterprise Security

The following has been added to Enterprise Security:

- "New Permission in Enterprise Security" on page 83

❖ ❖ ❖ ❖ ❖

New Permission in Enterprise Security

A new *ESS* permission called **Access Call Log Search** has been added under *Maintain Calls*. *CAD* administrators can use this permission to control who can:

- Use the **Call Log Search** on the *Search* Ribbon.
- View audit/accessed entries in the *CFS Call Log* tab.
- Include audit actions when printing a CFS Detail report.

When set to ***Allow***, users can access *Call Log Search*, view and audit entries, and include access information in the printed report.

When set to ***Deny***, The **Call Log Search** button is disabled, audit entries are hidden in the *Call Log*, and the audit option in the *Print* dialog is disabled.

By default, the permission is set to ***Allow*** for all existing roles.

Refer to the *Enterprise Security* online help for details about using the application.

Standard Web Reporting

The *Web Reports* website offers users access to reports that can be run outside of the *Enterprise CAD* suite of applications as the pertinent data from *Enterprise CAD* is replicated and stored on the DSS/Reporting Server. This allows users to run these reports using up-to-date data from *Enterprise CAD*.

The following has been added to *Standard Web Reporting*:

- "CFS Detail Report — Include Call Log Audits" on page 84

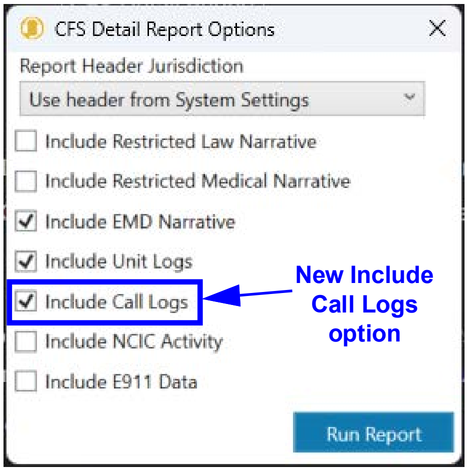
❖ ❖ ❖ ❖ ❖

CFS Detail Report — Include Call Log Audits

The *CFS Detail Report Options* page now includes an ***Include Call Log Audits*** checkbox. When selected, audit and accessed entries are included in the report's *Call Log* section.

This option is cleared by default.

This option is disabled for users without the **Access Call Log Search** permission.



Chapter 2
Mobile Applications

Introduction

This chapter describes enhancements made in the **2026.3** versions of the *Mobile* applications, including *Crew Mobile*, *Shield Mobile*, the *Mobile Management Portal*, etc.

See the following sections for additional information on the enhancements made to the *Mobile* applications:

❖ ❖ ❖ ❖ ❖

Enterprise Mobile and Mobility Applications Renamed

In **2026.3**, the *Enterprise Fire Mobile*, *Enterprise Law Enforcement Mobile*, and *Mobile Web View* applications were renamed to the following:

- *Enterprise Fire Mobile* is now *Crew Mobile*.
- *Enterprise Law Enforcement Mobile* is now *Shield Mobile*.
- The *Mobile Web View* is now the *Mobile Dashboard*.

Additionally, in the **2026.2** *Mobility* release, the *Fire Field Mobile* and *Law Enforcement Field Mobile* apps were renamed to the following:

- *Fire Field Mobile* is now the *Crew Mobile App*.
- *Law Enforcement Field Mobile* is now the *Shield Mobile App*.

To reflect these changes, the *Enterprise Public Safety* applications and associated documentation will be updated where appropriate.

Shield Mobile Enhancements

This section describes the enhancements made in the **2026.3** version of the *Shield Mobile* (*Enterprise Law Enforcement Mobile*) application. Enhancements that are also applicable to the *Crew Mobile* (*Enterprise Fire Mobile*) application are included in the "Crew Mobile Enhancements" section.

Additionally, many of the enhancements covered in this section have related changes on the *Mobile Management Portal* (*MMP*). Those changes can be found in the "Mobile Management Portal Enhancements" section.

See the following sections for additional information on the enhancements made to the *Shield Mobile* application:

❖ ❖ ❖ ❖ ❖

Running Multiple Instances of Shield Mobile

At times, the work of certain *Shield Mobile* users, such as those at state agencies, requires them to assist agencies across various counties/jurisdictions. Because of this, they need to be able to access multiple *Enterprise CAD* systems to retrieve their agency data and be dispatched to nearby calls for service. In previous versions of *Shield Mobile*, however, since only one instance of the application could be installed on a device, users had to contact a *Tyler Technologies* representative to change their agency's configuration settings to point to another agency's environment each time they traveled to a different county/jurisdiction.

In **2026.3**, users can now install and run up to three instances of *Shield Mobile* on a single device simultaneously. This enhancement eliminates the need to contact *Tyler Technologies* when traveling between counties/jurisdictions, allowing users to seamlessly monitor calls and access data across different agency environments.

Note: Running multiple instances of *Shield Mobile* requires an initial configuration by *Tyler Technologies*.

For additional information, contact a *Tyler Technologies* representative.

Data Archive Hyperlink for Location Alerts

The *Alerts* section of the *Assigned Dispatch* and *Incident Inquiry Result* windows in *Shield Mobile* provides users with important information about the CFS they are dispatched to, including prior incidents that occurred at the call location, building preplans, and officer safety messages about a person or vehicle. These alerts are sourced from *Enterprise CAD* or *Enterprise Records*.

Previously, when a CFS had a location alert containing information from the *Data Archive* application, its description contained a URL for the alert entry in *Data Archive*. However, this URL was read-only, requiring users to manually type it into their browser to view additional information about the alert.

In **2026.3**, the URL displaying for location alerts containing information from *Data Archive* has been replaced with the **View In Data Archive** hyperlink. Clicking this link opens the *Data Archive* application, where users can view additional information about the alert after logging in.

Chat Messages Updates

The *Shield Mobile* application offers chat messaging functionality that allows users to easily communicate with their peers throughout the *Enterprise Public Safety* suite of applications. This includes chatting with an individual user, groups of users, and within chat rooms.

In **2026.3**, multiple enhancements have been made to *Shield Mobile* concerning chat functionality. For additional information on these enhancements, see the following sections:

- "Missed Chat Messages Notifications Update" on page 96
- "Scroll Bar on Chats Updated" on page 97

❖ ❖ ❖ ❖ ❖

Missed Chat Messages Notifications Update

When users miss a chat message - whether this is due to not having the *Mobile Instant Communication window* open or being logged out of *Shield Mobile* - the **New Message** button appears in the upper-right corner of the status bar and begins flashing to gain their attention. The button also contains a red badge that, in previous versions of *Shield Mobile*, represented the number of chats with missed messages.

In **2026.3**, the number that displays on the **New Message** button has been updated to reflect the total number of missed messages the user currently has across all chats. Additionally, with this new functionality, it is important to keep in mind is that once a chat with unread messages is opened, the entire conversation is automatically marked as read, regardless of whether the user actually read all of the missed messages.

For example, consider the following:

- The user is actively chatting with user A.
- They are also chatting with users B, C, and D in a group chat.
- The chat with user A has three missed messages.
- The group chat with users B, C, and D has 15 missed messages.

In previous versions of *Shield Mobile*, the number displaying on the **New Message** button would have shown as 2. However, with the changes made to this functionality in the **2026.3** release, the number displaying would now show as 18.

If the user opens the group chat with users B, C, and D, the entire conversation is marked as read, regardless of whether the user actually reads through all the messages they missed. At this point, the **New Messages** button would now show as 3.

Scroll Bar on Chats Updated

When the user has an individual chat, group chat, or chat room open, they can scroll through previous messages using their mouse or the scroll bar on the right. If they continue scrolling and reach the top of the chat, additional messages display, if available. However, in previous versions of *Shield Mobile*, when using the scroll bar, additional messages displayed only after the user released their hold on it.

In **2026.3**, this functionality was enhanced so additional messages continue to load without requiring users to release their hold on the scroll bar.

Ability to Choose the User's Status When Creating a New CFS

In *Shield Mobile*, the *Create Call* window allows users to quickly create a new CFS directly from within the application. After entering/selecting information from the window's fields, clicking the **Send** button creates the new CFS. Unless the ***Stay On Assigned Call*** check box is selected, the *Assigned Dispatch* window opens, the user is assigned to the new CFS, and their status is automatically updated to Dispatched.

In **2026.3**, when the ***Enable Unit Status Selection*** check box is selected in the *MMP*, the **Send** button is replaced with **On Scene**, **Enroute**, and **Dispatched** buttons. These new buttons function similarly to the **Send** button for CFS creation, but instead allow the user to choose whether their status is set to On Scene, Enroute, or Dispatched.

Tip: For additional information on the ***Enable Unit Status Selection*** check box, see "Enable Unit Status Selection Check Box" on page 102.

For example, if the user is creating a new CFS directly from the scene of a crime, they can click the **On Scene** button when finished entering/selecting information on the *Create Call* window and their status is automatically set to On Scene after the CFS is created. This saves them time so they do not have to manually go and change their status from Dispatched to On Scene, as they would have had to do previously.

Alternatively, as there may be times when users need to create a CFS while staying on the one they are currently dispatched to, selecting the ***Stay On Assigned Call*** check box when the **On Scene**, **Enroute**, and **Dispatched** buttons are displayed on the navigation bar removes them and displays the **Send** button again.

Note: As with the **Send** button, the **On Scene**, **Enroute**, and **Dispatched** buttons only enable after a selection is made from the ***Call Type*** list. Additionally, the icons associated with these buttons may vary from agency to agency as they can be configured by their administrators in the *MMP*.

For additional information on configuring unit/apparatus status icons, refer to the *Mobile Management Portal Administrator Guide* or *Mobile Management Portal Online Help*.

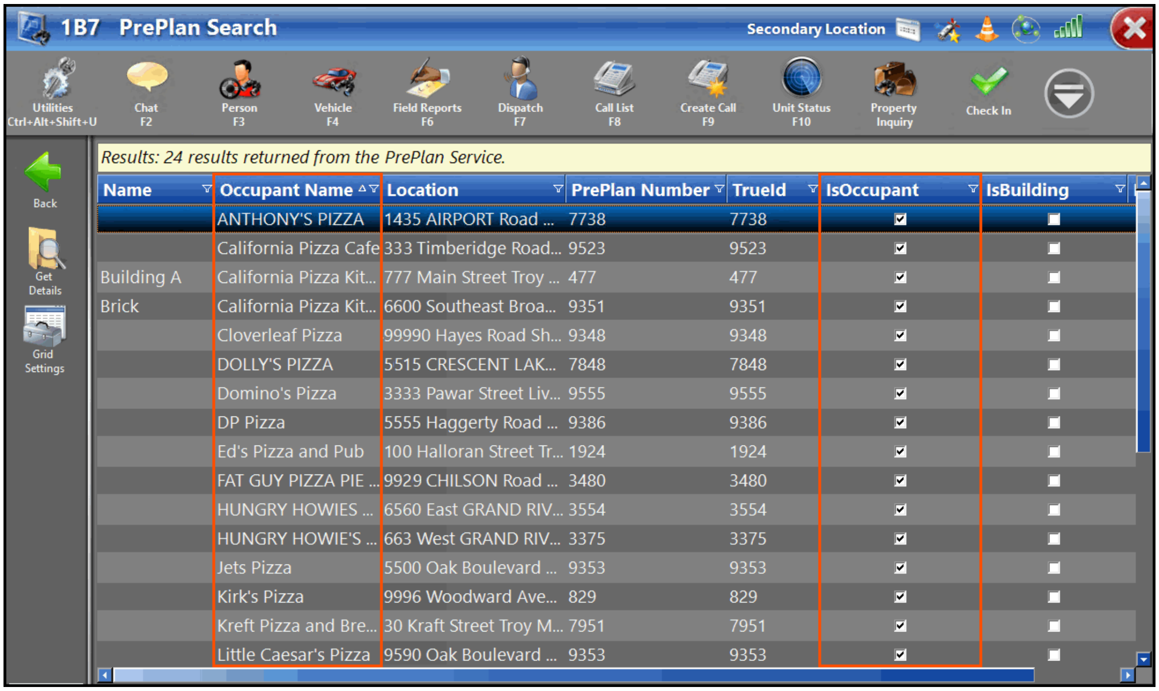
New Columns on PrePlan Search Results Grid for Agencies Using Fire Prevention Mobile

In *Shield Mobile*, the *PrePlan Search* window allows users to search their agency's *Enterprise Records*, *MSP LERMS*, or *Fire Prevention Mobile* database for preplan documents that are associated with a specific location. These documents provide important information about the location the user is traveling to, such as exit locations and potential hazards, including chemicals or highly flammable materials.

In **2026.3**, two new columns, IsOccupant and Occupant Name, now display in the search results grid on the *Preplan Search* window for agencies using *Fire Prevention Mobile* as their preplan source.

- IsOccupant column: Contains a check box that is automatically selected for search results that are associated with a specific occupant in a structure. Examples of occupants include retail stores and restaurants in shopping malls and strip malls.
- Occupant Name column: Displays the name of the occupant returned in the search results. Note that information only displays in this column when the check box in the IsOccupant column is selected for the search result.

Best Practice: For additional information on *Fire Prevention Mobile*, contact the *Fire Prevention Mobile Support* team.



Viewing Calls by Context

In *Shield Mobile*, the *Call List* window displays all active and pending calls for the agencies assigned to the user in *ESS*. However, at times, users may need to view calls outside their assigned agencies, especially when they share the same context - Police, Fire, or EMS.

In **2026.3**, *Shield Mobile* now has enhanced visibility for users whose role in *ESS* has the **View Calls by Context(s**) permission set to **Allow**. With this permission enabled, the *Call List* window now displays:

- Calls that have the same context as the user's unit, including secondary and tertiary contexts.
- Calls where a dispatched unit/apparatus has the same context as the user's unit.

Tip: For additional information on setting permissions for user roles in *ESS*, including **View Calls by Context(s)**, refer to the *Enterprise Security Online Help*.

Incident Number Added to Ticket Export

Previously, officers writing tickets while dispatched to a Call for Service had to manually enter the incident number into their external ticketing application.

In **2026.3**, *Mobile* now automatically includes the unit's active incident number when exporting a ticket to an external ticketing application. This enhancement eliminates that extra step and helps ensure the correct incident number is included with the exported ticket.

Client Impact

Officers frequently write tickets while responding to or working an active incident. Having the incident number automatically included in the ticket information reduces duplicate data entry and allows officers to spend more time focused on their field activities.

This enhancement helps officers and agencies:

- **Reduce Manual Data Entry**

  Officers no longer need to re-enter the incident number into an external ticketing application when writing a ticket during an active call.
- **Improve Efficiency**

  Automatically transferring the incident number streamlines the ticket-writing process, particularly for officers and agencies handling a high volume of tickets.
- **Maintain Accurate Incident Information**

  Including the active incident number directly in the exported ticket helps ensure the ticket is associated with the appropriate incident.

New Incident Number to Ticket Export Functionality

When an officer exports a ticket from *Mobile*, the unit's active incident number is now included in the exported XML file when one is available. The XML file can then be consumed by supported external ticketing applications, such as *BadgerTracs*™ and *Report Beam*™.

If the unit does not have an active incident number when the ticket is exported, the incident number field is omitted and the ticket export proceeds as it did previously.

Things to Remember

Below are some important things to remember:

- **Requires an Active Incident**

  The incident number is included only when the officer's unit has an active incident at the time the ticket is exported.
- **No Change When No Incident Is Available**

  If no active incident number exists, the ticket export continues normally without an incident number.

Crew Mobile Enhancements

This section describes the enhancements made in the **2026.3** version of the *Crew Mobile* (*Enterprise Fire Mobile*) application. Enhancements that are also applicable to the *Shield Mobile* (*Enterprise Law Enforcement Mobile*) application are included in the "Shield Mobile Enhancements" section.

Additionally, many of the enhancements covered in this section have related changes on the *Mobile Management Portal* (*MMP*). Those changes can be found in the "Mobile Management Portal Enhancements" section.

See the following sections for additional information on the enhancements made to the *Crew Mobile* application:

❖ ❖ ❖ ❖ ❖

Real Time Updates for Benchmark Time Functionality

In *Crew Mobile*, the *Benchmark Times* dialog is used to view and record the completion of specific events - known as benchmarks - that are associated with a CFS, such as the time first responders established their command center at a location or when they got a fire under control. These events can be marked as complete by any *Crew Mobile* or *Crew Mobile App* (*Fire Field Mobile*) user dispatched to the CFS, along with *Enterprise CAD* users.

Previously, if the user wanted to view updates made to benchmark events by other users, they had to manually refresh the *Benchmark Times* dialog by either closing and reopening it.

In **2026.3**, the *Benchmark Times* dialog has been enhanced so that when other users make changes to benchmark events, the dialog automatically updates in real time without requiring any action from the *Crew Mobile* user.

Running Multiple Instances of Crew Mobile

At times, the work of certain *Crew Mobile* users, such as those at state agencies, requires them to assist agencies across various counties/jurisdictions. Because of this, they need to be able to access multiple *Enterprise CAD* systems to retrieve their agency data and be dispatched to nearby calls for service. In previous versions of *Crew Mobile*, however, since only one instance of the application could be installed on a device, users had to contact a *Tyler Technologies* representative to change their agency's configuration settings to point to another agency's environment each time they traveled to a different county/jurisdiction.

In **2026.3**, users can now install and run up to three instances of *Crew Mobile* on a single device simultaneously. This enhancement eliminates the need to contact *Tyler Technologies* when traveling between counties/jurisdictions, allowing users to seamlessly monitor calls and access data across different agency environments.

Note: Running multiple instances of *Crew Mobile* requires an initial configuration by *Tyler Technologies*.

For additional information, contact a *Tyler Technologies* representative.

Data Archive Hyperlink for Location Alerts

The *Alerts* section of the *Assigned Dispatch* and *Incident Inquiry Result* windows in *Crew Mobile* provides users with important information about the CFS they are dispatched to, including prior incidents that occurred at the call location, building preplans, and officer safety messages about a person or vehicle. These alerts are sourced from *Enterprise CAD* or *Enterprise Records*.

Previously, when a CFS had a location alert containing information from the *Data Archive* application, its description contained a URL for the alert entry in *Data Archive*. However, this URL was read-only, requiring users to manually type it into their browser to view additional information about the alert.

In **2026.3**, the URL displaying for location alerts containing information from *Data Archive* has been replaced with the **View In Data Archive** hyperlink. Clicking this link opens the *Data Archive* application, where users can view additional information about the alert after logging in.

Chat Messages Updates

The *Crew Mobile* application offers chat messaging functionality that allows users to easily communicate with their peers throughout the *Enterprise Public Safety* suite of applications. This includes chatting with an individual user, groups of users, and within chat rooms.

In **2026.3**, multiple enhancements have been made to *Crew Mobile* concerning chat functionality. For additional information on these enhancements, see the following sections:

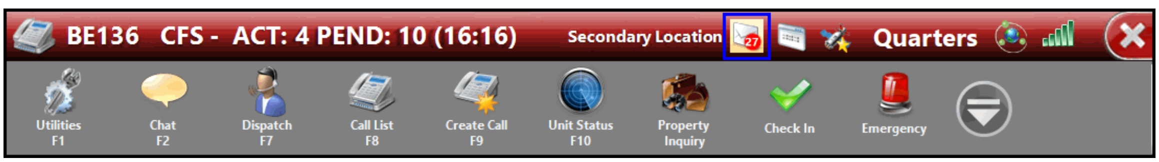
- “Missed Chat Messages Notifications Update” on page 96
- “Scroll Bar on Chats Updated” on page 97

❖ ❖ ❖ ❖ ❖

Missed Chat Messages Notifications Update

When users miss a chat message - whether this is due to not having the *Mobile Instant Communication window* open or being logged out of *Crew Mobile* - the **New Message** button appears in the upper-right corner of the status bar and begins flashing to gain their attention. The button also contains a red badge that, in previous versions of *Crew Mobile*, represented the number of chats with missed messages.

In **2026.3**, the number that displays on the **New Message** button has been updated to reflect the total number of missed messages the user currently has across all chats. Additionally, with this new functionality, it is important to keep in mind is that once a chat with unread messages is opened, the entire conversation is automatically marked as read, regardless of whether the user actually read all of the missed messages.



For example, consider the following:

- The user is actively chatting with user A.
- They are also chatting with users B, C, and D in a group chat.
- The chat with user A has three missed messages.
- The group chat with users B, C, and D has 15 missed messages.

In previous versions of *Crew Mobile*, the number displaying on the **New Message** button would have shown as 2. However, with the changes made to this functionality in the **2026.3** release, the number displaying would now show as 18.

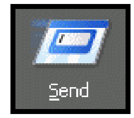
If the user opened the group chat with users B, C, and D, the entire conversation is marked as read, regardless of whether the user actually reads through all the messages they missed. At this point, the **New Messages** button would now show as 3.

Scroll Bar on Chats Updated

When the user has an individual chat, group chat, or chat room open, they can scroll through previous messages using their mouse or the scroll bar on the right. If they continue scrolling and reach the top of the chat, additional messages display, if available. However, in previous versions of *Crew Mobile*, when using the scroll bar, additional messages displayed only after the user released their hold on it.

In **2026.3**, this functionality was enhanced so additional messages continue to load without requiring users to release their hold on the scroll bar.

Ability to Choose the User’s Status When Creating a New CFS



In *Crew Mobile*, the *Create Call* window allows users to quickly create a new CFS directly from within the application. After entering/selecting information from the window’s fields, clicking the **Send** button creates the new CFS. Unless the ***Stay On Assigned Call*** check box is selected, the *Assigned Dispatch* window opens, the user is assigned to the new CFS, and their status is automatically updated to Dispatched.

In **2026.3**, when the ***Enable Unit Status Selection*** check box is selected in the *MMP*, the **Send** button is replaced with **On Scene**, **Enroute**, and **Dispatched** buttons. These new buttons function similarly to the **Send** button for CFS creation, but instead allow the user to choose whether their status is set to On Scene, Enroute, or Dispatched.

Tip: For additional information on the ***Enable Unit Status Selection*** check box, see “Enable Unit Status Selection Check Box” on page 102.

For example, if the user is creating a new CFS directly from the scene of a crime, they can click the **On Scene** button when finished entering/selecting information on the *Create Call* window and their status is automatically set to On Scene after the call is created. This saves them time so they do not have to manually go and change their status from Dispatched to On Scene, as they would have had to do previously.

Alternatively, as there may be times when users need to create a CFS while staying on the one they are currently dispatched to, selecting the ***Stay On Assigned Call*** check box when the **On Scene**, **Enroute**, and **Dispatched** buttons are displayed on the navigation bar removes them and displays the **Send** button again.

Note: As with the **Send** button, the **On Scene**, **Enroute**, and **Dispatched** buttons only enable after a selection is made from the ***Call Type*** list. Additionally, the icons associated with these buttons may vary from agency to agency as they can be configured by their administrators in the *MMP*.

For additional information on configuring apparatus/unit status icons, refer to the *Mobile Management Portal Administrator Guide* or *Mobile Management Portal Online Help*.

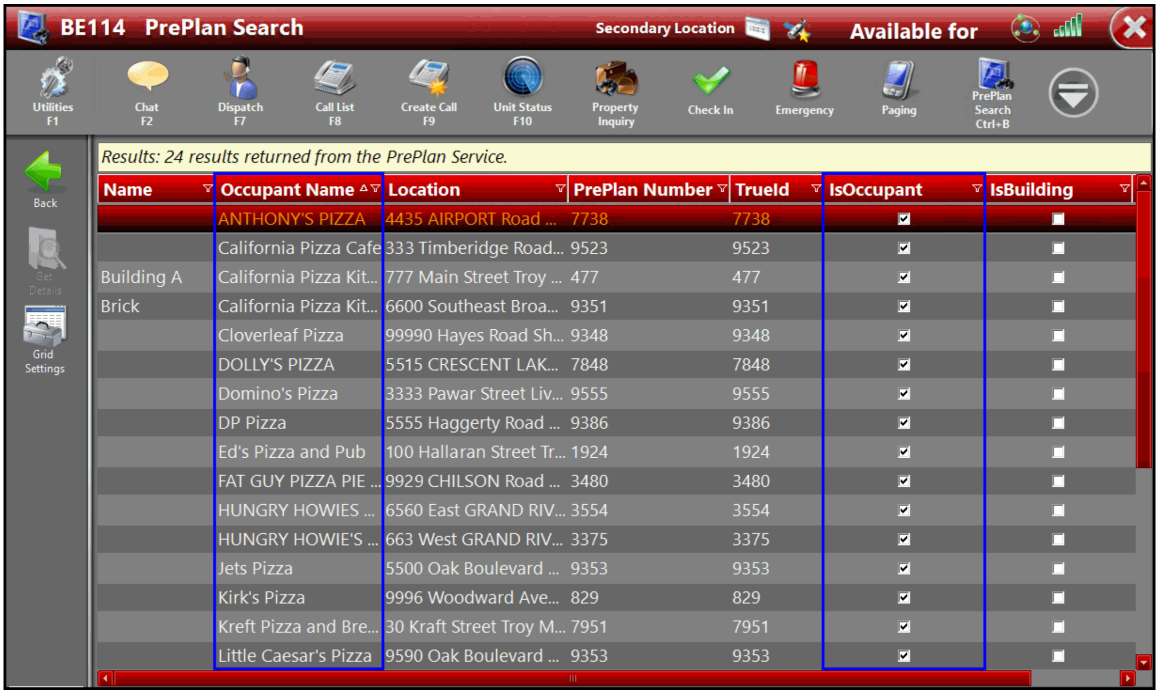
New Columns on PrePlan Search Results Grid for Agencies Using Fire Prevention Mobile

In *Fire Mobile*, the *PrePlan Search* window allows users to search their agency's *Enterprise Records*, *MSP Fire Records*, or *Fire Prevention Mobile* database for preplan documents that are associated with a specific location. These documents provide important information about the location the user is traveling to, such as exit locations and potential hazards, including chemicals or highly flammable materials.

In **2026.3**, two new columns, IsOccupant and Occupant Name, now display in the search results grid on the *Preplan Search* window for agencies using *Fire Prevention Mobile* as their preplan source.

- IsOccupant column: Contains a check box that is automatically selected for search results that are associated with a specific occupant in a structure. Examples of occupants include retail stores and restaurants in shopping malls and strip malls.
- Occupant Name column: Displays the name of the occupant returned in the search results. Note that information only displays in this column when the check box in the IsOccupant column is selected for the search result.

Best Practice: For additional information on *Fire Prevention Mobile*, contact the *Fire Prevention Mobile Support* team.



Viewing Calls by Context

In *Crew Mobile*, the *Call List* window displays all active and pending calls for the agencies assigned to the user in *ESS*. However, at times, users may need to view calls outside their assigned agencies, especially when they share the same context - Police, Fire, or EMS.

In **2026.3**, *Crew Mobile* now has enhanced visibility for users whose role in *ESS* has the **View Calls by Context(s**) permission set to **Allow**. With this permission enabled, the *Call List* window now displays:

- Calls that have the same context as the user's apparatus, including secondary and tertiary contexts.
- Calls where a dispatched apparatus/unit has the same context as the user's apparatus.

Tip: For additional information on the setting permissions for user roles in *ESS*, including **View Calls by Context(s)**, refer to the *Enterprise Security Online Help*.

Mobile Management Portal Enhancements

This section describes the enhancements made in the **2026.3** version of the *Mobile Management Portal (MMP)*.

Often times, changes to the *MMP* have an affect on functionality in the *Shield Mobile* (*Enterprise Law Enforcement Mobile*) and *Crew Mobile* (*Enterprise Fire Mobile*) applications. However, changes to those applications are documented in their respective "Shield Mobile Enhancements"and "Crew Mobile Enhancements"sections.

Note: Only users designated as system administrators can access the *MMP*.

For additional information on designating users as system administrators, refer to the *Enterprise Security Online Help*.

See the following sections for additional information on the enhancements made to the *MMP*:

- "ScenePD Version 8 Now Supported" on page 101
- "Enable Unit Status Selection Check Box" on page 102
- "Log Off Button Updated" on page 103
- "New Agency Management Tab" on page 104

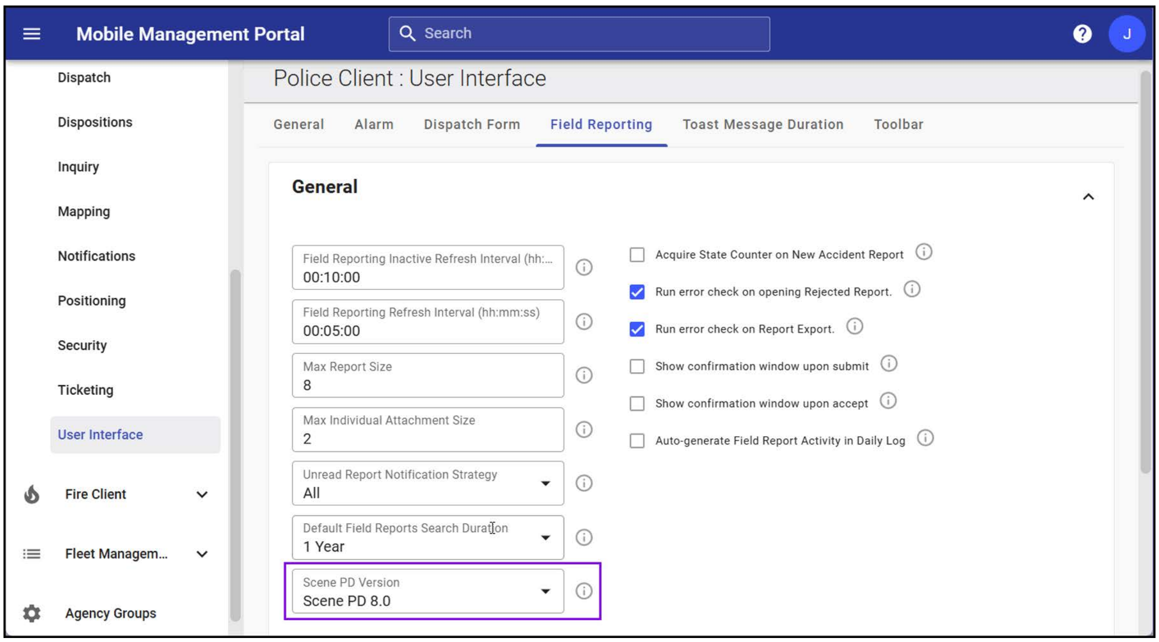
❖ ❖ ❖ ❖ ❖

ScenePD Version 8 Now Supported

ScenePD® is a third-party software created by *Trancite Logic Systems* that has been integrated with the *Mobile* applications, allowing users to create detailed diagrams of accidents or incidents. These diagrams can then be incorporated directly into field reports, when needed. In the *MMP*, agencies have the ability to designate the version of *ScenePD* they have installed and are using with the ***Scene PD Version*** list.

In **2026.3**, version **8.0** of *ScenePD* is now supported for use with the *Mobile* applications and can be selected from the ***Scene PD Version*** list.

Tip: The ***Scene PD Version*** list is accessed by navigating to the *Shield Mobile Client: User Interface* or *Crew Mobile Client: User Interface* page, then selecting the *Field Reporting* tab and expanding the *General* section.



Enable Unit Status Selection Check Box

In **2026.3**, a new ***Enable Unit Status Selection*** check box has been added to the *MMP*. When this check box is selected, the following occurs:

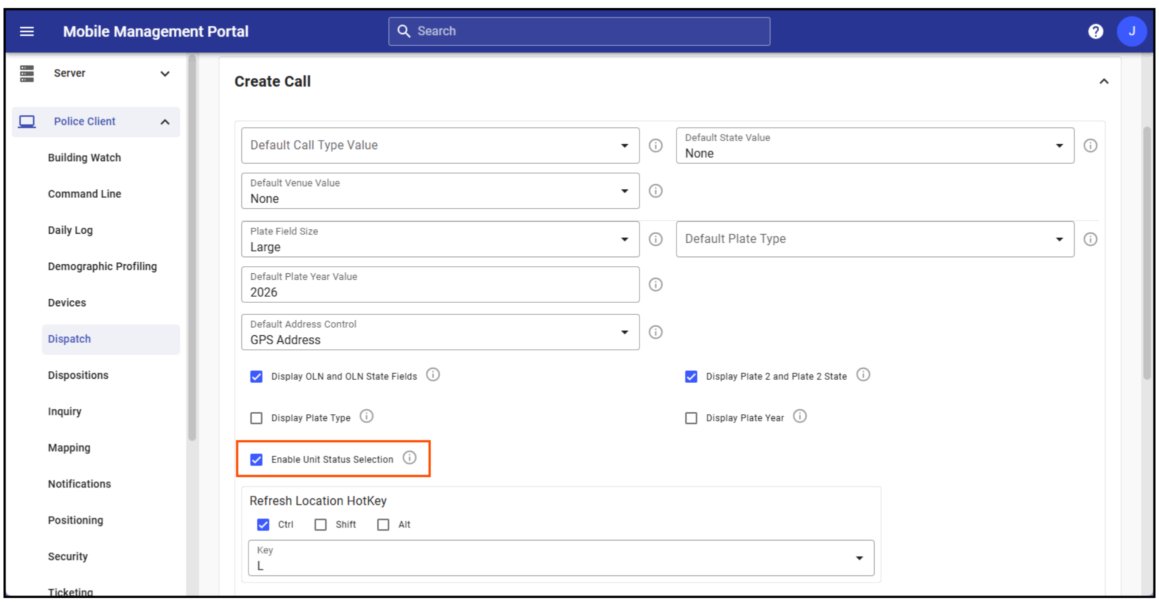
- In the *Mobile* applications, the *Create Call* window's **Send** button is replaced with **On Scene**, **Enroute**, and **Dispatched** buttons.
- In the *Mobility* applications, the *Create Call* widget's **CREATE** button is replaced with **Dispatched**, **Enroute**, and **Arrived** buttons.

For both the *Mobile* and *Mobility* applications, these new buttons allow users to select the status their unit/apparatus should be set to after the new CFS is created.

To access the new ***Enable Unit Status Selection*** check box, navigate to the **Shield Mobile Client** or **Crew Mobile Client** settings on the navigation bar, then select **Dispatch**. After the *Police Client: Dispatch* or *Fire Client: Dispatch* page opens, click the *Call* tab and expand the *Create Call* section. The check box appears within this section.

For additional information on the new **On Scene**, **Enroute**, and **Dispatched** buttons, see the following sections:

- *Shield Mobile*: "Ability to Choose the User's Status When Creating a New CFS" on page 90
- *Crew Mobile:* "Ability to Choose the User's Status When Creating a New CFS" on page 97

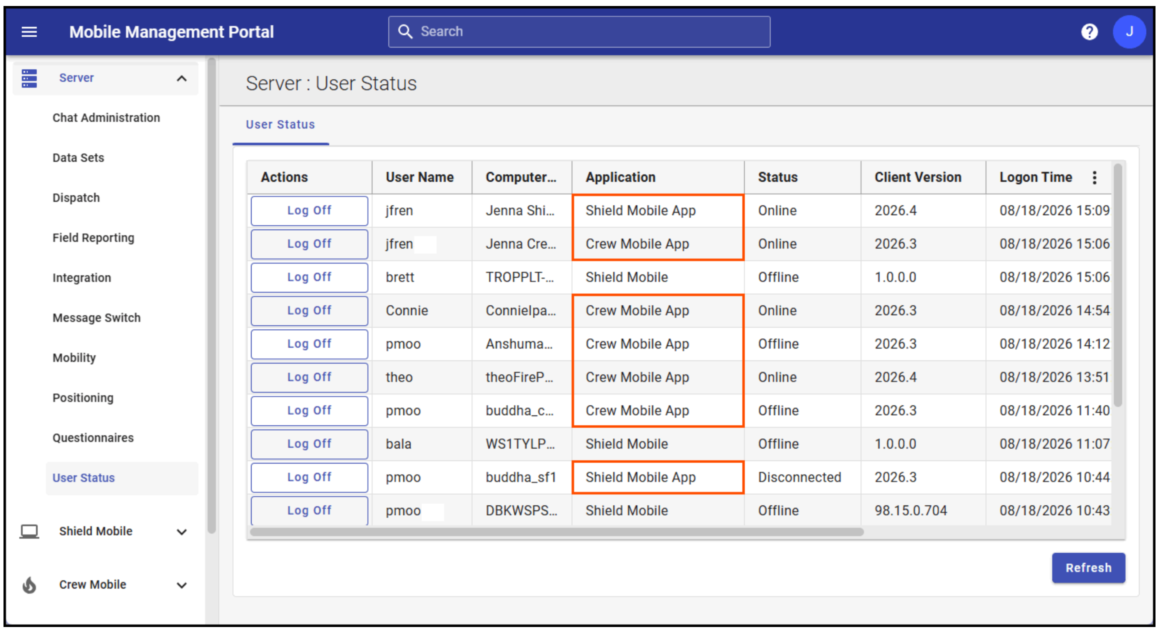


Log Off Button Updated

In a previous release, the ***Actions*** column was added to the grid on the *Server: User Status* page in the MMP. This column contains a **Log Off** button for each grid entry, which agency administrators can click to remotely log users out of the *Crew Mobile* and *Shield Mobile* applications.

In **2026.3**, agency administrators can now use the **Log Off** button to remotely log users out of the *Crew Mobile App* and *Shield Mobile App*. After the **Log Off** button is clicked, users receive a notification message stating an administrator has logged them out and are returned to the first *Login* screen. However, because this does not deactivate their device's registration to the *Mobility Portal*, they can still access the app's functionality by simply logging in again.

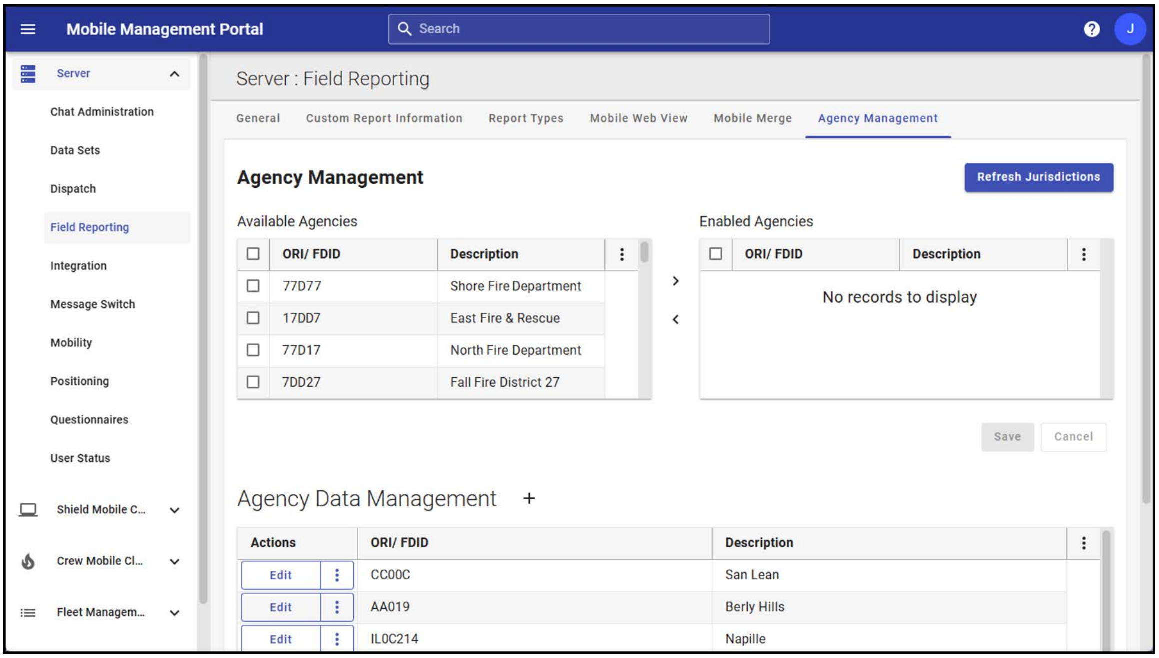
Note: The **Log Off** button only works for entries with a status of Online. If the button is clicked for an entry with a status of Offline, a notification message displays, stating the user is already logged off from the application.



New Agency Management Tab

Previously, agency creation and maintenance related to field reporting for the *Mobile* applications, *Crew Mobile* and *Shield Mobile*, was completed using the *ORI* workspace in the *Mobile Forms Administrator* application.

In **2026.3**, this functionality has been moved from the *Mobile Forms Administrator* application to the *MMP* with the addition of the new *Agency Management* tab on the *Server: Field Reporting* page.



The ***Available Agencies*** and ***Enabled Agencies*** lists on the *Agency Management* tab are used to designate the agencies that display on the *Fleet Management: Update Client Data* page's *Client Field Reporting* tab. These lists are populated using the agencies created *MSP LERMS*, *MSP Fire Records*, or *Enterprise Records*, and can be refreshed at any time using the **Refresh Jurisdictions** button in the upper-right corner.

Select the check boxes corresponding with the agencies from the ***Available Agencies*** list, then click the **> (Left to Right)** button to move them into the ***Enabled Agencies*** list. Alternatively, to remove agencies from the ***Enabled Agencies*** list, select their corresponding check boxes, then click the **< (Right to Left)** button.

When finished, click the **Save** button. A folder that matches the agency's name (ORI/FDID), is created on the *Mobile* server under ...\ProgramData\New World Systems\Aegis Mobile\Data, and typically holds items such as field reporting forms, XML data, etc.

Additionally, when an agency is added to the ***Enabled Agencies*** list, it also displays in the *Agency Data Management* grid below. This grid is mostly used as a reference tool to view all of the agencies that currently have folders on the *Mobile* server, but users can also use it to complete the following actions:

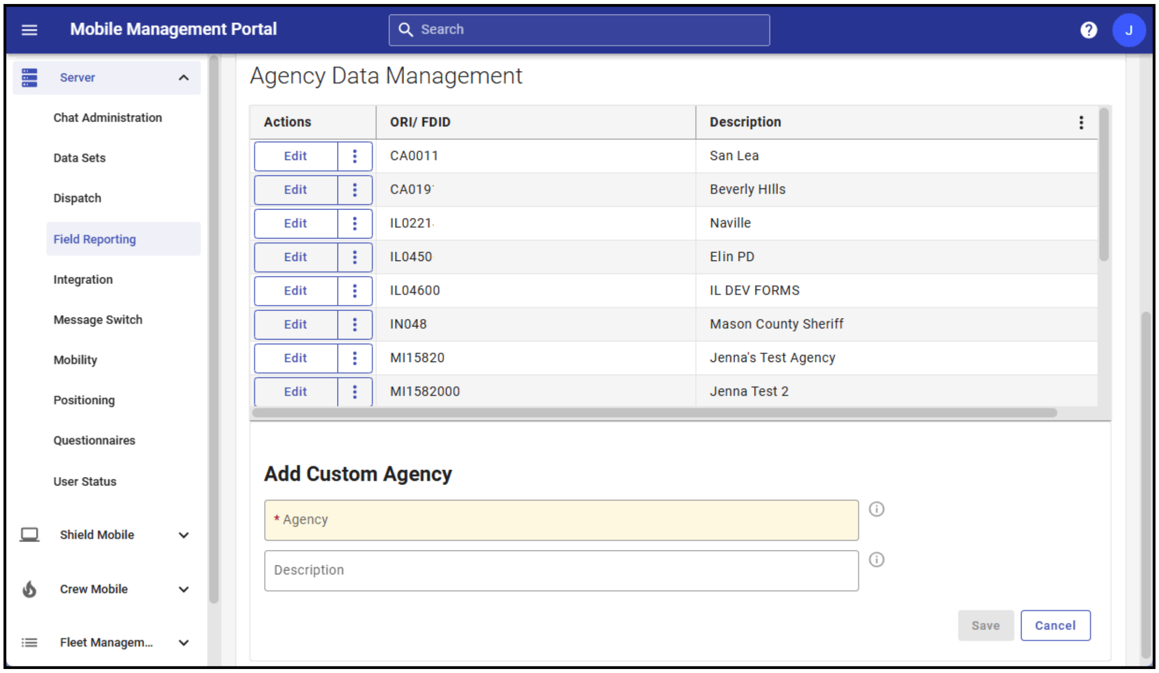
- Create custom agencies: Clicking the **Add** button opens the *New Custom Agency* section, where users can create custom agencies by entering an ORI/FDID code and a description in the corresponding ***Agency*** and ***Description*** text boxes. Note that the ***Agency*** text box is a required field.

  Note: Custom agencies created on the *Agency Management* tab are for the *Mobile* applications only and are not related to the agencies created and maintained in *MSP LERMS*, *MSP Fire Records*, or *Enterprise Records*. Custom agencies are typically used in situations when users need to create and use special field reporting forms that are different from, or not applicable to, an agency's standard field reporting form configuration.

  For additional information on custom agencies, contact a *Tyler Technologies* representative.

- Edit standard and custom agencies: Clicking the **Edit** button in the *Actions* column of the grid opens the *Edit Custom Agency* section, allowing users to edit the agency's description. However, as agency ORIs/FDIDs cannot be edited once created, the ***Agency*** text box in this section is disabled.
- Delete custom agencies: To delete a custom agency, click the ***Options Menu*** ⋮ button in the grid's action column, then select **Delete**. A confirmation message displays, asking the user to confirm whether they want to delete the selected agency ORI/FDID. Click **Delete** to complete the action.

  After a custom agency is deleted, its corresponding folder is removed from the Data folder on the *Mobile* server as well.



Mobile Forms Administrator Enhancements

This section describes the enhancements made in the **2026.3** version of the *Mobile Forms Administrator* application.

See the following sections for additional information on the enhancements made to the *Crew Mobile* application:

- “Mobile Forms Administrator Functionality Moved to the MMP” on page 106

❖ ❖ ❖ ❖ ❖

Mobile Forms Administrator Functionality Moved to the MMP

In the *Mobile Forms Administrator* application, the *ORI* workspace is used by agencies to create and maintain ORI records.

In **2026.3**, this functionality has been moved from the *Mobile Forms Administrator* application to the *MMP*. For additional information, see “New Agency Management Tab” on page 104.

Chapter 3
Enterprise Security

Introduction

This chapter describes the enhancement made in the **2026.3** version of *Enterprise Public Safety Enterprise Security* (*ESS*).

Note: Only users designated as system or agency administrators can access *ESS*.

For additional information on designating users as system or agency administrators, refer to the *Enterprise Security Online Help*.

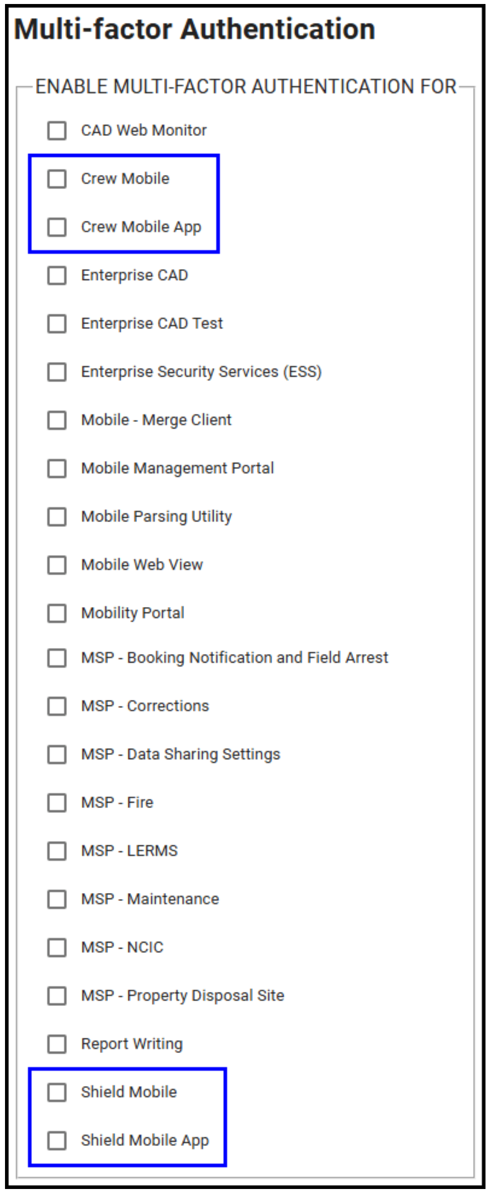
See the following sections for additional information on the enhancement made to *ESS*:

Multiple Check Boxes Renamed

In **2026.3**, the *Enterprise Fire Mobile* and *Enterprise Law Enforcement Mobile* applications were renamed to *Crew Mobile* and *Shield Mobile*. Additionally, in the **2026.2** *Mobility* release, *Fire Field Mobile* and *Law Enforcement Field Mobile* were renamed to *Crew Mobile App* and *Shield Mobile App*.

To reflect the new names of these applications, the following changes have been made within the *Multi-factor Authentication* section of the *Security Policy* page in *ESS*:

- The ***Mobile - Fire*** check box has been renamed to the ***Crew Mobile*** check box.
- The ***Mobility - Fire Field Mobile*** check box has been renamed to the ***Crew Mobile App*** check box.
- The ***Mobile - Police*** check box has been renamed to the ***Shield Mobile*** check box.
- The ***Mobility - Law Enforcement Field Mobile*** check box has been renamed to the ***Shield Mobile App*** check box.



Assign CAD User Mappings Page and Assigned Map Lists Removed

In *ESS*, the *Assign CAD User Mappings* page was used to designate which map users see on the *Enterprise CAD Dispatch Client* and *Enterprise CAD Mapping Client* applications. Users could also do this using the ***Assigned Map*** lists within the *Add Users* and *View/Edit User* pages' *General* sections.

In **2026.3**, the *Assign CAD User Mappings* page and ***Assigned Map*** lists were removed from the *ESS* application because the *GIS* application, which is used in conjunction with *Enterprise CAD*, supports only one map. Thus, there is no need for users to select the map to use from within *ESS*.

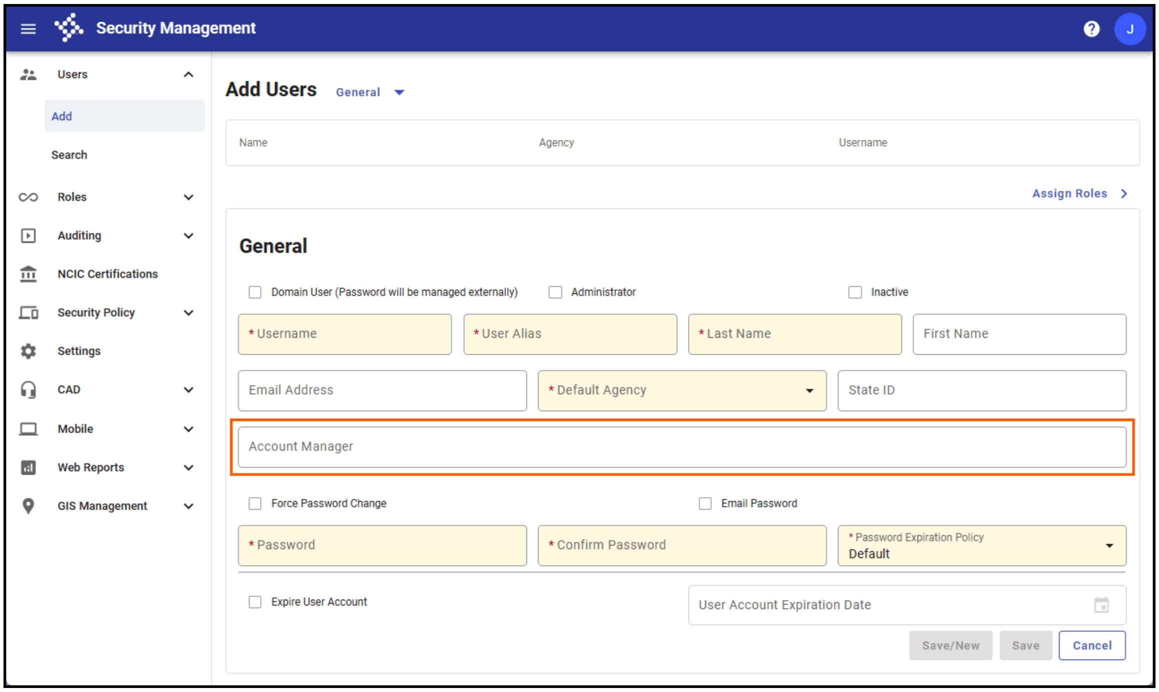
Password Reset Functionality Enhanced

In *ESS*, users designated as system administrators or agency administrators with reset password permissions can reset passwords for other users and administrators. However, in previous releases, these users could not reset their own passwords.

In **2026.3**, the reset password functionality has been updated to allow these designated administrators to reset their own passwords.

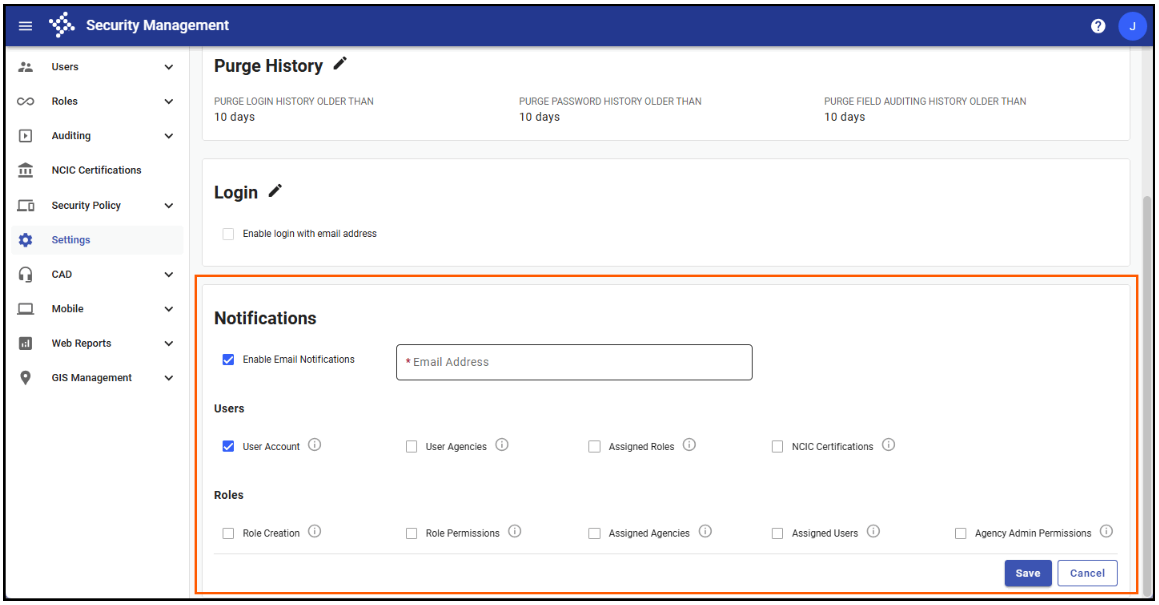
New Account Manager Text Box

In **2026.3**, a new ***Account Manager*** text box has been added to the *General* section of the *Add Users* and *View/Edit User* pages. This text box is primarily used for auditing purposes and to meet CJIS requirements by providing the name or username of the account manager responsible for the user.



New Notifications Section and Fields Added to Settings Page

In **2026.3**, a new *Notifications* section has been added to the *Settings* page in *ESS*, and within it, are fields that allow the user to configure whether email notifications should be sent to a specified email address when certain actions are completed in *ESS*, such as creating a new user or role. This functionality is typically used by the agency's security compliance officer or a designated system administrator to easily track the changes made to users and roles in *ESS*.



To configure email notifications, follow the steps below:

1. Click the *Notification* section's **Edit** button. The fields within the section display, but only the ***Enable Email Notifications*** check box enables.
2. Select the ***Enable Email Notifications*** check box. This enables the other fields within the *Notification* section.
3. Enter the email address of the person who should receive the email notifications using the associated ***Email Address*** text box. Typically, this is the agency's security compliance officer. This field is required.
4. Using the various check boxes, select which actions should trigger an email notification to be sent. Note that at least one check box must be selected.
   - ***User Account*** check box: Sends an email notification when a new user is created or an existing user is edited.
   - ***User Agencies*** check box: Sends an email notification when the *Enterprise CAD* or *Mobile* agencies assigned to a user are changed.
   - ***Assigned Roles*** check box: Sends an email notification when the roles assigned to a user are changed.
   - ***NCIC Certifications*** check box: Sends an email notification when NCIC certifications for a user are changed.

- ***Role Creation*** check box: Sends an email notification when a new role is created.
- ***Role Permissions*** check box: Sends an email notification when the selections from the ***Role Type Permissions*** list are changed.

  Note: This is only applicable for roles where **Application - Enterprise Security** was selected from the ***Role Type*** list.

- ***Assigned Agencies*** check box: Sends an email notification when the agencies assigned to a role are changed.
- ***Assigned Users*** check box: Sends an email notification when the users assigned to a role are changed.
- ***Agency Admin Permissions*** check box: Sends an email notification when the selections from the ***Agency Admin Permissions*** list are changed.

  Note: This is only applicable for roles where **Application - Enterprise Security** was selected from the ***Role Type*** list.

5. When finished, click the **Save** button to retain the changes made or **Cancel** to discard them.

Error Messages for Failed Login Attempts Updated

In the cybersecurity world, user enumeration is a term that describes a security vulnerability where an application reveals information about users within the system to malicious actors. Examples of this could include when a login attempt fails and the application displays an error message stating that the password they entered was incorrect. This tells the malicious actor that the username they entered exists in the system, which they can use to continue trying to log in with various passwords, build a list of potential targets for phishing attacks, etc.

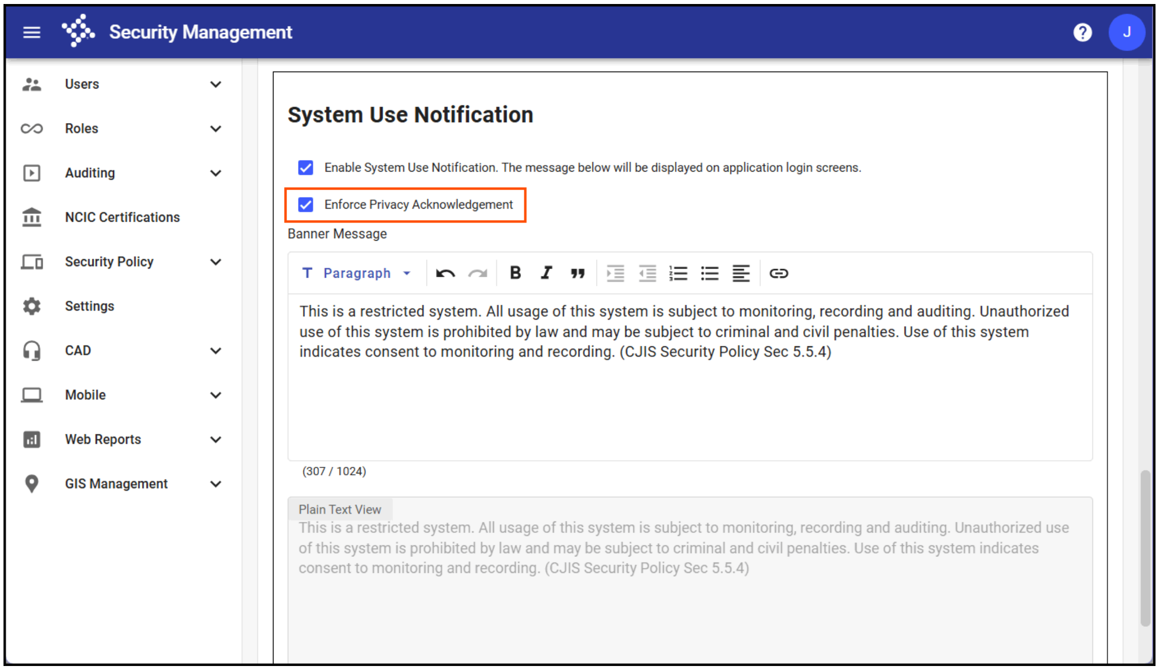
In **2026.3**, as an extra security precaution, the error messages that display for users on the *Login* page when their login attempts fail have been simplified to be more generic. For example, instead of stating that the entered password was incorrect, the error message now states that the username or password was invalid, which does not specify which part of the login information entered was actually incorrect. This new functionality helps protect agencies from potential user enumeration situations.

Tip: Although regular users receive the new simplified error messages, system and agency administrators can still find the true reason behind the failed login attempt under the Reason Code column of the *Search Login History's* grid in *ESS*.

New Enforce Privacy Acknowledgement Check Box

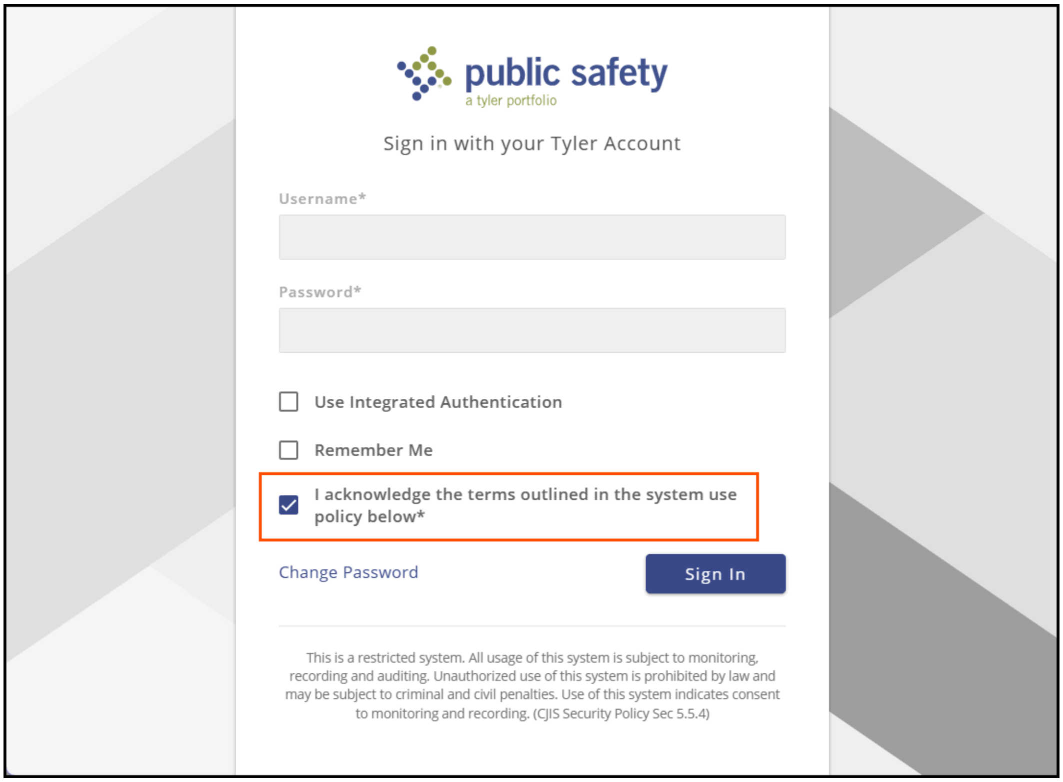
The *System Use Notification* section of the *Security Policy* page in *ESS* is used to create a system message that displays at the bottom of the *Login* page for the *Enterprise Public Safety* applications. For example, a system message may be used by a CJIS-certified agency to display a unique security message that is visible to their users each time they log in to an application. In previous releases, simply proceeding with the login process was the user's way of acknowledging the message.

In **2026.3**, a new ***Enforce Privacy Acknowledgement*** check box has been added to the *System Use Notification* section, allowing agencies to require users to manually acknowledge that they have read the system message before completing the login process.



When the ***Enforce Privacy Acknowledgement*** check box is selected in *ESS*, the following occurs:

- The ***Banner Message*** text editor in the *System Use Notification* section becomes a required field.
- The new ***I acknowledge the terms outlines in the system use policy below**** check box displays on the *Login* page, and must be selected before clicking the **Sign In** button. If the check box is not selected before clicking the button, error messages display, reminding the user that they must acknowledge the system policy as the ***I acknowledge the terms outlines in the system use policy below**** check box is a required field.



New CAD Permissions

The *Assign CAD Role Permissions* page allows administrators to configure whether users with roles created in *ESS* are allowed to use various pieces of functionality in the *Enterprise CAD* applications. For example, creating a new CFS, editing unit statuses, or dispatching units/apparatuses to a CFS.

In **2026.3**, multiple permissions have been added to the *Assign CAD Role Permissions* page. They are detailed in the table below.

Tip: To access the new permissions, navigate to the **CAD** module on the navigation bar, then select **Permissions**. After the *Assign CAD Role Permissions* page opens and the user's role is selected from the corresponding ***Role*** list, all available permissions display. Enter the name of a specific permission (or permission group) in the ***Filter*** text box, or manually scroll through the permissions to locate it.

Permission Group	Permission Name	Summary
Maintain Calls	**Access Call Log Search**	Used to determine whether users with the selected role can use call log search functionality, view and edit entries in the *CFS Call Log* tab, and include audit actions when printing a CFS Detail report. **Tip:** For additional information on the call log functionality mentioned above, see "Dispatch Client Enhancements" on page 80.
Templates and Layout	**Lock Window**	Used to determine whether users with the selected role can lock templates, layouts, and windows using the **Lock Windows** button. **Tip:** For additional information on locking windows in *Enterprise CAD*, see "Added the Ability to Lock Templates" on page 29.

New Mobile Permissions

The *Assign Mobile Role Permissions* page allows administrators to configure whether users with roles created in *ESS* are allowed to use various pieces of functionality in the *Mobile* and *Mobility* applications. For example, creating a new CFS, running a person inquiry/search, or viewing BOLOs.

In **2026.3**, multiple permissions have been added to the *Assign Mobile Role Permissions* page. They are detailed in the table below.

Tip: To access the new permissions, navigate to the **Mobile** module on the navigation bar, then select **Permissions**. After the *Assign Mobile Role Permissions* page opens and the user's role is selected from the corresponding ***Role*** list, the available permissions display. Enter the name of a specific permission (or permission group) in the ***Filter*** text box, or manually scroll through the permissions to locate it.

Permission Group	Permission Name	Summary
Call List/Inquiry	**View Calls by Call Context(s)**	Used to determine whether users with the selected role can see calls on the Call List window that are not part of their assigned agencies, but share the same context. **Tip:** For additional information on viewing calls by context, see: • "Viewing Calls by Context" on page 92. • "Viewing Calls by Context" on page 99
System	**View Advanced Settings**	Used to determine whether the **Advanced Settings** button displays on the *Utilities* window in *Crew Mobile* and *Shield Mobile* for users with the selected role. When the **Advanced Settings** button is clicked, the window that opens contains a setting that allows users to enable verification mode. **Tip:** For additional information on enabling and using verification mode, refer to the *Crew Mobile User Guide* or *Shield Mobile User Guide*.

New GIS Permissions

The *Assign GIS Role Permissions* page allows administrators to configure whether users with roles created in *ESS* are allowed to use various pieces of functionality in the *GIS Management* application. For example, editing general map settings, adding a new venue, or deleting a routing source.

In **2026.3**, multiple permissions and permission groups have been added to the *Assign GIS Role Permissions* page. They are detailed in the table below.

Tip: To access the new permissions, navigate to the **GIS** module on the navigation bar, then select **Permissions**. After the *Assign GIS Role Permissions* page opens and the user's role is selected from the corresponding ***Role*** list, all available permissions display. Enter the name of a specific permission (or permission group) in the ***Filter*** text box, or manually scroll through the permissions to locate it.

Permission Group	Permission Name	Summary
Data Management (New permission group)	**Download**	Used to determine whether users with the selected role can download content from the *Downloads* page.
	Upload	Used to determine whether users with the selected role can upload content on the *Uploads* page.
Distribution	**Deploy Analytics Map Service**	Used to determine whether users with the selected role can deploy analytics map services on the *GIS Service Maintenance* page.
	Deploy GIS Management GeoVerification Services	Used to determine whether users with the selected role can deploy geoverification services on the *GIS Service Maintenance* page.
	Deploy Web CAD Monitor Map Services	Used to determine whether users with the selected role can deploy *Web CAD Monitor* map services on the *GIS Service Maintenance* page.

Permission Group	Permission Name	Summary
GIS Barrier Sources Maintenance (New permission group)	**Add GIS Barrier Source**	Used to determine whether users with the selected role can add new GIS barrier sources on the *GIS Barrier Source Maintenance* page.
	Delete GIS Barrier Source	Used to determine whether users with the selected role can delete GIS barrier sources on the *GIS Barrier Source Maintenance* page.
	Edit GIS Barrier Source	Used to determine whether users with the selected role can edit GIS barrier sources on the *GIS Barrier Source Maintenance* page.
Indoor Mapping Maintenance Permission Group (New permission group)	**Add Indoor Mapping Layer**	Although this permission has been added to *ESS* in the **2026.3** release, its functionality will not be available for use until a future release.
	Delete Indoor Mapping Layer	Although this permission has been added to *ESS* in the **2026.3** release, its functionality will not be available for use until a future release.
	Edit Indoor Mapping Layer	Although this permission has been added to *ESS* in the **2026.3** release, its functionality will not be available for use until a future release.
Type Ahead Maintenance (New permission group)	**Edit Type Ahead Settings**	Used to determine whether users with the selected role can edit type ahead configurations.

Chapter 4
GIS Management

Introduction

This chapter describes enhancements made in the **2026.3** version of *Enterprise GIS Management* application.

Following are the enhancements included in this release. Click the link for more detailed information.

❖ ❖ ❖ ❖ ❖

Administration

GIS administrative-related activities within Tyler Technologies Enterprise Public Safety Software suite uses *Esri ArcGIS Pro* with *Tyler's Enterprise Public Safety* software. The intended audience includes, but is not limited to, GIS personnel, IT, and system administrators. Basic understanding of *ArcGIS Pro* (standard or advanced licensing) is recommended to maintain the *GIS* environment as well as update *GIS* data within an SQL SDE Enterprise geodatabase . Refer to the *GIS Administrator Guide* for more details.

Unsupported GIS Data

In *ArcGIS Pro version 3.2*, *Esri* introduced the following GIS data enhancements:

- 64-bit ObjectID
- BIG Int
- Date Only
- Time Only

The current versions of *Enteprise Public Safety GIS* do not support these *GIS* data options.

If a layer package containing these configurations is uploaded, the layer package job fails.

In **2026.3**, a more intuitive message has been added to the Job Messaging grid, contained on the *Job Activity* page and the *Job History* page, that explains why the job has failed.

GIS Management Application

The *Tyler GIS Management* Web application allows authorized users access to map settings, venue maintenance, common name maintenance, area, and area types. Additionally, users can perform distribution and packaging of updated map files. These tools are necessary for base configuration of *GIS* as well as ongoing maintenance of common names, area types, and areas.

In **2025.2**, the *GIS Management* application has a refreshed appearance. Additionally, many of the buttons have been updated and functionality has moved to enable a smooth workflow. For example, *Cache Sets* has moved out of *System Settings*. Each cache refresh has a new button representing the type of cache refresh and the buttons are dispersed to resides on the toolbar on each page it updates.

For more details, see the following enhancements that were made to the *GIS Management Application*:

- "Map settings" on page 121
  - "Enhanced Global Turn Delays" on page 122
- "Settings" on page 141
  - "Added Configuration Settings for Geocoding Services to ArcGIS Server Toolbox Configuration" on page 141

❖ ❖ ❖ ❖ ❖

Map settings

The **Map Settings** Navigation bar section contains various *GIS* configuration options for the *Enterprise Public Safety Suite*. These options include geoverification, locator, and routing configuration. Refer to the online help within the *GIS Management Web* application for more information about the various configuration options.

See the following:

- "Enhanced Global Turn Delays" on page 122

❖ ❖ ❖ ❖ ❖

Enhanced Global Turn Delays

Global turn delays are time penalties, measured in seconds, that are automatically applied at intersections, when calculating routes. Delays make travel time estimates more realistic by accounting for the delay to make different types of turns in estimated real-world traffic conditions.

In **2026.3**, field names have been changed to reflect how turn delays are defined and calculated.

Minimum Turn Azimuth: 120
Maximum Turn Azimuth: 120

	Local-Local (seconds)	Local-Secondary (seconds)	Secondary-Local (seconds)	Secondary-Secondary (seconds)
Right				
Local or Secondary Cross Road	2	3	2	3
No Cross Road	1	1.5	1	1.5
Left				
Local or Secondary Cross Road	2	10	5	8
No Cross Road	1	5	2.5	4
Straight				
Across Local Road	2	2	2	3
Across Secondary Road	15	15	15	5
Reverse				
Either or No Cross Road	3	15	5	5

These changes help properly set the maximum azimuth value when a network dataset is configured to use global turn delays. This reduces issues with reverse turn penalties.

Requirements

Hierarchy: Configured within all street sources (legal and non-legal)

Travel Time: Configured within all street sources (legal and non-legal)

Types of Turns

- Right
- Left
- Straight
- Reverse

Assumptions

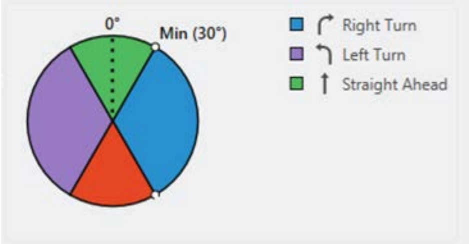
- A left turn across oncoming traffic typically takes longer than a right turn.
- Turns at busy intersections (crossing major roads with stop lights) take more time than turns at simple intersections (stop or yield sign).
- Reverse or U-turns are the highest time case of all turn types.
- Across: Road segment lying opposite the intersection that the turning movement passes across.

Defining Turns

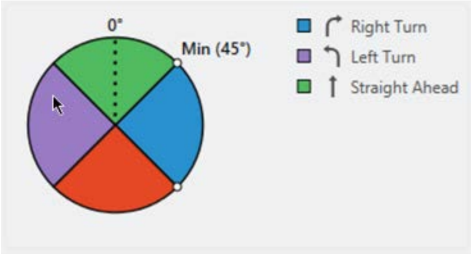
An Azimuth is the horizontal direction expressed as the angular distance between the direction of a fixed point (such as the observer's heading) and the direction of the object. For GIS purposes, it is the turns by angle.

Minimum Turn Azimuth: Determines when a turn is no longer straight and becomes left or right.

The following image demonstrates 30 degrees for a stricter classification:

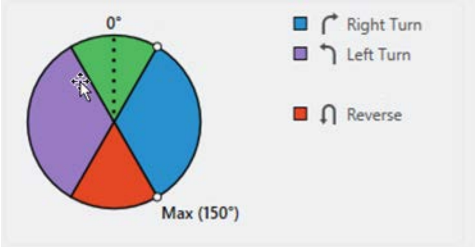


The following image demonstrates 45 degrees for a lenient classification:

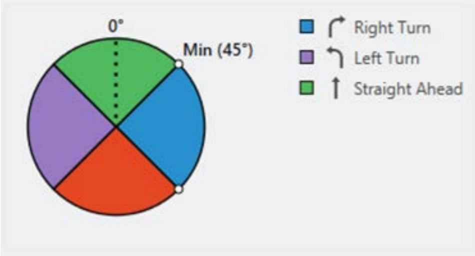


Maximum Turn Azimuth: Determines when a turn is no longer reverse and becomes left or right.

The following image demonstrates 150 degrees for stricter classification:



The following image demonstrates 135 degrees for lenient classification:



Turns by Hierarchy: Defines turns based on straight, left, right, or reverse from one hierarchy value to another, such as:

- Across another hierarchy value

- Across nothing
- Hierarchy value = 1 (Primary)
  - Never intersect another hierarchy value
  - Access and exit of primary street segments are handled via off or on ramps and travel time on the ramp; not global turn delays
  - Overpass and underpass broken as Intersections. See Planar Elevation section.
  - No Turn cost for traveling straight from primary.

The following are satellite images showing examples of the different turns.

Right Turns across a road:

- Local to local at a 4-way stop sign or yield sign

- Local to secondary at a stop sign

- Secondary to local across oncoming traffic

- Secondary to secondary at a traffic light

Right turns across no road:

- Local to local at a stop sign or yield sign

- Local to secondary at a stop sign

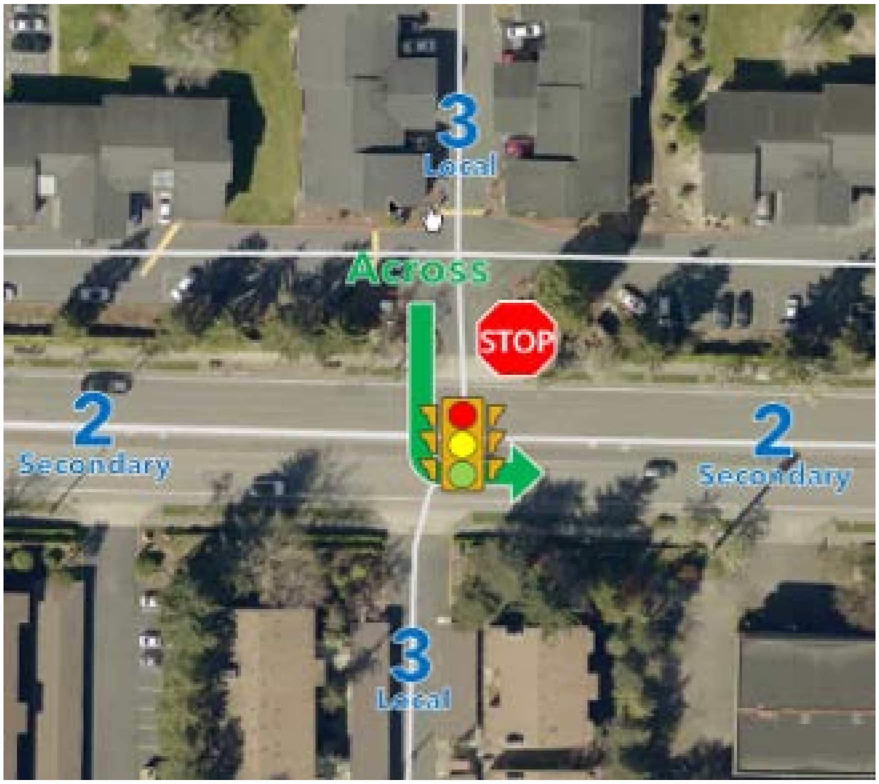
- Secondary to local is an uncommon scenario. No image provided because of this.

- Secondary to secondary at a stop sign

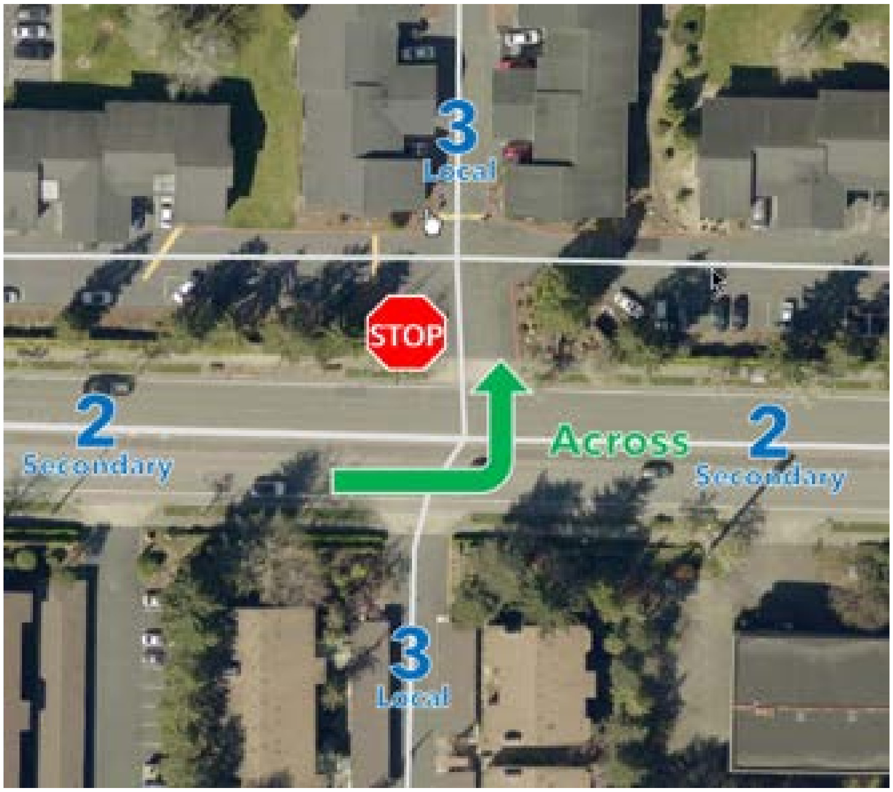
Left Turns across a road:

- Local to local at a four-way stop or yield sign

- Local to secondary at a stop sign or traffic light



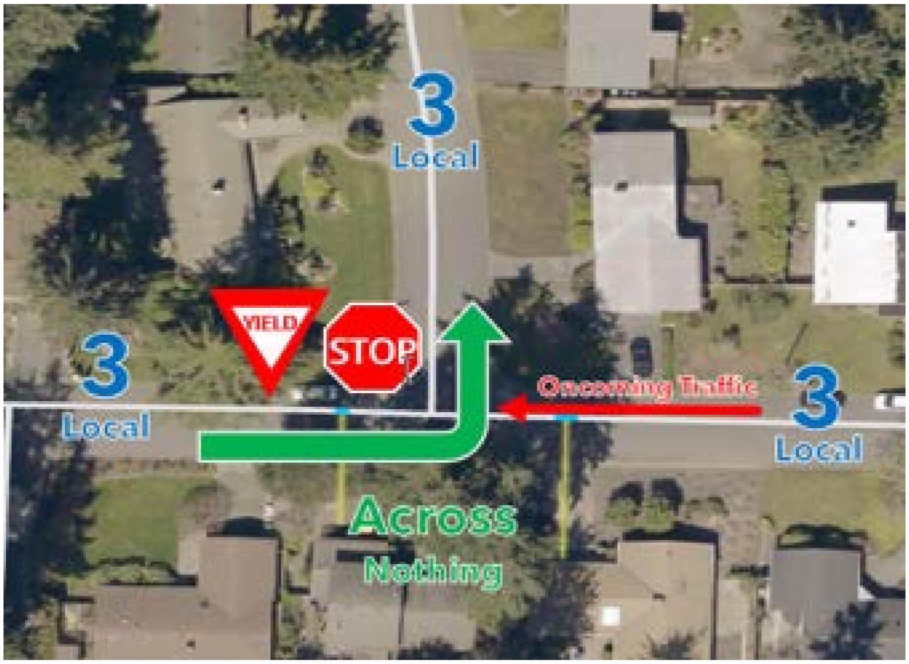
- Secondary to local across oncoming traffic



- Secondary to secondary at a traffic light

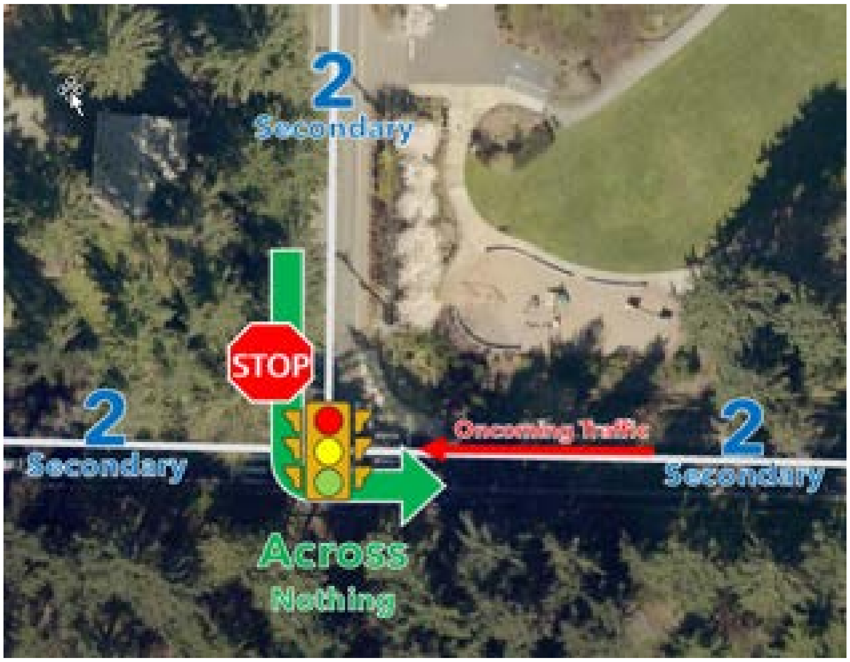
Left turns across no road:

- Local to local at a stop sign or yield sign



- Local to secondary at a stop sign or yield sign

- Secondary to local is an uncommon scenario. No image provided because of this.
- Secondary to secondary at a stop sign or traffic light



Straight across local:

- Local to local at a 4-way stop sign or yield sign

- Local to secondary at all-way stop sign

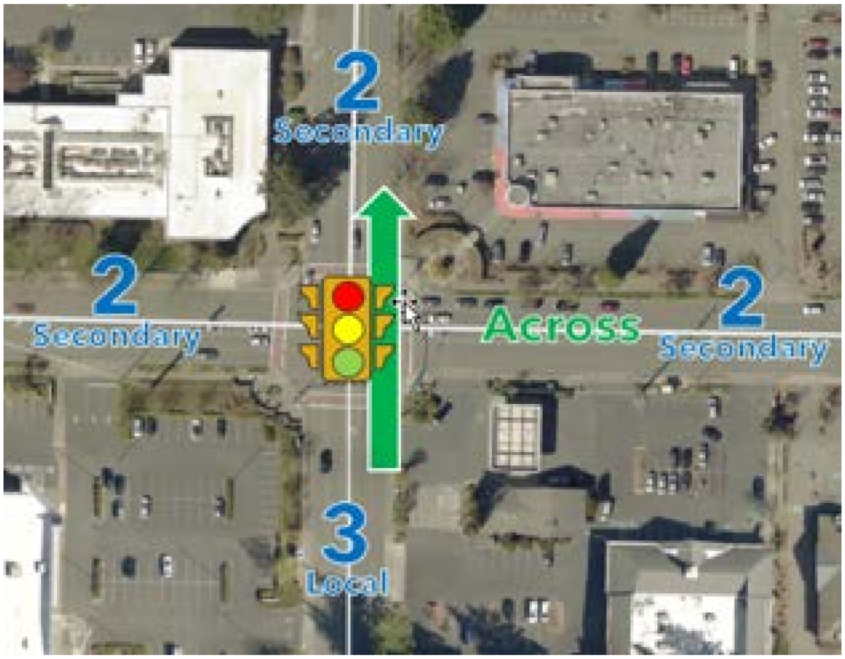
- Secondary to local at all-way stop sign

- Secondary to secondary at traffic light

Straight across secondary:

- Local to local at a stop sign or traffic light

- Local to secondary at a traffic light



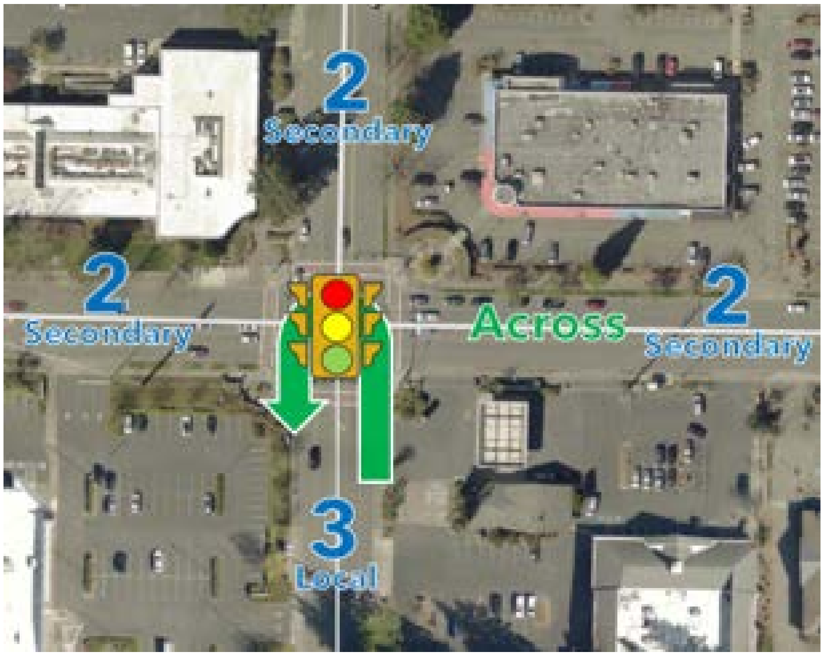
- Secondary to local at a traffic light

- Secondary to secondary at a traffic light

Reverse across local, secondary, or no street:

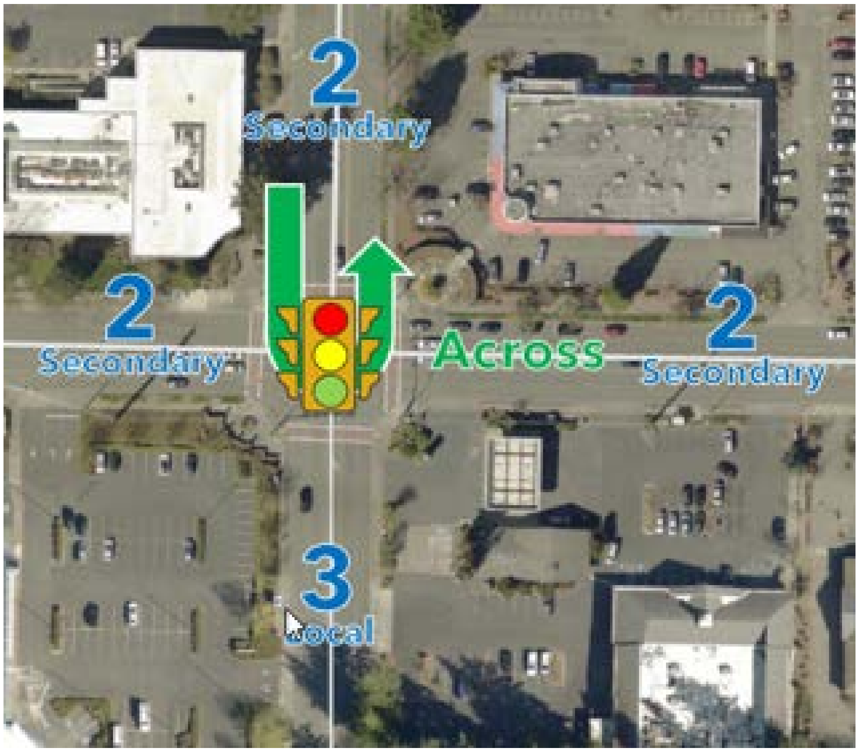
- Local to local across local

- Local to local across no road (No image provided)
- Local to secondary across secondary

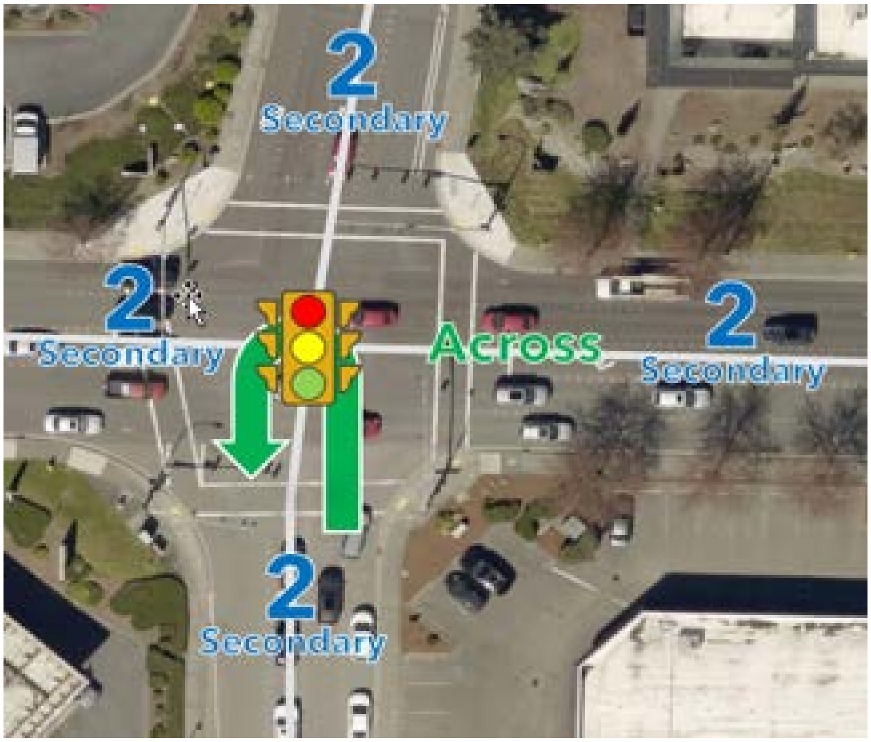


- Local to secondary across no road (No image provided)

- Secondary to local across secondary



- Secondary to secondary across secondary



- Median U-Turn (Michigan Left):Designed to eliminate direct left turns at main intersections. Left turns are accomplished by using designated median openings.

In the following example, the left turn at the light in the first image is prohibited.

Instead, driver's should use the median u-turn demonstrated in the second image.

Non-legal Streets and Global Turn Delays

If the hierarchy and travel time is configured for all routing street sources and one or more of the street sources is non legal streets, such as driveways, a turn feature class (TYL_DRIVEWAY_PASSTHROUGH_TURNS) is automatically created during a *GIS* packaging job.

The TYL_DRIVEWAY_PASSTHROUGH_TURNS is populated with a turn feature at every straight turn in which a legal street crosses a non legal street.

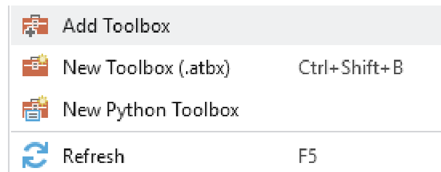
Each turn feature is set with an impedance cost of 0 to prevent a straight turn cost being added at every Legal to non-legal, straight turn.

Overriding Turns

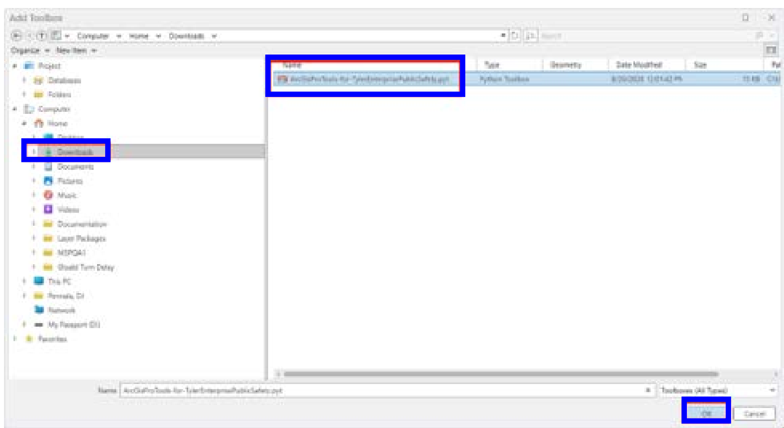
To override TYL_DRIVEWAY_PASSTHROUGH_TURNS:

If needed, the TYL_DRIVEWAY_PASSTHROUGH_TURNS can be overridden to prevent a *GIS* package from creating and populating a new turn feature class each time.

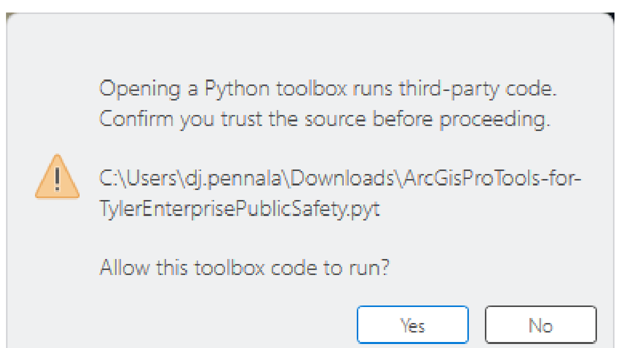
1. Within the *GIS Management* application, click **Data Management** on the Navigation bar.
2. Choose **Downloads** from the sub-menu.
3. Click to expand the *Enterprise Public Safety ArcGIS Pro Toolbox*.
4. Click the **ArcGISPro Tools for TylerEnterprisePublicSafety** link to download the ArcGISProTools-for-TylerEnterprisePublicSafety.pyt file.
5. Open the *Tyler Enterprise Public Safety ArcGIS Pro* project in *ArcGIS Pro*.
6. Within the *Catalog* view, right-click **Toolboxes**, and select **Add Toolbox** from the menu. The *Add Toolbox* window displays.



7. Browse to and select the folder that contains the ArcGISProTools-for-TylerEnterprisePublicSafety.pyt file on the Toolbox Directory pane.



8. Select the ArcGISProTools-for-TylerEnterprisePublicSafety.pyt file from the contents pane.
9. Click **OK**. A warning displays.



10. Click **Yes**. A new toolbox called ArcGISProTools-for-TylerEnterprisePublicSafety displays within the *ArcGIS Pro Toolboxes* list.
11. Expand the toolbox, and double-click **Create Routing Passthrough Turns Feature Class** or right-click it and choose **Open** from the menu. The *Geoprocessing* dialog opens.

12. Within the *Create Routing Passthrough Turns Feature Class Geoprocessing* tool parameters enter the following:
    - ***Target Geodatabase***: For connected systems, browse to the *Enterprise Public safety Enterprise Geodatabase*. For disconnected systems, browse to the default file geodatabase within the *Enterprise Public Safety ArcGIS Pro* project.
    - ***Target Feature Dataset***: After the ***Target Geodatabase*** has been selected, the T***arget Feature Dataset*** automatically populates with the feature dataset named **NetworkDataSet_data**. This is the appropriate location to create the TYL_DRIVEWAY_PASSTHROUGH_TURNS.
13. Click **Run**.
14. When the tool completes, browse to the target geodatabase, and expand the **NetworkDataSet_Data** to see the TYL_DRIVEWAY_PASSTHROUGH_TURNS.

For connected systems that created the new turns feature class directly within the *Tyler Enterprise Public Safety* geodatabase, the next time a *GIS* Packaging job is run the creation of the TYL_DRIVEWAY_PASSTHROUGH_TURNS isskipped.

For disconnected systems, the TYL_DRIVEWAY_PASSTHROUGH_TURNS needs to be packaged and uploaded as a layer package prior to the next *GIS* packaging job to achieve the override.

Settings

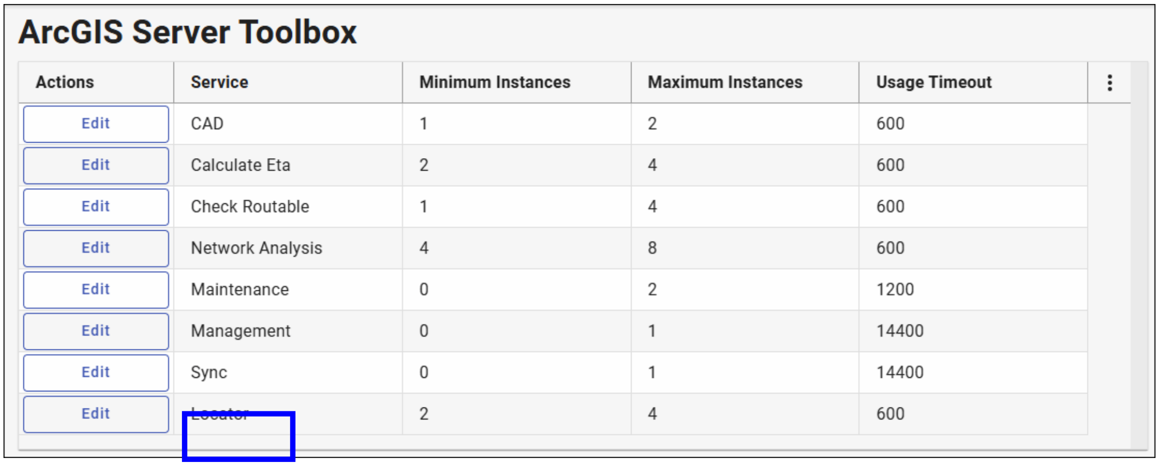
Settings contains the ability to clear and to refresh the cache. Additionally, users can deploy management services for geoverification.

Added Configuration Settings for Geocoding Services to ArcGIS Server Toolbox Configuration

Geocoding services are published from *Esri* Locator configured within *Tyler Enterprise Public Safety*. They are published as part of a *GIS* packaging job in which *GIS* data that is used within the geoverification process has been updated.

Applications performing geoverification remotely use the geocoding services. Examples are the *GIS Management Application*'s *Common Name Maintenance*, *Enterprise CAD*'s ASAP Interface, and *Enterprise Mobile*'s *Create Call* workflow.

In **2026.3**, the *ArcGIS Server Toolbox* configuration, found under *Settings* in the *GIS Management* application, now includes a Locator option in the Service column.


ArcGIS Server Toolbox

Actions	Service	Minimum Instances	Maximum Instances	Usage Timeout
Edit	CAD	1	2	600
Edit	Calculate Eta	2	4	600
Edit	Check Routable	1	4	600
Edit	Network Analysis	4	8	600
Edit	Maintenance	0	2	1200
Edit	Management	0	1	14400
Edit	Sync	0	1	14400
Edit	Locator	2	4	600

Click the **Edit** button to open the configuration options for ***Min*** and ***Max*** instances, and ***Usage Timeout***.

If experiencing a slow remote geoverification processes, use a ***Min*** of **2** and a ***Max*** of **4** as the proper starting configuration for testing.

Chapter 5
Enterprise Records

Introduction

This chapter describes enhancements made to the **2026.3** version of *Enterprise Records Management System*.

The following are enhancements included in this release. Click the links for more detailed information.

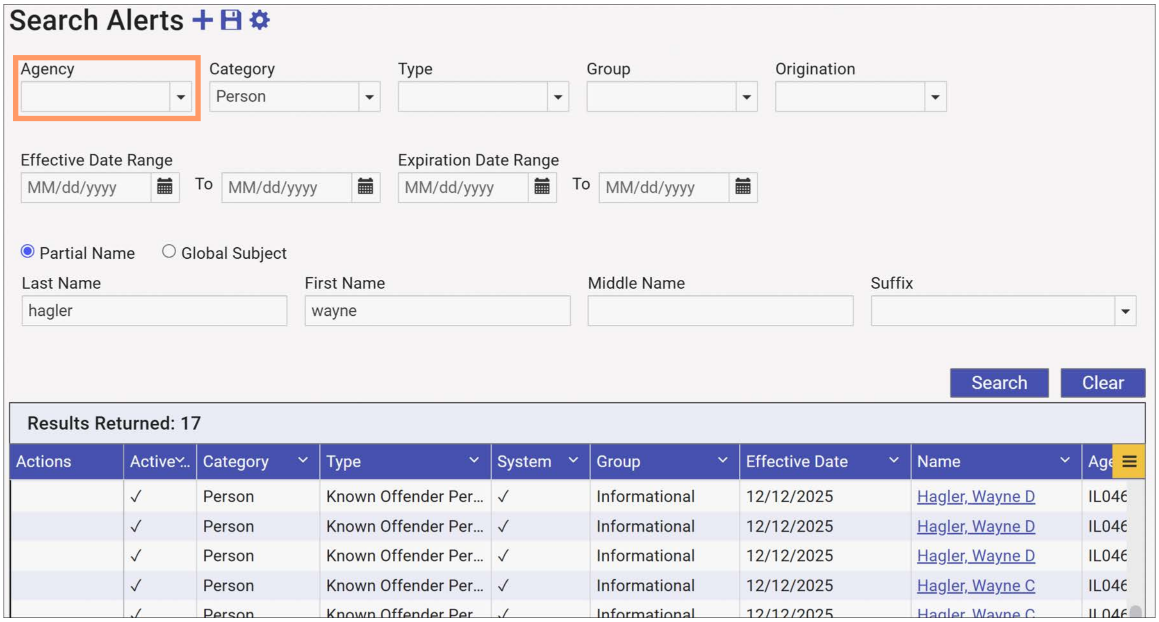
v v v v v

Alerts

Alerts are applied to subjects, locations, and vehicles in any application and displayed in all applications within the suite for which an agency is licensed, alerting agency and station personnel to situations such as prior offenses for a subject, chemical hazards at a location, or stolen vehicles. Global alert types come in two forms: system and agency-defined.

Search Alerts Agency is now Optional

The *Search Alerts* page allows users to search for alerts using user-defined criteria, including agency, category, type, group, organization, effective date range, and expiration date range. In **2026.3**, the page has been enhanced by making the ***Agency*** field optional. This allows users to see alerts across all agencies they have permission to without having to perform multiple searches.



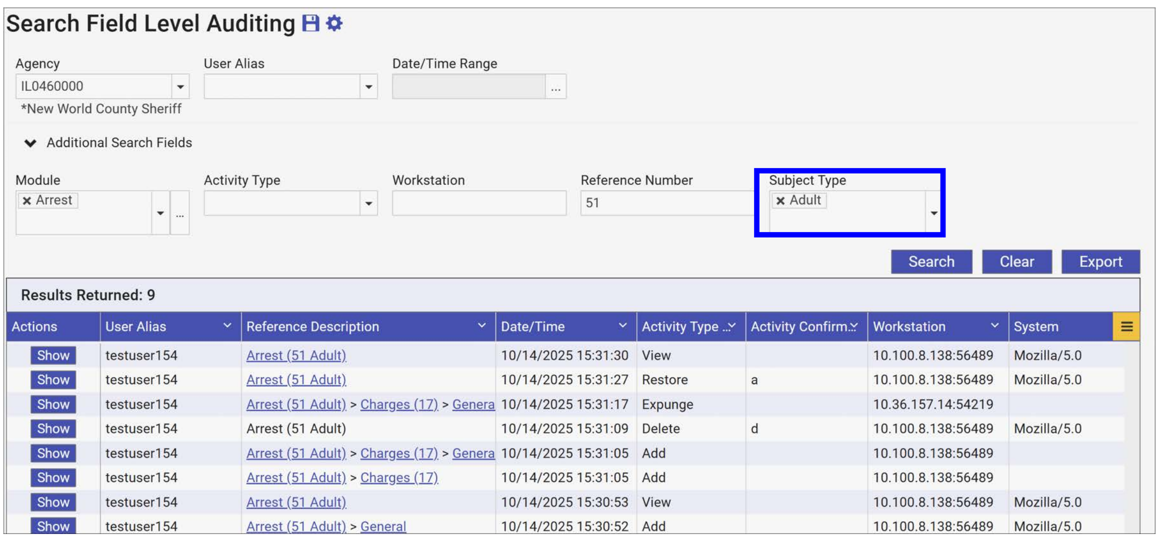
Arrests

The *Arrests* module allows authorized users to enter and maintain information related to the arrests of global subjects. Such arrests may result from active case investigations, occur after an officer serves a warrant or civil paper, or occur when a crime is observed in progress. Arrests cross multiple jurisdictions and generate global person and location records for the arrestee and arrest location.

Ensure that Adult and Juvenile Arrest Numbers are Unique

In **2026.3**, enhancements were made so that arrest subject types of adult or juvenile can be differentiated throughout *Enterprise Records.*

The *Search Field Level Auditing* page allows authorized users to locate records that have been added, edited, deleted, or viewed by the user or other authorized users. The ***Subject Type*** field was added to this page and can be used to search for adult or juvenile arrest records.



In *Enterprise Print Designer* a ***Subject Type*** field was added for Adult and Juvenile arrestees.

In the *Expungement Tool*, the ***Subject Type*** field was added for arrests.

Associated Records

Associated Records is a standard section throughout several *Enterprise Records* modules that displays agency records linked from one record to another. For example, an incident is automatically associated with a case when a case is created from an incident. Additionally, records can be manually associated. For example, a case can manually be associated with another.

See the following:

- "Ability to Edit Manually Associated Records" on page 147
- "Associated Records Section Includes External Record Link" on page 148

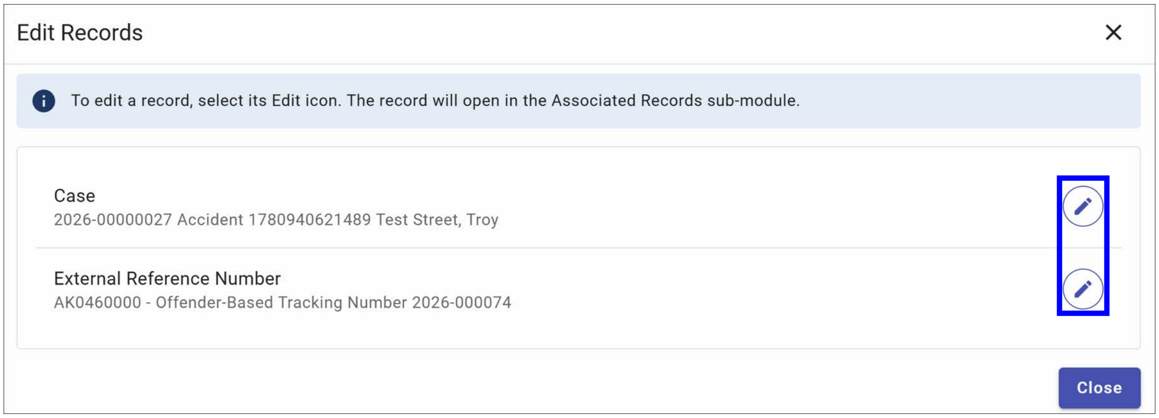
Ability to Edit Manually Associated Records

In **2026.3**, the ability to edit manually associated records has been added. This solves this issue of having to unlink a record and create a new link.

To edit a manually associated record:

1. Click the **Edit** button in an *Associated Records* section. The *Edit Records* dialog displays.

2. Click the **Edit** button associated with the external record. The record displays in edit mode.



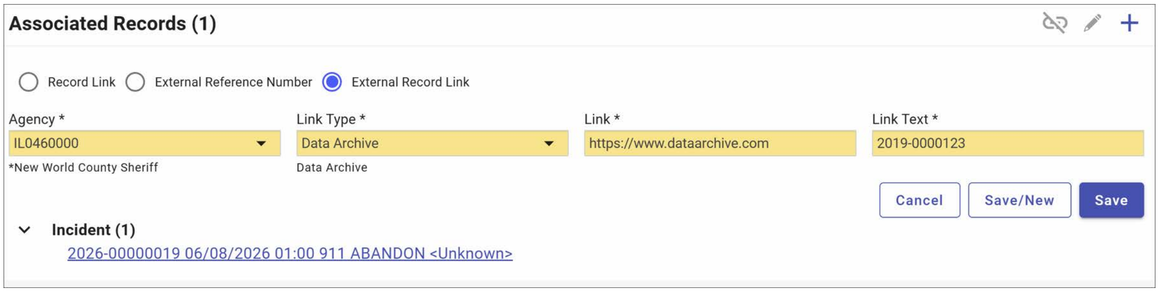
3. Make the changes and click the **Save** button.

Associated Records Section Includes External Record Link

In **2026.3**, the *Associated Records* section in the *Cases* and *Incidents* modules were enhanced to allow external record links to be associated with a case. This feature can be used to add a direct hyperlink to another Tyler or 3rd party record that is associated with the Case.

To associate an external record link:

1. Select the ***External Record Link*** button. The entry fields enable.



2. Select the ***Agency***.
3. Select the ***Link Type***. This is the specific site, type, or category for the link that is displayed in the formatted link.
4. Enter a valid URL that contains http:// or https:// in the ***Link*** field. For example, http://data-archive.com.
5. Enter the number or description of the record to show in the link ***Link Text***.
6. Click the **Save** *button.* The record is saved as an external record link. Clicking the link launches the record directly.

Cases

The *Cases* module allows authorized users to enter and maintain case and case assignment records.

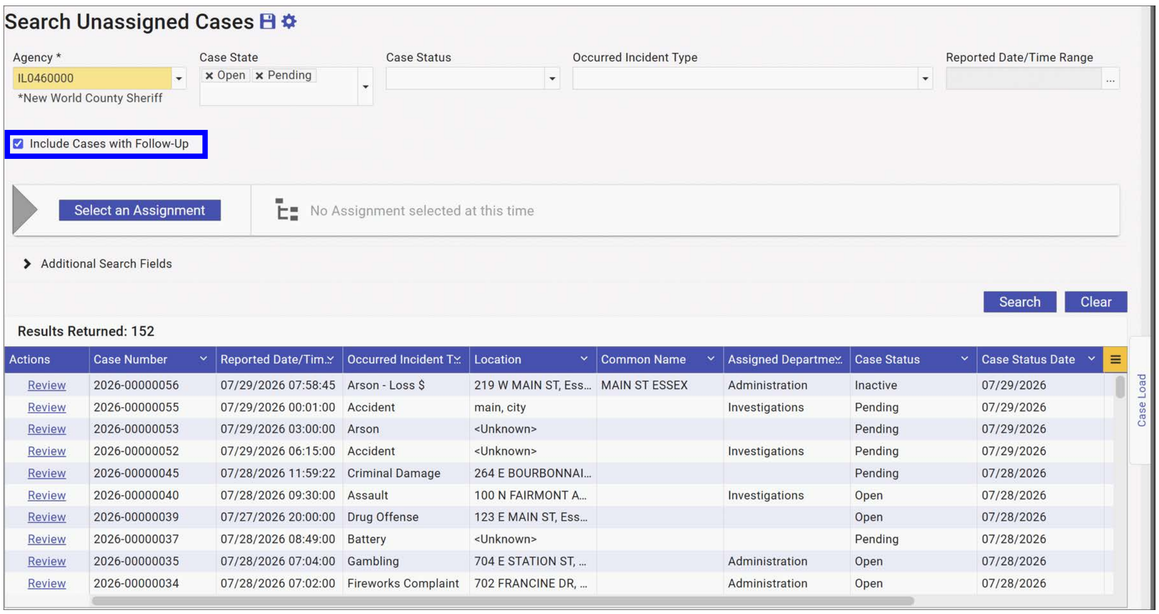
Ethnic Origin and Age Range Added to Create Unknown Subject

When a subject is being added to a case, the name is not always known. Therefore, the ability to add an Unknown/Partially Known subject is available. In **2026.3**, the *Create Unknown Subject* dialog has been enhanced with the addition of the ***Ethnic Origin*** and ***Age Range*** fields.

Search Unassigned Cases Enhanced

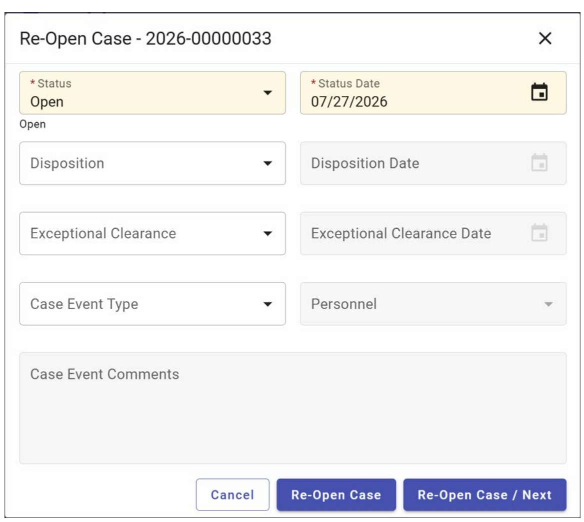
In **2026.3**, the *Search Unassigned Cases* page has been enhanced to optionally expand the scope from new cases to include cases with follow-up reports, which includes closed cases. This page was originally designed to search for unassigned cases in an Open status.

As part of this, the ***Include Cases with Follow-Up*** check box has been added to the *Search Unassigned Cases* page. Selecting this check box includes all cases that have had a follow-up report created for them in *Report Writing*. The problem this solves is that when a case was closed in the past, if a follow-up report was written by an officer, the report would not be noticed as something that needed to be reviewed.



Actions	Case Number	Reported Date/Tim…	Occurred Incident T…	Location	Common Name	Assigned Departme…	Case Status	Case Status Date
Review	2026-00000056	07/29/2026 07:58:45	Arson - Loss $	219 W MAIN ST, Ess…	MAIN ST ESSEX	Administration	Inactive	07/29/2026
Review	2026-00000055	07/29/2026 00:01:00	Accident	main, city		Investigations	Pending	07/29/2026
Review	2026-00000053	07/29/2026 03:00:00	Arson	<Unknown>			Pending	07/29/2026
Review	2026-00000052	07/29/2026 06:15:00	Accident	<Unknown>		Investigations	Pending	07/29/2026
Review	2026-00000045	07/28/2026 11:59:22	Criminal Damage	264 E BOURBONNAI…			Pending	07/28/2026
Review	2026-00000040	07/28/2026 09:30:00	Assault	100 N FAIRMONT A…		Investigations	Open	07/28/2026
Review	2026-00000039	07/27/2026 20:00:00	Drug Offense	123 E MAIN ST, Ess…			Open	07/28/2026
Review	2026-00000037	07/28/2026 08:49:00	Battery	<Unknown>			Pending	07/28/2026
Review	2026-00000035	07/28/2026 07:04:00	Gambling	704 E STATION ST, …		Administration	Open	07/28/2026
Review	2026-00000034	07/28/2026 07:02:00	Fireworks Complaint	702 FRANCINE DR, …		Administration	Open	07/28/2026

As part of this enhancement, the **RE-OPEN** toolbar button has been added for closed cases. When clicked, the *Re-Open Case* dialog displays. Once the information is entered, the user can click the **Re-Open Case** or **Re-Open Case / Next** button to proceed. This allows a user to continue reviewing cases or remain on the case that was just re-opened. Also, for a closed case, assigning personnel to it causes the *Re-Open Case* dialog to appear.

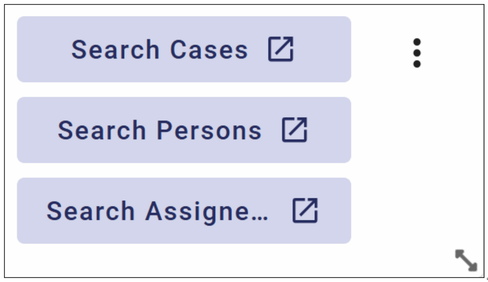


Dashboards

A dashboard is a user interface that presents information clearly and concisely, making it easy to read and comprehend. Dashboards are user-specific and can only be maintained by the user who is logged in. The dashboards on the home page of *Enterprise Records* are easily configurable and provide users with instant information upon login. If no boards have been configured, the System Board is the default, which shows the Introduction tile.

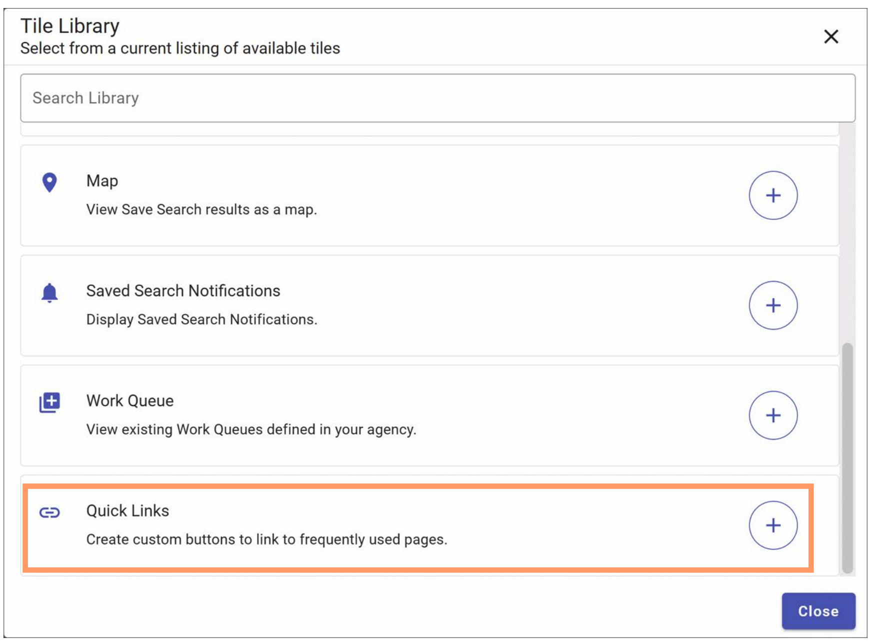
Quick Links Dashboard Tile Added

Users often need to access several links or areas quickly in the application. For example, admins might need to access *Enterprise Security*. Users may also have different areas in the application they want quick navigation to, which should be front and center. In **2026.3**, the *Quick Links* tile was added to the dashboard tile library.



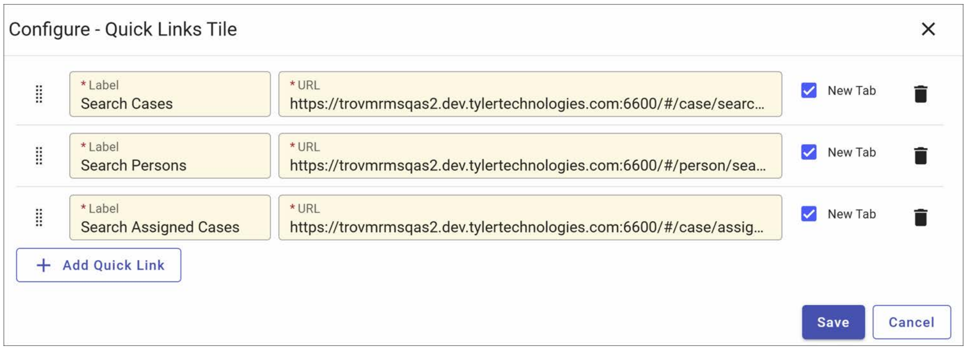
To add the *Quick Links* tile:

1. From an existing dashboard, click the **Add Tiles** button. The *Tile Library* dialog displays.
2. Click the **Add Quick Links** button. The *Configure - Quick Links Tile* dialog displays.



3. Enter a ***Label*** and ***URL*** for each link to be included. The ***New Tab*** check box is selected by default.

4. Click the **Add Quick Link** button to add additional links.



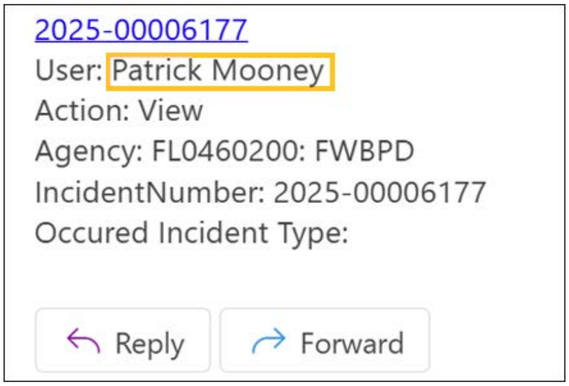
5. Click **Save**.

Email Notifications

Users can subscribe to a record such as a case, a global subject, or a vehicle and be notified when the record has activity. When subscribed to a record, whenever another user opens, edits, or copies that record, a notification is automatically sent to inform the subscribed user of the activity. The notification can be delivered via the notification button on the Main Toolbar or via email.

Email now Includes who Triggered the Notification

In **2026.3**, the email that is sent when triggered by another person opening, editing, or copying a record now includes that user; this matches the information available in the in-app notification. Seeing the person who triggered the notification will allow the subscribe to know who to follow up with if they want to know what the record was viewed or modified. Previously it included the user who subscribed to the email notification.



Email Servers

Enterprise Records contains two locations for setting up email server communications. System Settings is used as the default, but in Agency Settings, individual agencies can be set up and this overrides the system settings.

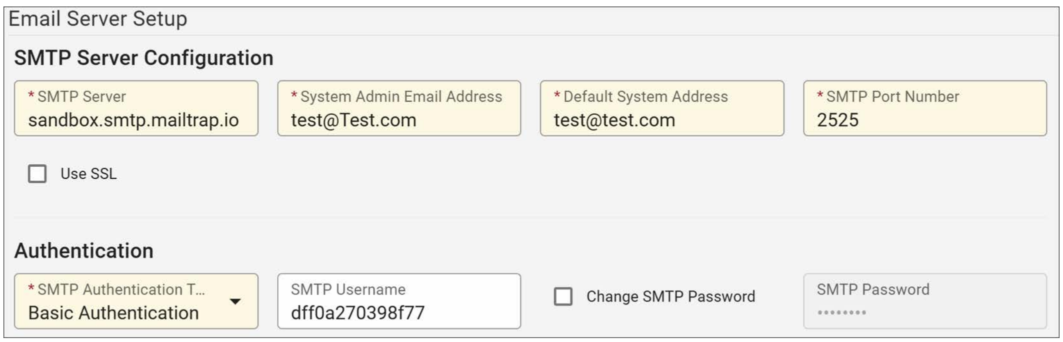
Email Server Setup Page Enhanced

In **2026.3**, the *Email Server Setup* page has been enhanced with a more modern look and a new authentication fields. This applies to both System Settings page and the Agency Settings - Communication page.

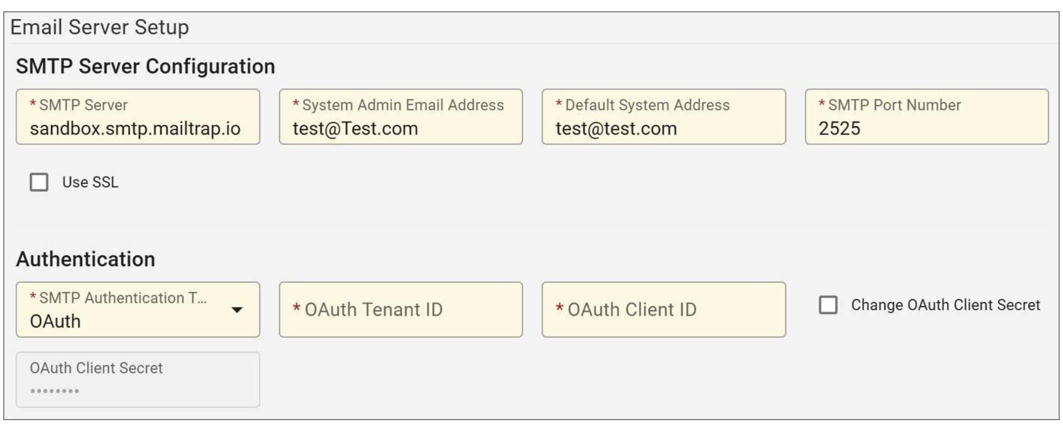
The fields in the *SMTP Server Configuration* section remain the same as previous. The *Authentication* section is new as changes were made to support end of life of SMTP Basic Authentication for Microsoft Exchange Online.

In the ***SMTP Authentication Type***, field, select **Basic Authentication** *or* ***OAuth***.

- If **Basic Authentication** is selected, the user needs to enter the ***SMTP Username***. If the password needs to be changed, select the ***Change SMTP Password*** check box, which enables the ***SMTP Password*** field.



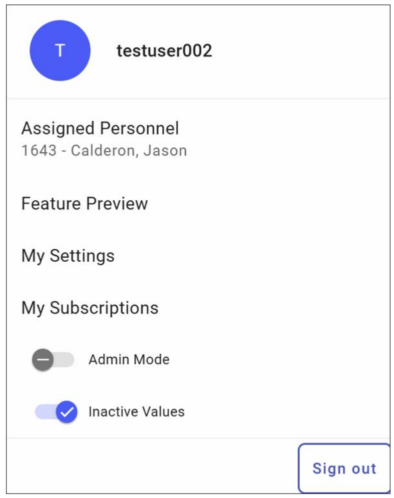
- If **OAuth** is selected, the ***OAUTH Tenant ID*** and ***OAuth Client ID*** fields need to be entered. If the secret needs to be changed, select the ***Change OAuth Client Secret*** check box, which enables the ***OAuth Client Secret*** field.



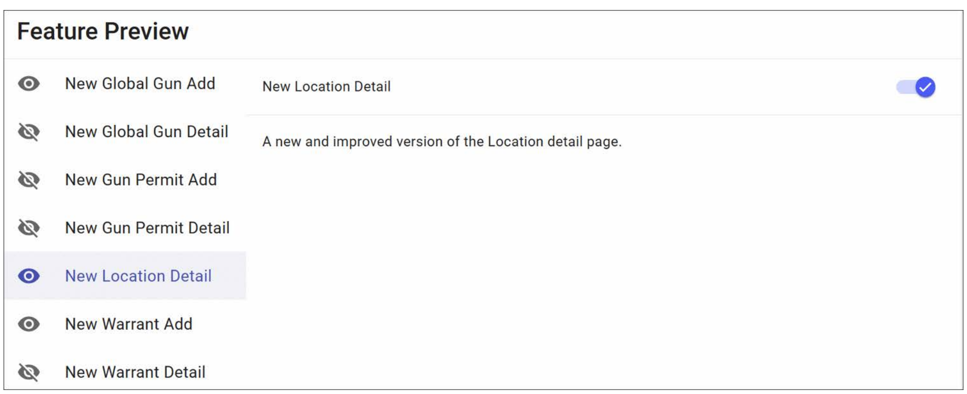
Feature Preview

In **2026.3**, a **Feature Preview** option was added. As new versions of pages in *Enterprise Records* are rolled out, the **Feature Preview** allows users to look at the new pages before they become part of the base software. For example, Global Guns has been going through an extensive update. Clients can see these updates and provide feedback before the pages are made permanent.

As part of this enhancement, **Feature Preview**, a system permission has been added. This must be enabled for users to see the **Feature Preview** option in the **Profile Menu**.



In the *Feature Preview* page, select a feature and click the slider bar to enable disable the preview. Then, navigate to the page to view the new version.



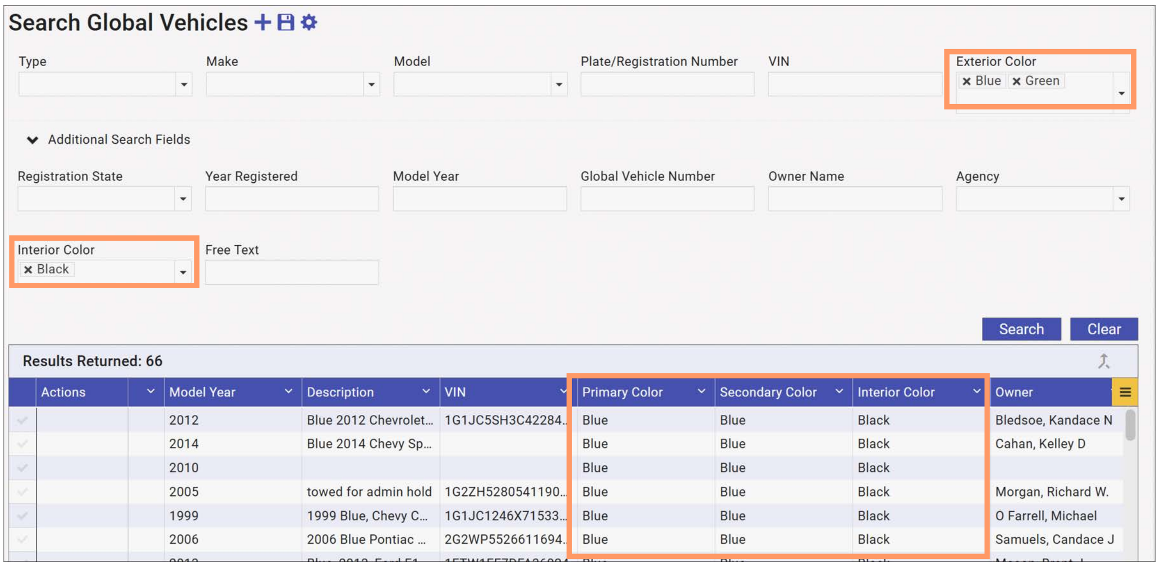
Global Vehicles

Global Vehicles are vehicle records that may be entered and searched for across modules and applications in Enterprise Records. Global vehicle types include passenger cars, motorcycles, buses, commercial trucks, bicycles, jet skis, boats, airplanes, helicopters, and snowmobiles.

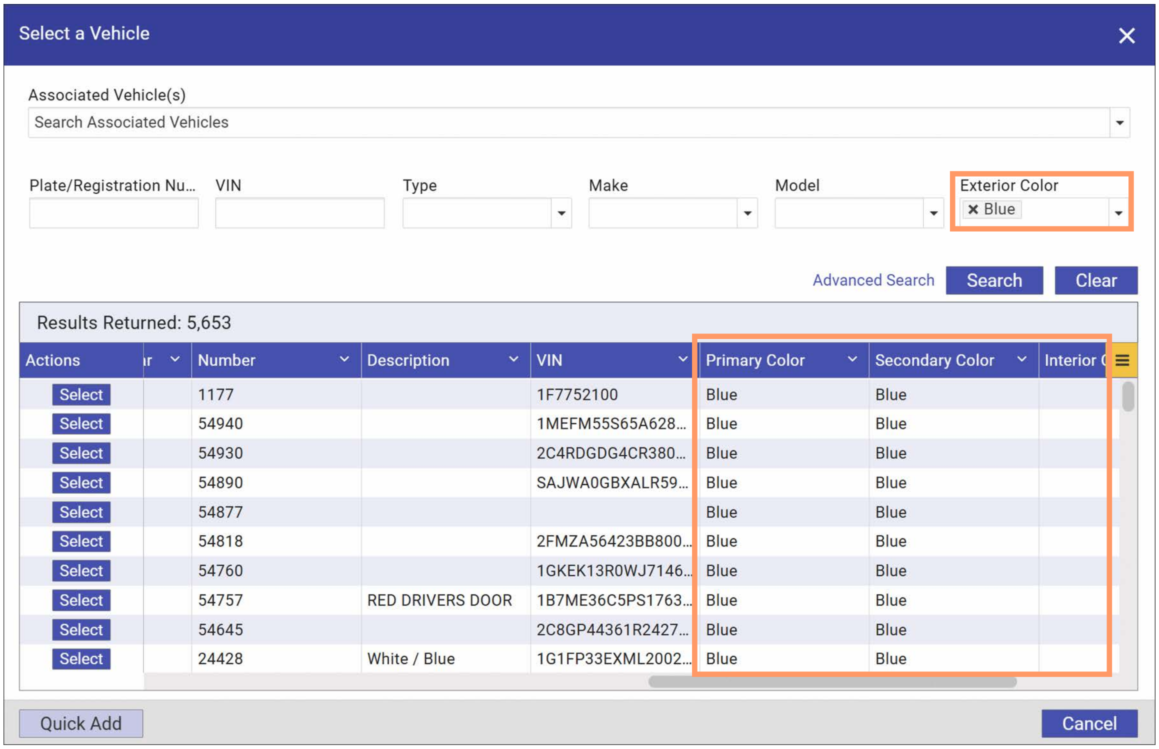
Search Global Vehicles by Color Added

In **2026.3**, the ability to search for vehicles by color has been added.

On the *Search Global Vehicles* page, the ***Exterior Color*** list field was added to search for a vehicle record's Primary and Secondary Colors. In the *Additional Search Fields* section, the ***Interior Color*** list field was added. Also, the results grid was enhanced with the addition of the Primary, Secondary, and Interior color columns.



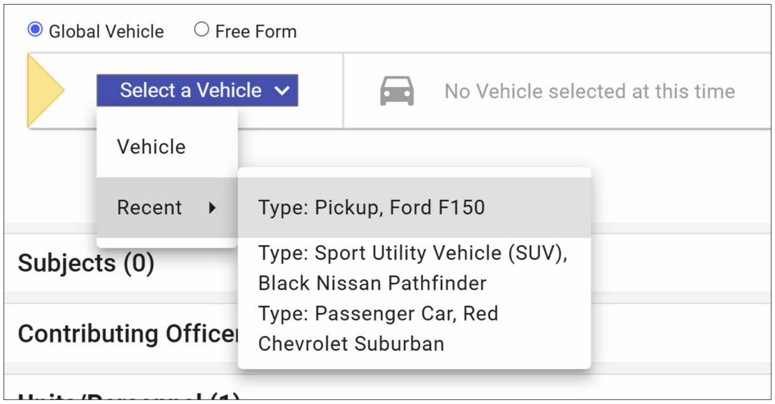
On the *Select a Vehicle* page, the ***Exterior Color*** list field was added to search for a vehicle record's Primary and Secondary Colors. Also, the results grid was enhanced with the addition of the Primary, Secondary, and Interior color columns. The *Select a Vehicle* page is accessed via many modules throughout *Enterprise Records*.

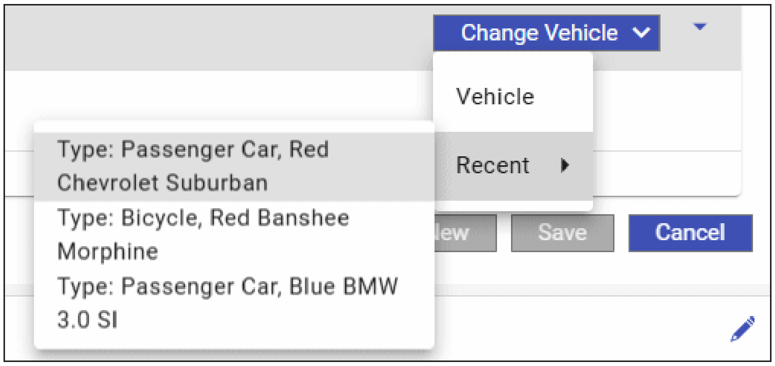


Select Recent Global Vehicles

The **Select a Vehicle** button is used throughout *Enterprise Records* to specify a particular vehicle, such as a stolen vehicle in an Incident record or the vehicles in a Crash record.

In **2026.3**, the **Select a Vehicle** button has been enhanced so that up to 10 previously selected vehicles by the user display under the **Recent** option when the **Select a Vehicle** or **Change Vehicle** button is clicked. This feature saves users time as they don't have to enter the vehicle information a second time.



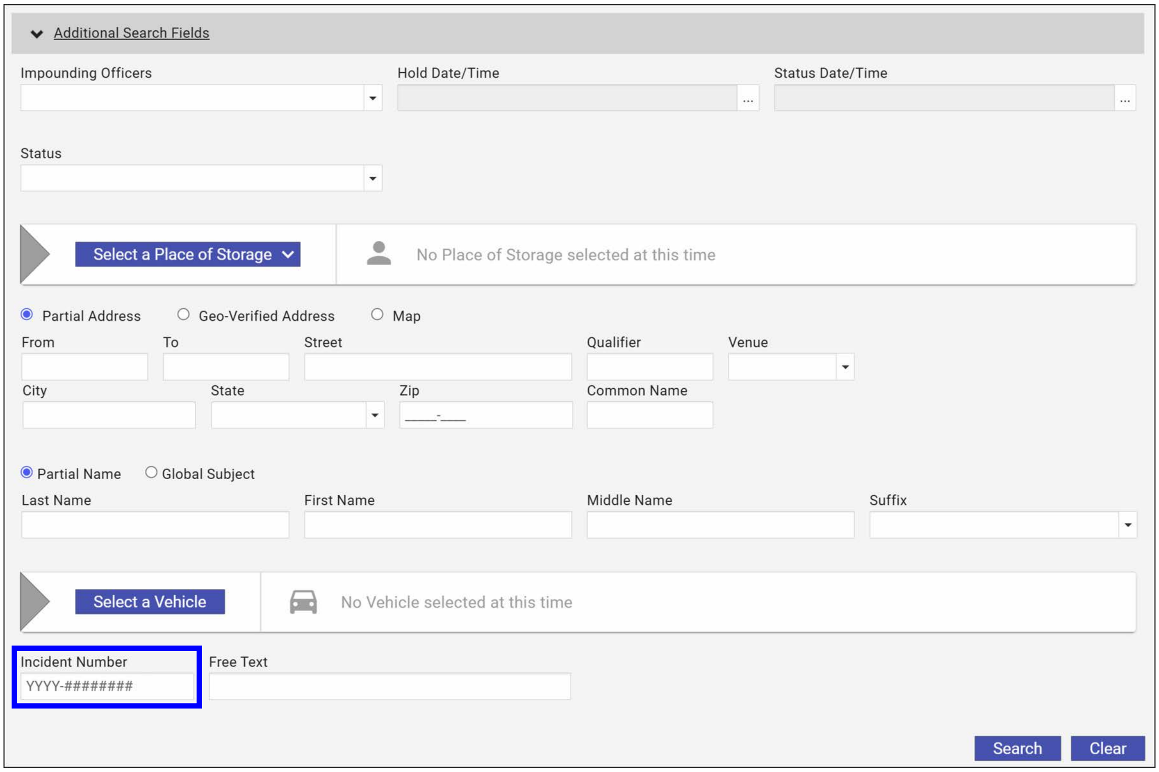


Impounded Vehicles

Impounded vehicles are vehicles that have been impounded by an agency and may be entered and searched for across modules and applications in Enterprise Records. Impounded vehicles include passenger cars, motorcycles, buses, commercial trucks, bicycles, jet skis, boats, airplanes, helicopters, and snowmobiles.

Search Impounded Vehicles by Incident Number

In **2026.3**, the *Search Impounded Vehicles* page has been enhanced with the addition of the ***Incident Number*** field, which enables users to search for impounded vehicles that are attached to an incident. This field was added to the *Additional Search Fields* section.

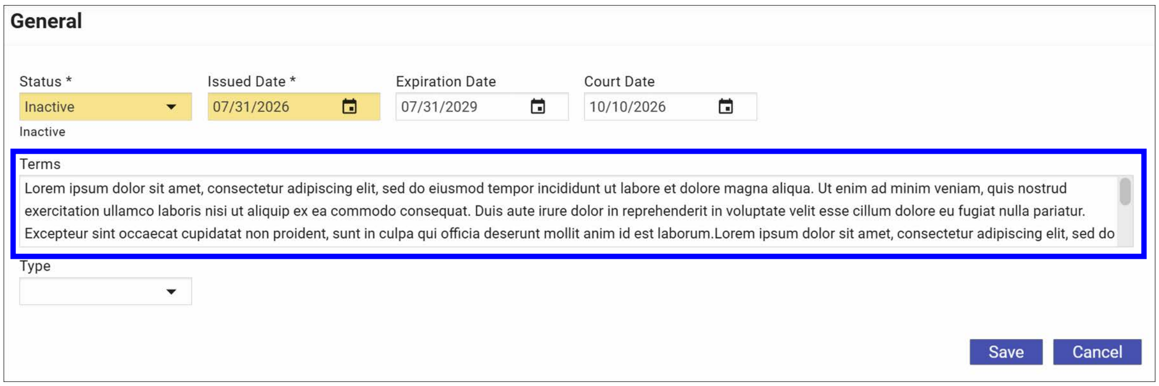


Orders of Protection

An order of protection is a directive or mandate issued by a judge or court to protect a complainant from alleged defendants or aggressors. An order of protection allows agencies to enter all of an order's details and related information, such as associated subjects, locations, cases, terms, activity, remedies, NCIC, and cancellation information. Users can also attach related documentation to a given order record.

Terms Text Field Expanded

In **2026.3**, the ***Terms*** text field in the *General* section was expanded from 128 characters to 2000.



Narcotics Management

The *Narcotics Management* module allows users to enter and maintain records related to narcotics investigations, intelligence gathered, informants, and a fund ledger used to track money used for drug buys and informant payoffs required as part of a sting or investigation.

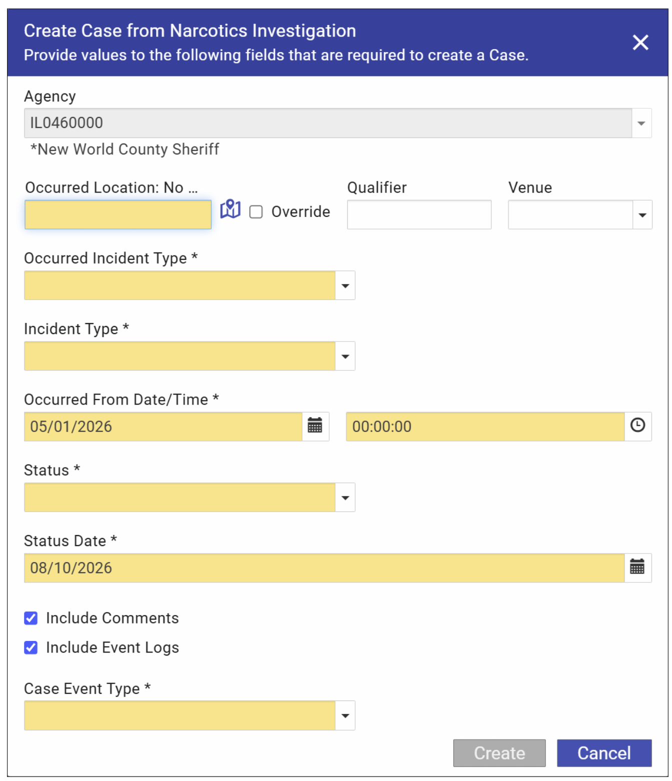
Create a Case Directly from the Narcotics Investigation Page

In **2026.3**, the **Create Case** button was added to the *Narcotics Investigation* toolbar. This enhancement saves users time as they no longer have to duplicate information when creating an incident and case based on a narcotics investigation.

Note: To create a case from the *Narcotics Investigation* page, the user needs permissions to Edit a Narcotics Investigation and to Add a Case.

To create a case from a narcotics investigation:

1. Click the **Create Case** toolbar button. The *Create Case from Narcotics Investigation* dialog displays.
2. Enter the ***Occurred Location***.
3. Select the ***Occurred Incident Type***.
4. Select the ***Incident Type***.
5. Verify the ***Occurred From Date*** is correct; this defaults from the ***Start Date*** field in the investigation. Enter a ***Time***, if needed.
6. Select a ***Status***. The ***Status Date*** defaults to the current date and must be equal to or after the ***Occurred From Date***.
7. Verify the ***Include Comments*** and ***Include Event Logs*** check boxes should be selected. These fields pull information from the *Comments* and *Event Logs* sections.
8. Select a ***Case Event Type***.
9. Click the **Create** button. Another tab opens with the newly created case. The case is associated with the narcotics investigation via the *Associated Records* section. Also created is an incident.



Peripheral Services

In **2026.3**, there is a new version of the Peripheral Services, 2.1.50, available for download. This should be installed on any client machine that uses peripheral services such as:

- Property Room barcode scanner - for computers with Bluetooth scanners.
- Property Room barcode printer - if attached to a computer and not on the network.
- NCIC terminal - anyone using NCIC in *Enterprise Records*.

Installer downloads are available on the **Tools** menu on the navigation bar.

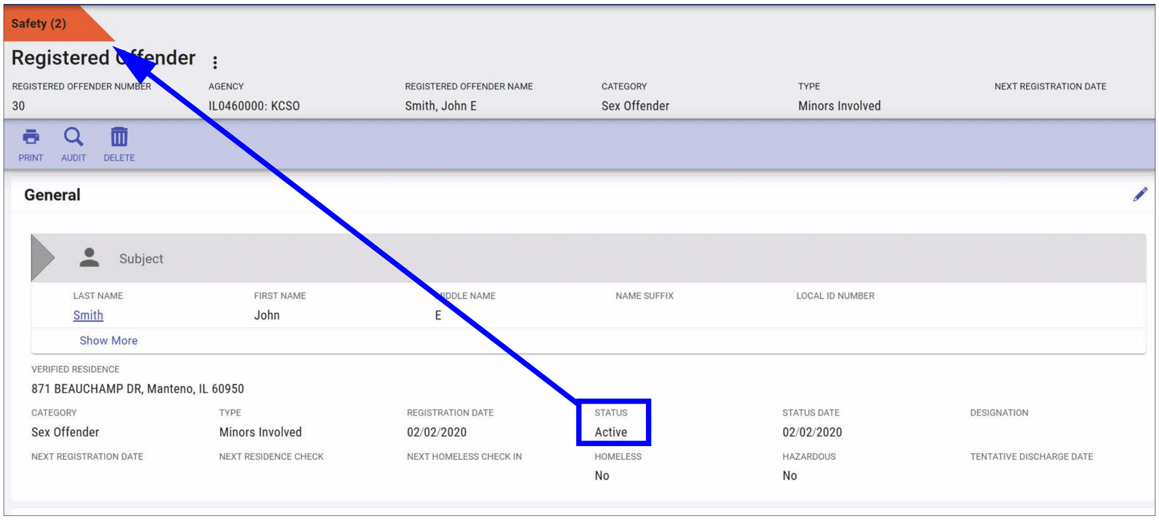
Registered Offender

The *Registered Offenders* module tracks information about habitual offenders and parolees. Although the definition of a registered offender varies from state to state, the term generally applies to multiple and repeat felony offenders.

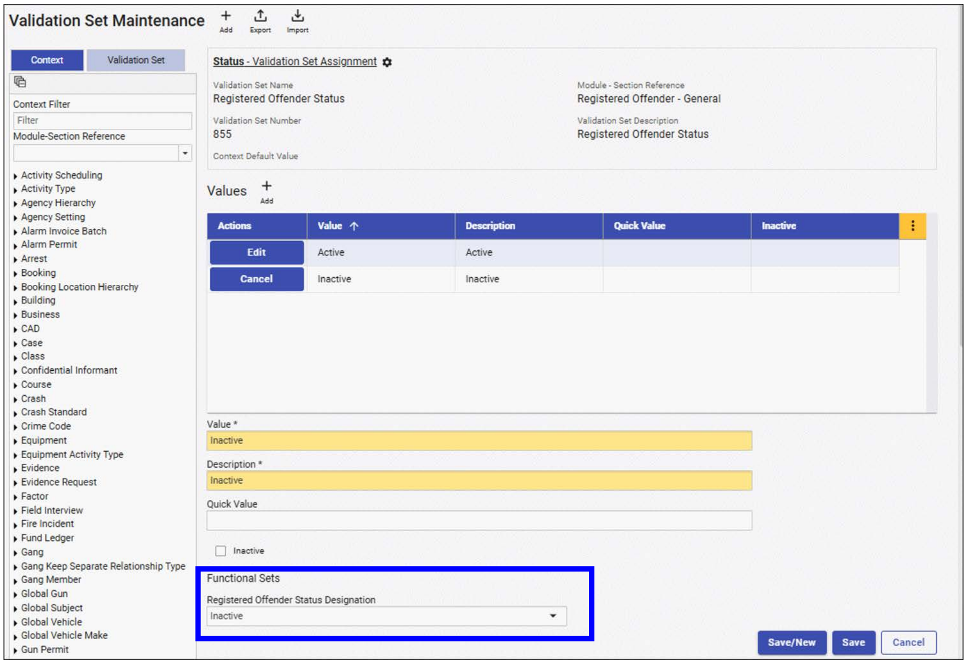
Inactive Offender Expires Associated Alerts

When a Registered Offender record is created, the system creates two Registered Offender alerts: one for the Global Subject and one for the Verified Residence location. Previously, these alerts would never expire, even after the registered offender's ***Status*** was changed to **Inactive**. Some agencies requested to keep the alert active so their officers would see that this person has a past registration; many agencies want the alert to go away when the person is no longer an active registrant; relying on global activity to show historical information.

In **2026.3**, when the ***Status*** of a Registered Offender is changed from **Active** to **Inactive**, the Registered Offender alert on the subject and the location is expired.



The registered offender status is a functional validation set value. To have an active alert, the status must have a functional value of **Active**. To remove the alert, the ***Status*** must have a functional value of **Inactive**. If the agency wants to keep the registered offender alerts regardless of the ***Status***, then the **Inactive** value should be set to a functional value of **Active**.



Note: When an agency first upgrades to the release or patch containing this change, the system performs a one-time update to expire any alerts tied to an inactive Registered Offender. This only happens during the upgrade; if the functional value of a validation set is changed after the upgrade, the system will not mass update alerts. It is highly recommended that agencies review their Registered Offender Status validation set to ensure the functional values are correctly configured for how you want your alerts to function.

Reports

Enterprise Records contains several report types:

- Standard, or system reports, are out-of-the-box reports that are included with the software. Standard reports have a predefined set of fields and layouts that cannot be deleted.
- Custom reports are a variation of a standard report, and the agency configures and saves them. Custom reports allow an agency to configure an existing report to match its needs. After creating a custom report, the agency may choose to inactivate the base standard report, making it easier to find the correct report.
- Templates are created using Microsoft Word. An example of when a template would be used is generating a batch of alarm invoices. Templates are not technically reports; however, they are stored as an option on the Report Manager page.
- The Enterprise Print Designer process is to import an image (PDF) of a state or agency form, overlay dynamic fields on to the image, and save the form. The form is then available in the associated module, and the data is pulled into the form. The form is then saved and distributed to the intended audience.
- Dynamic reports are queries created from the ground up and used to collect agency-specific information. Reports may be designed to search specific data groups, such as Cases or Incidents, and are used to select sub-elements to include under this broad category, such as Case Suspect Global Vehicle Make and Model or Case Property Stolen From Location.

The general workflow for reports is that supervisors/administrators assign logos to the reports, create watermarks, and create custom reports. After this is completed, users can schedule and run reports.

Refer to the following:

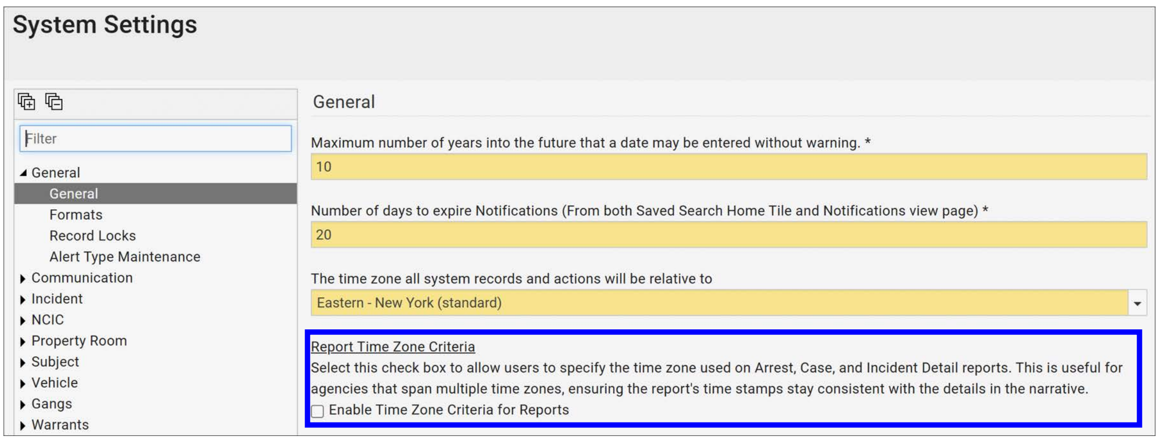
- “Report Time Zone Criteria” on page 166
- “Attach a PDF Copy of a Report to an Email” on page 167
- “Update Reporting Fields” on page 168
- “Dynamic Reports” on page 169

Report Time Zone Criteria

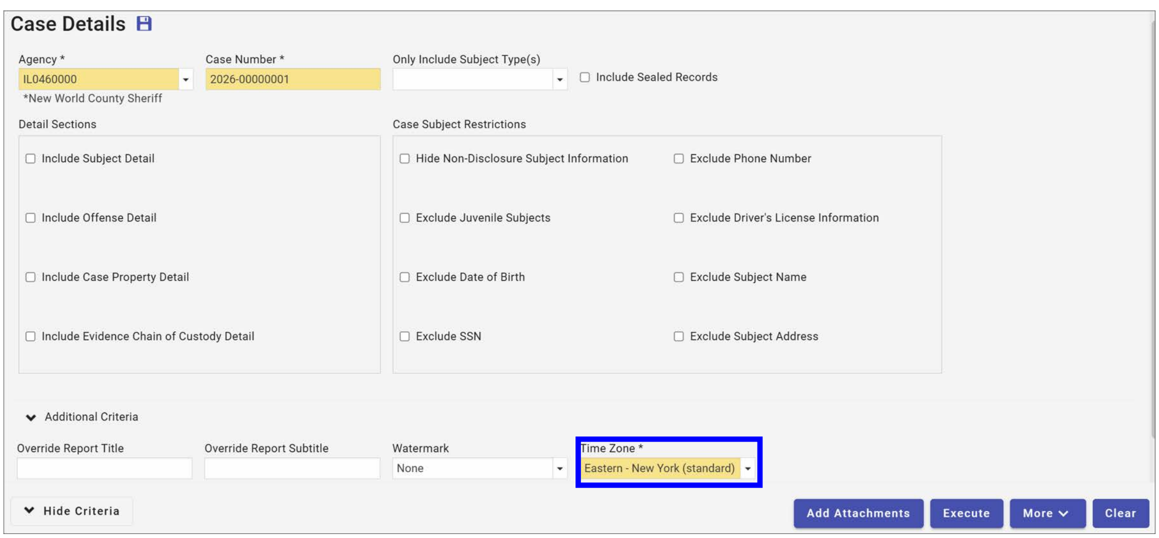
For agencies that span multiple time zones, reports display times without time zone indicators, creating ambiguity for courts, external agencies, and multi-jurisdiction operations. Recipients cannot determine whether displayed times represent their local time, the officer's time zone, or the system's configured time zone.

To solve this, in **2026.3**, the ability to select the time zone in Incident, Case, and Arrest reports has been added.

As part of this enhancement, the ***Enable Time Zone Criteria for Reports*** check box has been added to System Settings. When selected, users can select a time zone in the Incident, Case, and Arrest Details reports.

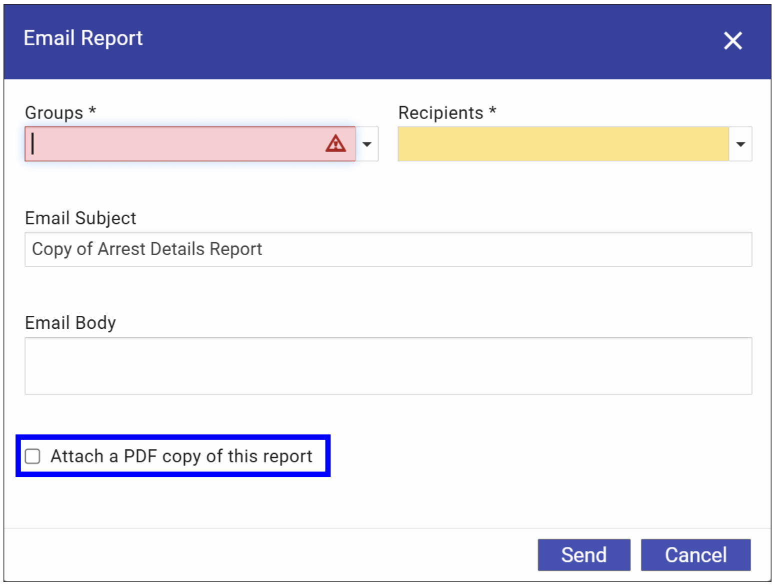


The ***Time Zone*** field is then available in the *Additional Criteria* section of the Incident, Case, and Arrest reports. When the reports is executed, the reports header includes verbiage denoting the time zone. For example, Report time zone: Eastern - New York (standard). All times are shown in this time zone unless otherwise noted.



Attach a PDF Copy of a Report to an Email

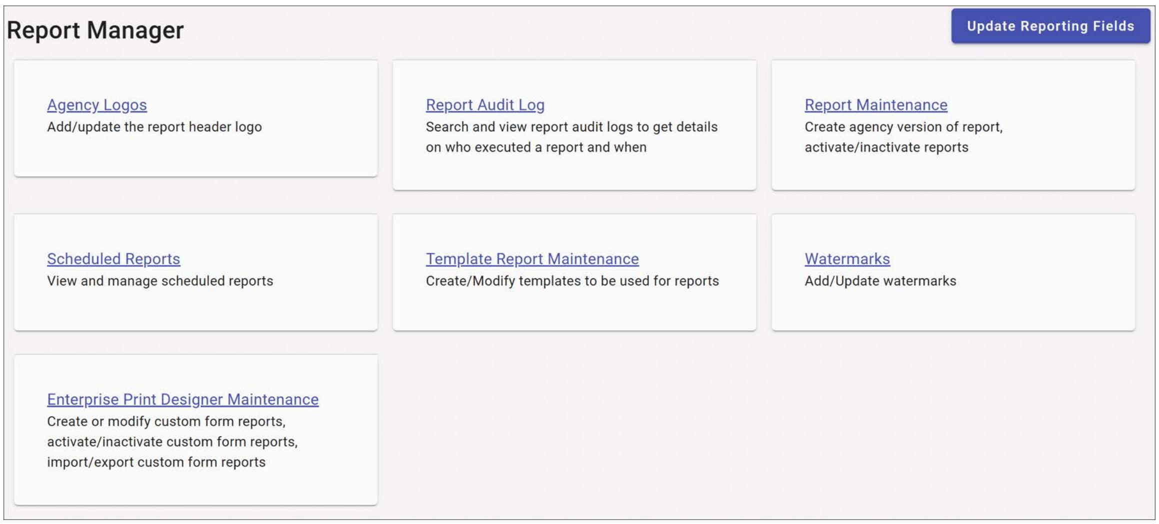
In **2026.3**, the ability to attach a PDF copy of a report to an email has been added. After executing a report, the report information displays. Click the **More** button and select **Email**. The *Email Report* dialog displays with the new ***Attach a PDF Copy of this report*** check box. Selecting this includes the PDF on the email that is sent to the recipients. This also applies to scheduled reports.



Update Reporting Fields

In **2026.3**, the *Report Manager* page has been enhanced with the addition of the **Update Reporting Fields** button. This enables system administrators to immediately update the Reports database with the latest User Defined Fields information in *Enterprise Records*. Click the button, and a confirmation dialog displays; click **Update** to begin the process. The update may take up to ten seconds.

Without using this feature, updates to User Defined Fields are not immediately available in the Reports database and may take an hour to be reflected.



Note: The System Administrator permission is needed to see the Update Reporting Fields button.

Dynamic Reports

In **2026.3**, changes have been made to Dynamic Reports.

Added or Changed Sections and Fields

Changes have been made to the Arrest module in Dynamic Reports:

- In the General submodule, every field that is accessible in a Person report is available.
- In the Charges submodule, Bond section, every field that is accessible in a Person report is available.
- Every business field within the Arrest Charge Posted By section is available for the following subsections:
  - Business Activities
  - Business Addresses
  - Business Auto Extinguishment System
  - Business Available Resource
  - Business Business Contacts
  - Business Comments
  - Business Contact Information
  - Business Events
  - Business Factors
  - Business Fire Alarms
  - Business General
  - Business Hazardous Material
  - Business Registry Information

Changes have been made to the Booking module in Dynamic Reports:

- The following fields were added:
  - Inmate Race
  - Inmate Ethnic Origin

Changes have been made to the Case module in Dynamic Reports:

- Every business field within the Subject General and Property Subject is available for the following subsections:
  - Activities
  - Addresses
  - Auto Extinguishment System
  - Available Resource
  - Business Contacts
  - Comments
  - Contact Information
  - Events
  - Factors
  - Fire Alarms

  - General
  - Hazardous Materials
  - Registry Info
- The following fields were added to the Vehicles and Property Vehicles submodules:
  - Category
  - Condition
  - Engine SEC ICC Number
  - Expiration Date
  - Interior Color
  - Make
  - Mileage/Hours
  - Model
  - Model Year
  - OAN
  - Plate County
  - Plate Month
  - Plate Registration Number
  - Plate State
  - Plate Type
  - Primary Color
  - Secondary Color
  - Style
  - Vehicle Description
  - VIN
  - Year Registered

Changes have been made to the Evidence module in Dynamic Reports:

- The following fields were added to the General section:
  - Current Status
  - Current Status Date/Time

Changes have been made to the Incident module in Dynamic Reports:

- In the Subjects, General tab, Person submodule, every field that is accessible in a Person report is available.
- The following fields were added to the Vehicles section:
  - Category
  - Condition
  - Engine SEC ICC Number
  - Expiration Date
  - Interior Color
  - Make
  - Mileage/Hours

- Model
- Model Year
- OAN
- Plate County
- Plate Month
- Plate Registration Number
- Plate State
- Plate Type
- Primary Color
- Secondary Color
- Style
- Type
- Vehicle Description
- VIN
- Year Registered

- Every business field within Incident Subjects is available for the following subsections:
  - Business Activities
  - Business Addresses
  - Business Auto Extinguishment System
  - Business Available Resource
  - Business Business Contacts
  - Business Comments
  - Business Contact Information
  - Business Events
  - Business Factors
  - Business Fire Alarms
  - Business General
  - Business Hazardous Material
  - Business Registry Information

Changes have been made to the Use of Force module in Dynamic Reports:

- The following fields were added to the Related Subject tab in the Officer section:
  - Baton
  - Caliber
  - Cartridge Serial Number
  - Decontamination
  - Drive Stun Used Independently
  - Duration of Sprays
  - Firearm
  - Serial Number - Firearm
  - Firearm Type

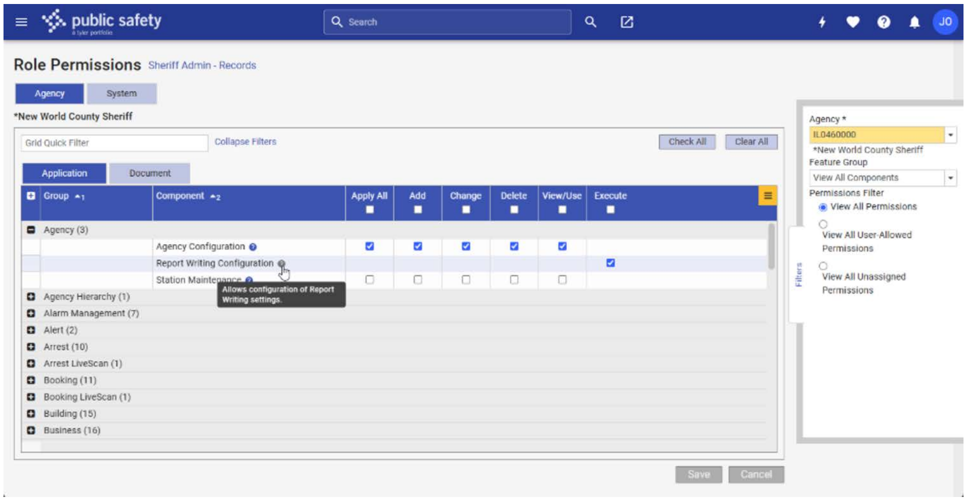
- Head Strike
- Make
- Model
- Number of Cartridges Used
- Number of Sprays
- Number of Strikes
- Pepper Spray
- Compliance to Policy - Pepper Spray
- Target Distance (ft.) - Pepper Spray
- Probes Removed By
- Tactic Used
- Taser
- Compliance to Policy - Taser
- Reviewed by Coordinator
- Taser Discharged w/Drive Stun
- Serial Number - Taser
- Target Distance (ft) Taser
- Turned into Evidence
- Cycle Duration

Report Writing Configuration

A review level is a graduated security system based on levels of authority, and it enables different features for different levels of users. New in **2026.3** is the ability to add review levels to *Report Writing* reports.

Grant Agency Administrators Access to Report Writing Configuration

In *Role Permissions*, assign each Agency a role with Execute permission for the new **Report Writing Configuration** agency permission.

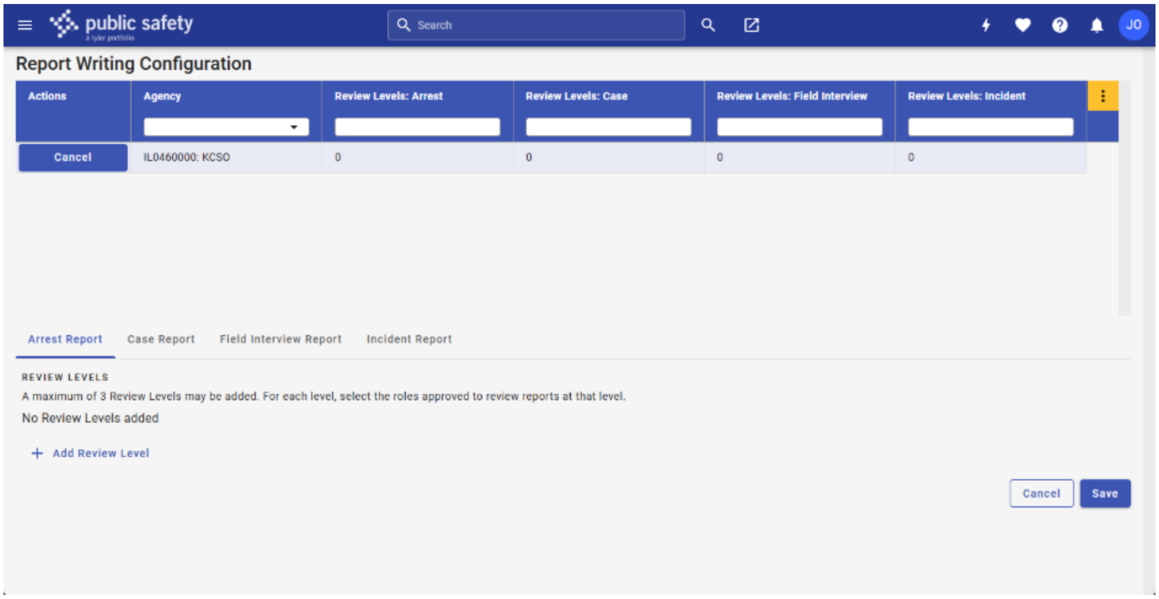


Add Review Levels

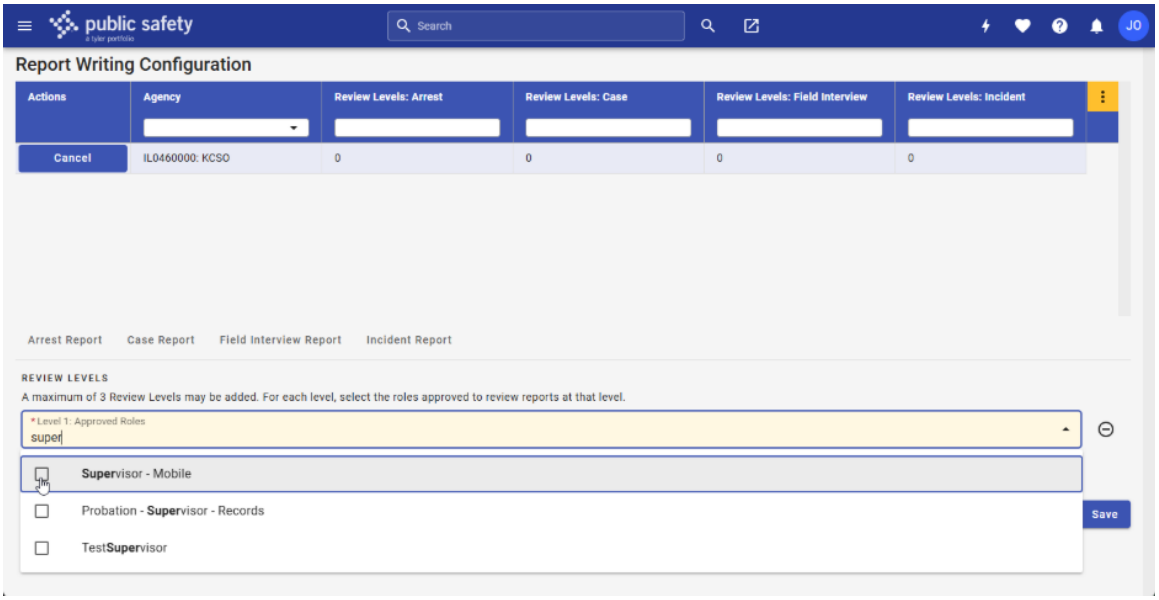
To add review levels:

1. Select **Settings** and then **Report Writing Configuration** from the navigation menu. The *Report Writing Configuration* page displays and lists all agencies the user has access to configure. By default, all agencies are configured with 0 reviews for all report types.
2. Click the **Edit** button associated with an agency. The *Arrest Report* tab is activated.

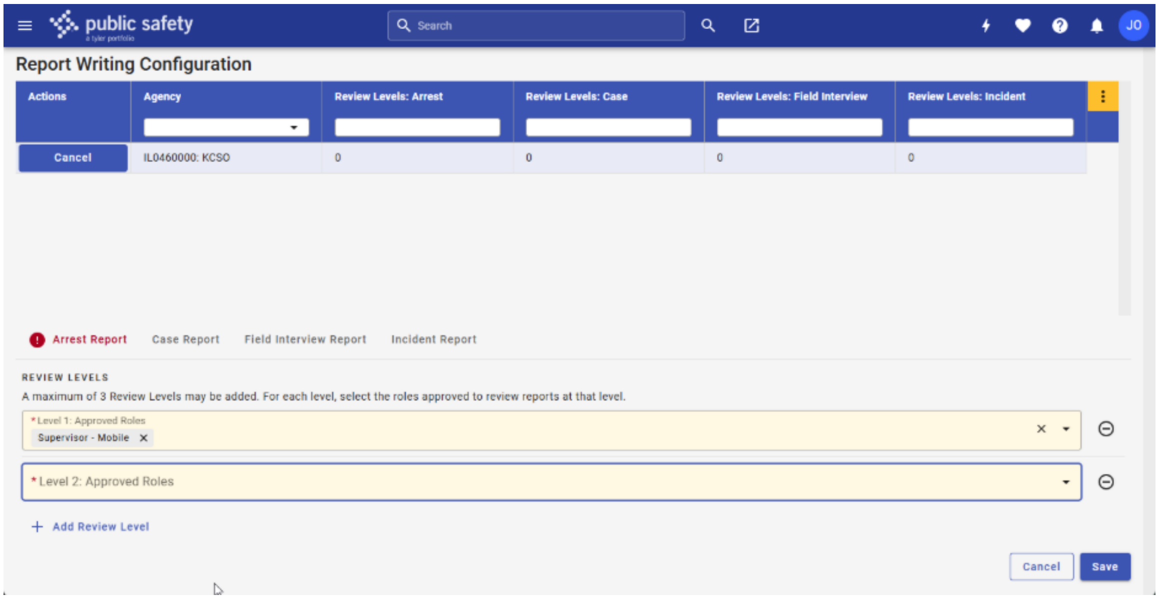
3. Click the **+ Add Review Level** button to add a first review level.



4. Select which role(s) are allowed to review reports for that agency for Arrests at level 1.



5. Click the **+ Add Review Level** button again to add a second or third review level. Each report type can have between 0 and 3 review levels.



6. Click **Save**.
7. Continue with the same process for the other reports requiring supervisor reviews. The *Case Report* tab contains the ***Ignore Case Status Changes on Follow-Up Reports*** check box. Select this check box, and the case Status and Status Date in *Enterprise Records* are not updated when completing the review of a follow-up report in the field.

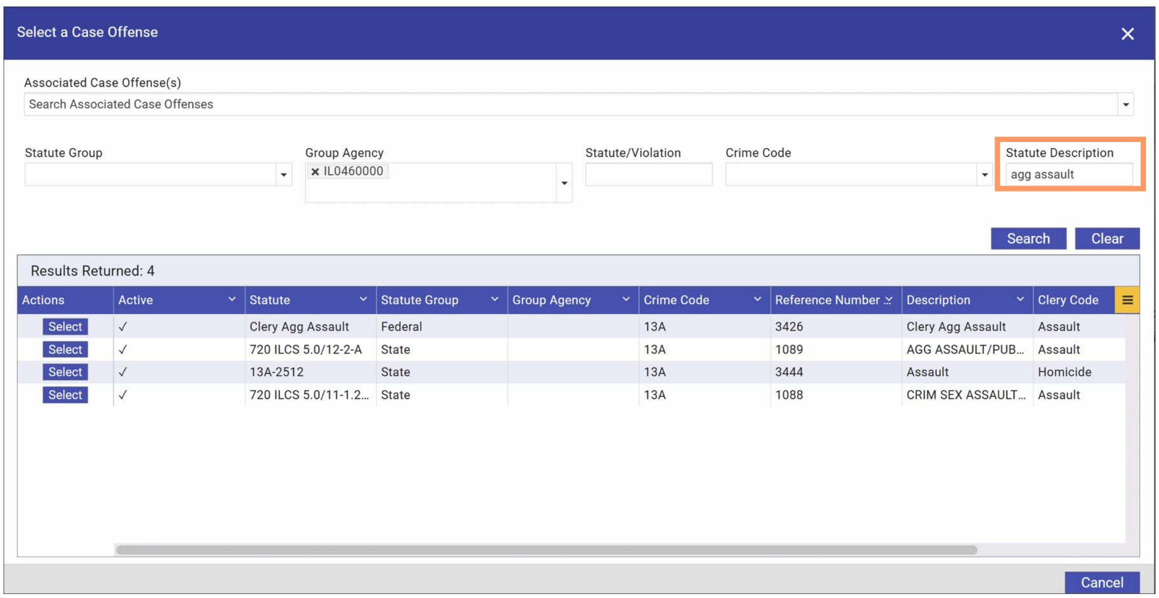
8. Configure any other agencies listed on the *Report Writing Configuration* page.

Statute Selection Control

The statute select control goes by various names throughout the software. For example, in the Arrests module, it is the Select an Arrest Charge, whereas in Cases, it goes by Select a Case Offense.

Statute Description Field Enhanced

in **2026.3**, the ***Statute Description*** field has been enhanced with the ability to search by multiple words. For example, entering Aggravated Assault searches for any statues with either of those terms. The search uses fuzzy technology. For example, if Agg is entered, any statutes containing Aggravated are included in the results.

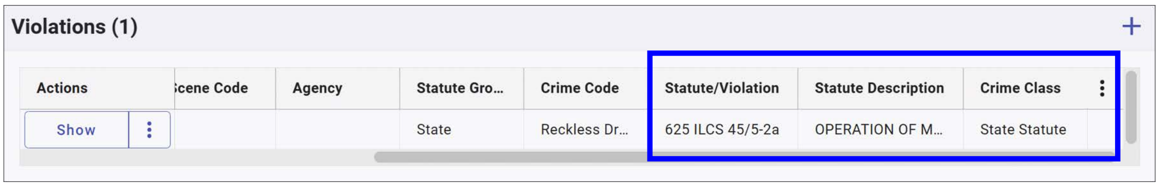


Ticket and Citation Processing

The Tickets and Citations module allows authorized users to enter and maintain information about tickets and citations for traffic law or city ordinance violations. Additionally, users can maintain information about voided tickets and issued ticket books.

Ticket Violations Grid Enhanced

In **2026.3**, the Violations grid on the Ticket page has been enhanced with three new columns: Statute Violation, Crime Class, and Statute Description.

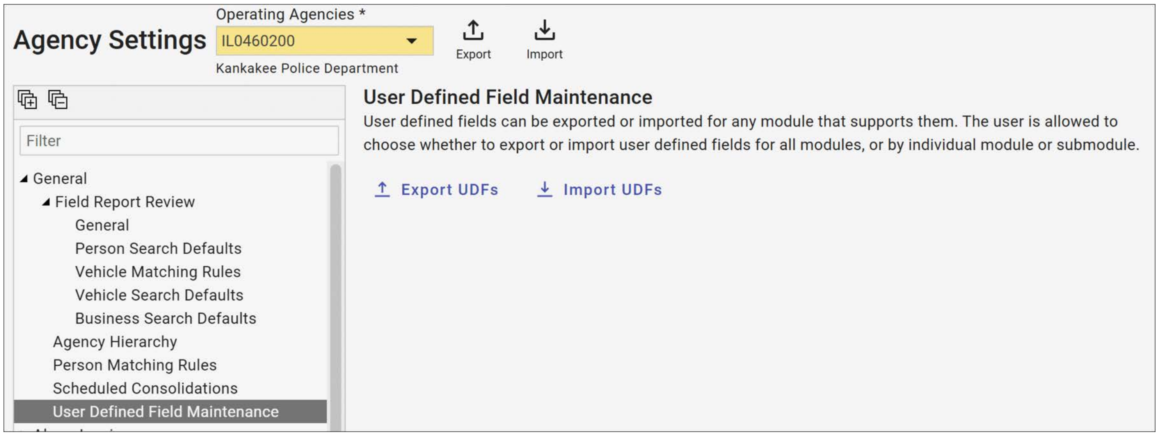


User-Defined Fields

A user-defined field can be created and added to a section within a module.

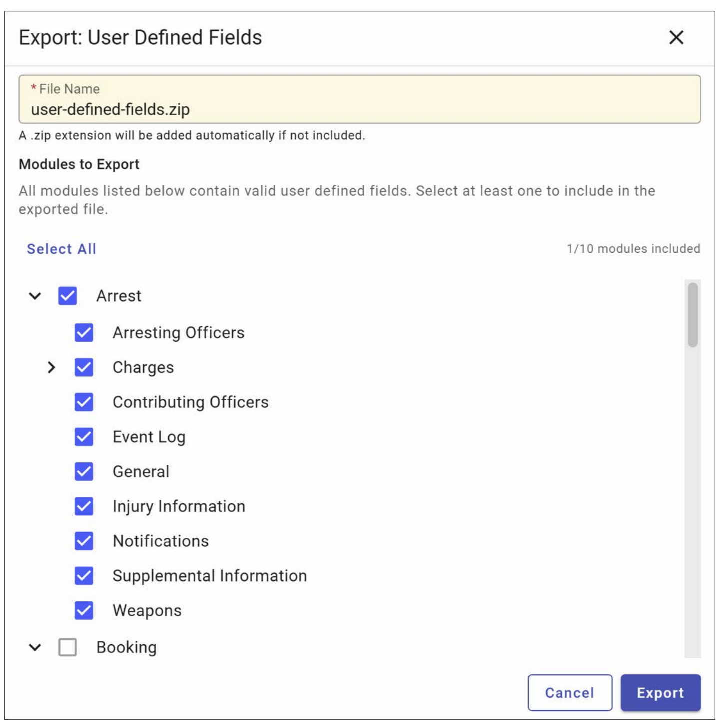
Import and Export User-Defined Fields Functionality Added

In **2026.3**, the ability to import and export user-defined fields between agencies was added. In Agency Settings, from the navigation tree, select **General** and then **User Defined Field Maintenance**. The *User Defined Field Maintenance* section displays.



To export the user-defined fields:

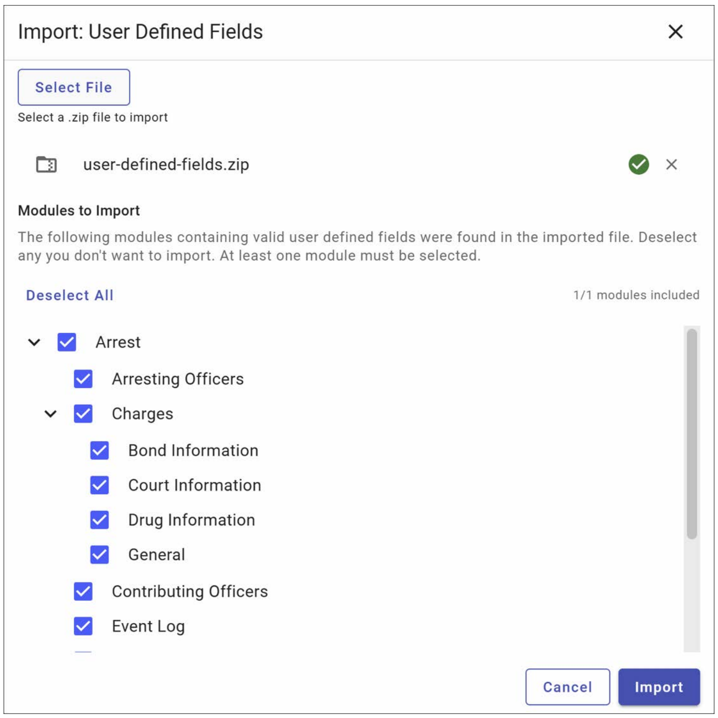
1. Click the **Export UDFs** button. The *Export: User Defined Fields* dialog displays.
2. Click the **Select All** button to select every user-defined field, or individually select modules or the fields in the ten modules.



3. Click the **Export** button. The *Save As* dialog displays; the file name defaults to user-defined-fields.zip.
4. Select the location for the Zip file to be saved and click the **Save** button.

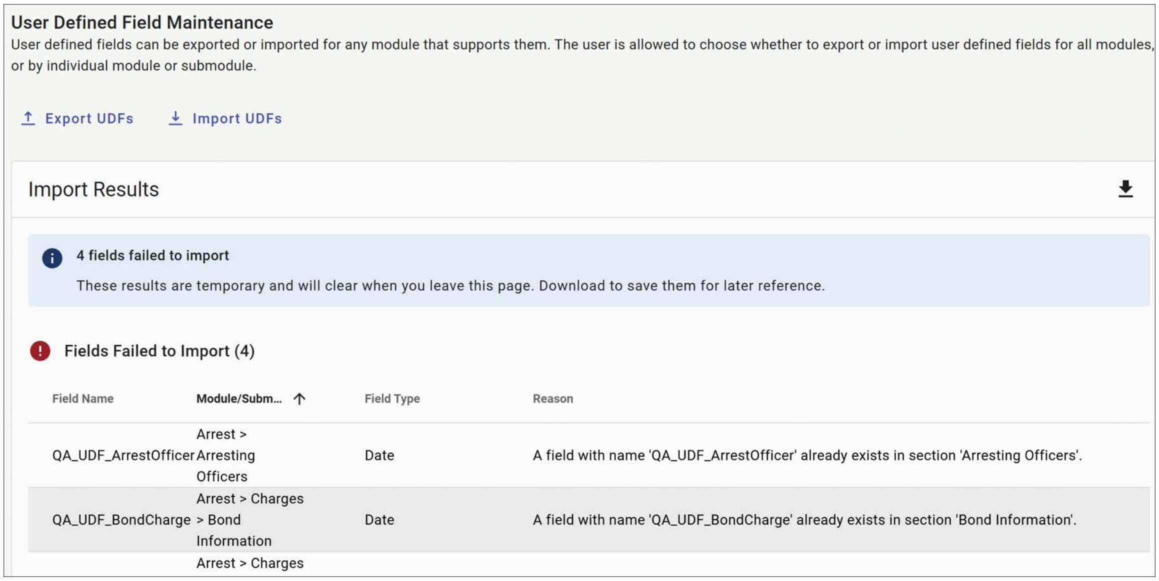
To import the user-defined fields:

1. Click the **Import UDFs** button. The *Import: User Defined Fields* dialog displays.
2. Click the **Select File** button. The *Open* dialog displays.
3. Select the zip file and click the **Open** button. The fields available in the zip file populate the dialog.



4. Select the fields to be imported.

5. Click the **Import** button. The *Import Results* information is displayed on the screen, showing which fields were imported and which were not. This information can be exported to a .CSV file by clicking the **Download Results** button. When the screen is exited, the *Import Results* are cleared and are no longer accessible.



The imported fields are appended to the end of the fields in their respective sections; a user or administrator must move them to the correct order in Module Configuration.

Chapter 6
MSP

Introduction

This chapter describes enhancements made to the **2026.3** version of *MSP*. It includes all enhancements made in *MSP Maintenance*.

See the following sections for additional information:

❖ ❖ ❖ ❖ ❖

Email Servers

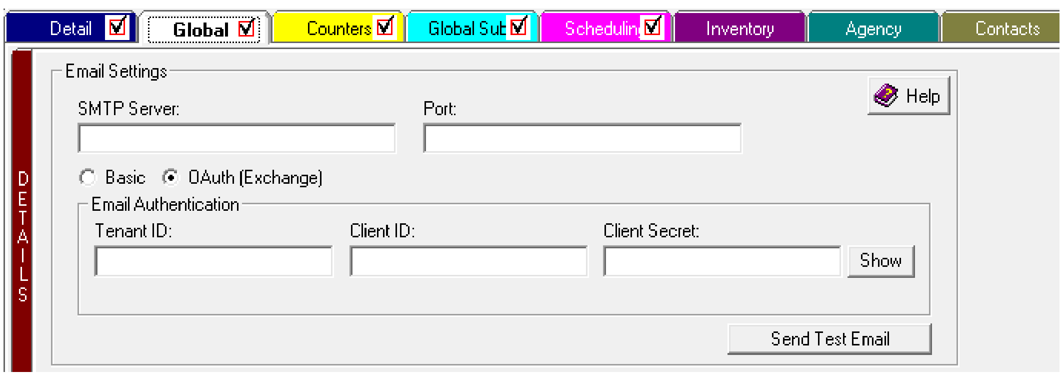
MSP contains two locations for setting up email server communications. *System Settings* is used as the default, but in *Jurisdiction Maintenance*, individual agencies can be set up, which overrides the *System settings*.

Email Servers Enhanced Pages Enhanced

In 2027, *Microsoft* is deprecating basic authentication for their Exchange Online SMTP. With that in mind, in **2026.3**, *Jurisdiction Maintenance* and *System Settings* have been enhanced with new authentication fields to support OAuth for email settings.

- In *MSP Maintenance*, select **System Settings** and the *Communication* tab.
- In *MSP Maintenance*, select a jurisdiction, then **Jurisdiction Maintenance**, the *Global* tab, and the *DETAILS CONT* sub-tab.

In both situations, radio buttons have been added to select ***Basic*** or ***OAuth (Exchange)***. Basic retains the fields used previously. The ***OAuth*** option displays three new fields: The ***Tenant ID*** and ***Client ID*** fields. If the secret needs to be changed, click the **Show** button to enable the ***Client Secret*** field.



Note: Additional set up is required for any agencies using OAuth. Please contact Tyler support for assistance.

Property Room Handheld

The *Property Room Handheld* app allows *MSP LERMS* users to perform property room tasks, such as checking inventory with their *Zebra Barcode Scanner* device or other mobile device.

Permission Checks Added to Prevent Users from Updating Items for Agencies they aren't Authorized

In **2026.3**, the **Property Room Entry** permission was updated so that if a user does not have access to it in a particular agency, they cannot move or dispose of items in that agency. If they attempt to change an item in an agency they do not have permission to, they receive the message, “There was an error retrieving the scanned item: No items found with barcode <barcode number>.”

This enhancement prevents users from accidentally making property room changes to items outside of their agency.

This change impacts:

- Property Room personnel using the PRH app in multi-agency environments.
- Agencies sharing a multi-ORI configuration where users may encounter items from other agencies during barcode scanning.

This enhancement leverages the existing **Property Room Entry** (Change) permission settings already configured in Permissions Maintenance. No additional configuration is needed. Agencies should verify their current permission assignments reflect the intended access levels.