MOTOROLA SOLUTIONS

Flex™

Flex Release Notes

System Release: 2024.4, 2024.3, 2024.2, 2024.1, 2023.4, 2023.3, 2023.2, 2023.1, 2022.4, 2022.3, 2022.2, 2022.1, 2021.4, 2021.3, 2021.2, 2021.1, 2020.4

OCTOBER 2024

MN010159A01-J

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive


The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end users in EU and UK countries should contact their local equipment supplier representative or service center for information about the waste collection system in their country.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

Service agreement customers should be sure to call the CMSO in all situations listed under Customer Responsibilities in their agreement, such as:

- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN010159A01-001	First release of the *Flex Release 2023.2* document. This document presents additional changes made to Flex for the 2023.2 Release.	April 2023
MN010159A01-002	Second release of the *Flex Release 2023.2* document. This document presents additional changes made to Flex for the 2023.2 Release. Updated section: • Datalogic Memor X3 and Windows Mobile Device Center on page 194	April 2023
MN010159A01-C	Initial release of the consolidated *Flex Release Notes*. Includes the notes from Releases 2020.4 – 2023.3. New chapter: • Release 2023.3 on page 155 Updated section (in Release 2023.2 on page 181): • Configuring the Amount of Cached CAD Windows on page 181	July 2023
MN010159A01-D	Updated release of the consolidated *Flex Release Notes*. New chapter: • Release 2023.4 on page 128	October 2023
MN010159A01-E	Updated release of the consolidated *Flex Release Notes*. New chapter: • Release 2024.1 on page 99	January 2024
MN010159A01-F	Updated release of the consolidated *Flex Release Notes*. New chapter: • Release 2024.2 on page 79 Updated section (in Release 2023.3 on page 155): • New and Updated Reports on page 170	April 2024
MN010159A01-G	Updated release of the consolidated *Flex Release Notes*. New chapter: • Release 2024.3 on page 61	July 2024
MN010159A01-H	Updated release of the consolidated *Flex Release Notes*. New topic: • LO Command Removal on page 64	August 2024
MN010159A01-J	Updated release of the consolidated *Flex Release Notes*. New chapter:	October 2024

Version	Description	Date
	• Release 2024.4 on page 34	

Contents

List of Tables

List of Figures

List of Procedures

About Flex Release Notes

Welcome to the Flex Release Notes document.

This consolidated document presents additional changes made to Flex for the consecutive releases.

Information intended specifically for the administrator at your agency is labeled "Admin". All other information is for general users, as well administrators.

NOTE: Each **latest** (first) chapter of this is document is intended for temporary use by agencies needing enhancement information prior to a given release. When the applicable release is officially released, the enhancement information is integrated into the corresponding product manuals. The previous chapters allow users to track changes that were made earlier.

Chapter 1

Release 2024.4

This chapter presents changes made to Flex for the 2024.4 release.

1.1 CAD

1.1.1 VESTA 9-1-1 ICC Integration

Flex CAD can integrate with VESTA 9-1-1 ICC so that dispatchers can use call controls in the **CAD Incident** screen, which simplifies the workflow. To use the integration, your agency must purchase VESTA 9-1-1 ICC and your administrator must set up the connection.

Once your administrator establishes your connection to VESTA 9-1-1 ICC through Flex, whenever you answer a call, or redial an abandoned call, the **CAD Incident** screen automatically opens and displays the call controls on the left. If you are silently monitoring a phone call, the **CAD Incident** screen does not open. However, if you unmute yourself to join the conversation, then the **CAD Incident** screen opens.

NOTE: For more information about how to set this up, see the *Flex CAD Administrator Manual*.

1.2 Mapping

1.2.1 ArcGIS Pro

ArcGIS Server 11.3 is now available and only compatible with ArcGIS Pro.

Updating to ArcGIS Pro is a major update, which will require models and locators to be rebuilt. Please review the *Flex Hardware and System Requirements* for more information and contact your administrator or Motorola Representative about updating to ArcGIS Pro.

1.2.2 EagleView Integrated Explorer

The Flex Mobile Map in Flex version 2024.4 and above is now compatible with the EagleView Integrated Explorer instead of Pictometry Map. Pictometry International was acquired by Eagleview Technologies and they have made the decision to sunset the Pictometry Map product.

Pictometry is being replaced because the control used to access images in Pictometry is no longer supported. EagleView Integrated Explorer imagery is hosted by EagleView in the Cloud, where the Pictometry Imagery was stored on the local PC.

Set Up

To set up EagleView Integrated Explorer, administrators must adjust certain settings in the Administration Manager on the Module > Module.Mapping screen. These settings include:

- **obliqueImageryClientID**: EagleView provides this information to agencies.
- **obliqueImageryClientSecret**: EagleView provides this information to agencies.
- **obliqueimageryTokenURL**: This URL is entered by default.

When these required settings are adjusted, users gain access to EagleView Integrated Explorer imagery.

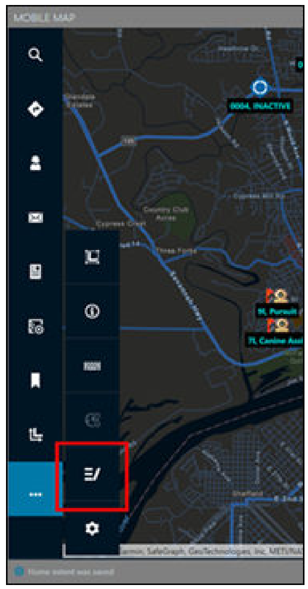
For more information on setting up EagleView Integrated Explorer, see the *Flex EagleView Map Manual*.

EagleView Integrated Explorer in Flex Mobile Map

Users can access EagleView Integrated Explorer on the Flex Mobile Map using one of the following methods:

- Users can click the **EagleView** button on the Flex Mobile Map toolbar.

Figure 1: EagleView Button



- Users can right click on a specific location on the Flex Mobile Map and select **EagleView** from the right click menu to view that location in EagleView.

When the EagleView Integrated Explorer displays, users can access the EagleView toolbar. This toolbar contains buttons that allow access to different EagleView features.

Figure 2: EagleView Map with EagleView Toolbar Highlighted

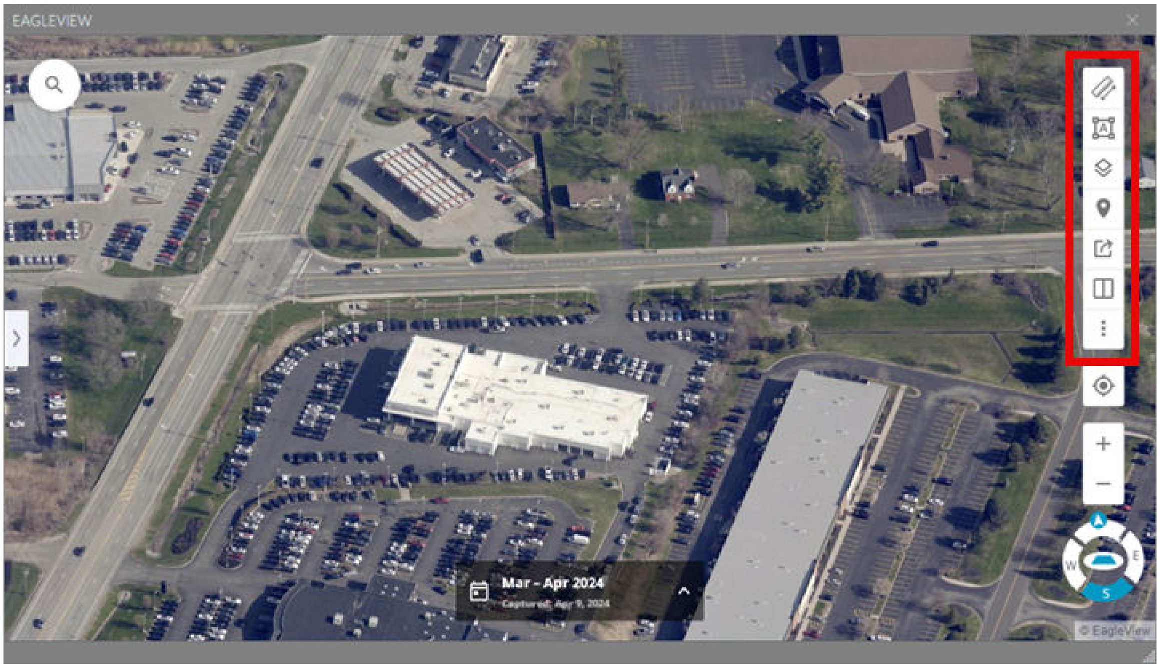
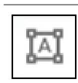
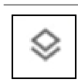
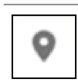
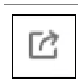
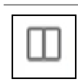
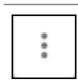


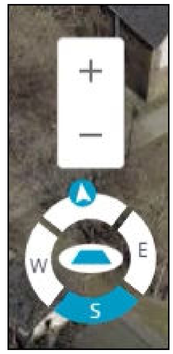
Table 1: EagleView Toolbar Buttons

Button	Name	Description
	**Measure**	The **Measure** menu allows users to measure distance, area, and height of features visible in images.
	**Annotate tools**	The **Annotate tools** menu allows users to annotate images and maps.
	**GIS Layers**	The **GIS Layers** menu allows users to search for information within different layers available to your agency.
	**Location and Image Info**	The **Location and Image Info** menu allows users to view specific location information.
	**Export**	The **Export** menu allows users to export images from maps as a `jpg`, `png`, or `pdf` file.
	**Dual Pane**	The **Dual Pane** menu allows users to view the map in Dual Pane mode.
	**More**	The **More** menu displays options to hide the toolbar or access user settings.

Users can change the directional view of the EagleView image by clicking the direction buttons in the bottom right corner of the screen. For example, users can click the **S** button to view the image from the South.

Users can also zoom into the image by pressing the plus (**+**) button, or zoom out of the image by pressing the minus (**-**) button.

Figure 3: EagleView Direction Buttons and Zoom Buttons



For more information on using the tools in the EagleView toolbar and for detailed descriptions of other available features, see the *Flex EagleView Map Manual*.

1.2.3 Mobile Map Updates

We made the following updates to the mobile map:

- You can now toggle the visibility of incident and unit labels as well as icons. These are activated by toggling the switches to the **Mobile Map Settings** pane. The **Show Icon** and **Show Label** switches appear in both the **Incidents** and **Units** sections.
- We added the ability to toggle the Incident Nature and Unit Status labels on the map.
  - You can toggle these labels on or off by using the following two new adminutil settings: **Module.Mapping.showCADIncidentNature** and **Module.Mapping.showUnitStatus**. If these two adminutil settings are set to **False**, the Incident Nature and Unit Status labels do not display on the Mobile Map. If they are set to **True**, the Incident Nature and Unit Status labels do display on the Mobile Map. You must close and re-open the Mobile Map to reflect any changes made to these two settings.

1.3 Mobile

1.3.1 File Lists in Mobile

The additional fields added to the **File Capture** screen in Flex desktop have now been extended to file lists in Mobile.

- Added the following new fields: **Captured By**, **Created Time**, **Retention**, **Storage Location**
- Updated **Date Added** field label to **WhenAdded** field
- Updated the column order to match Flex desktop
- If files are stored in CommandCentral Evidence, you can now open the files directly in CC Evidence

1.4
Platform

1.4.1
2024.4 Schema Changes

Starting with 2024.4, we are publishing a document on the LXP which lists all of the schema changes that have been made in Flex since 2023.1+. You can find this document by using the Flex Documentation link in the Help menu or by searching in the LXP for Document ID `MN006565-A01`.

1.4.2
Added Ability to View Initial TOTP Authentication Code

We improved the TOTP registration process for agencies that do not allow cell phones at their work stations and need to register devices for TOTP, for example, a desktop TOTP app or a physical programmable 2FA device.

Now, in addition to using a QR Code, users can view the authentication key on their screen to enter the key manually when they are completing the initial registration of their TOTP device.

When you are logging in for the first time after TOTP is enabled for your agency and reach the QR code screen in the device registration process, you can see the registration code and enter it manually by clicking **View Key for Manual Entry**.

Figure 4: QR Registration Screen

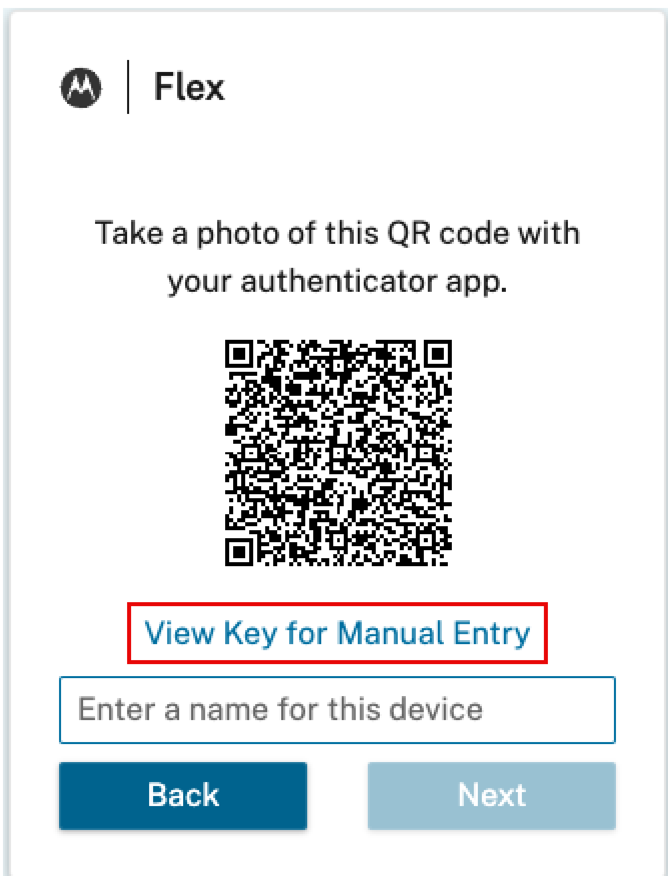
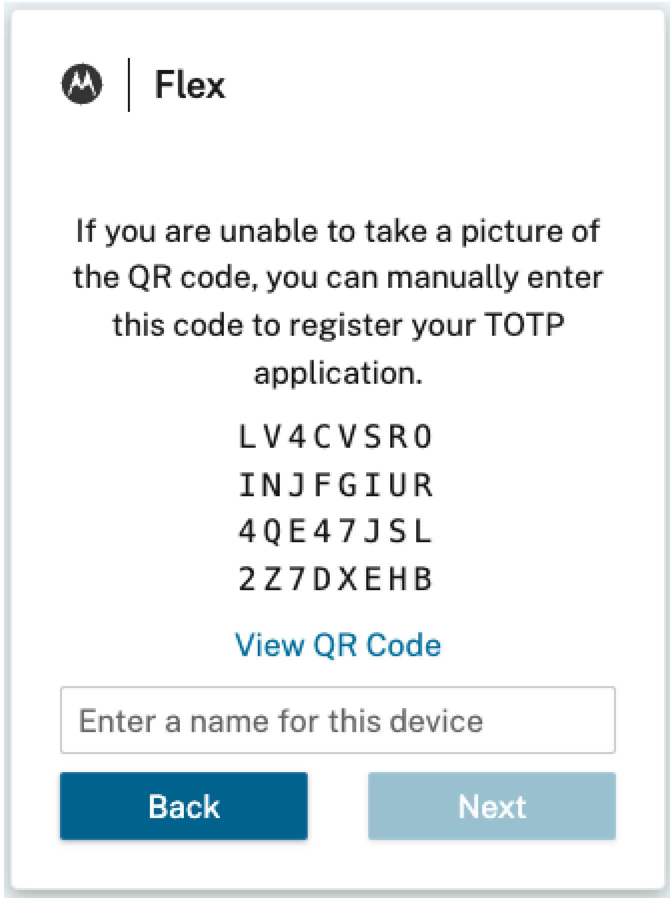


Figure 5: Manual Entry Registration Screen



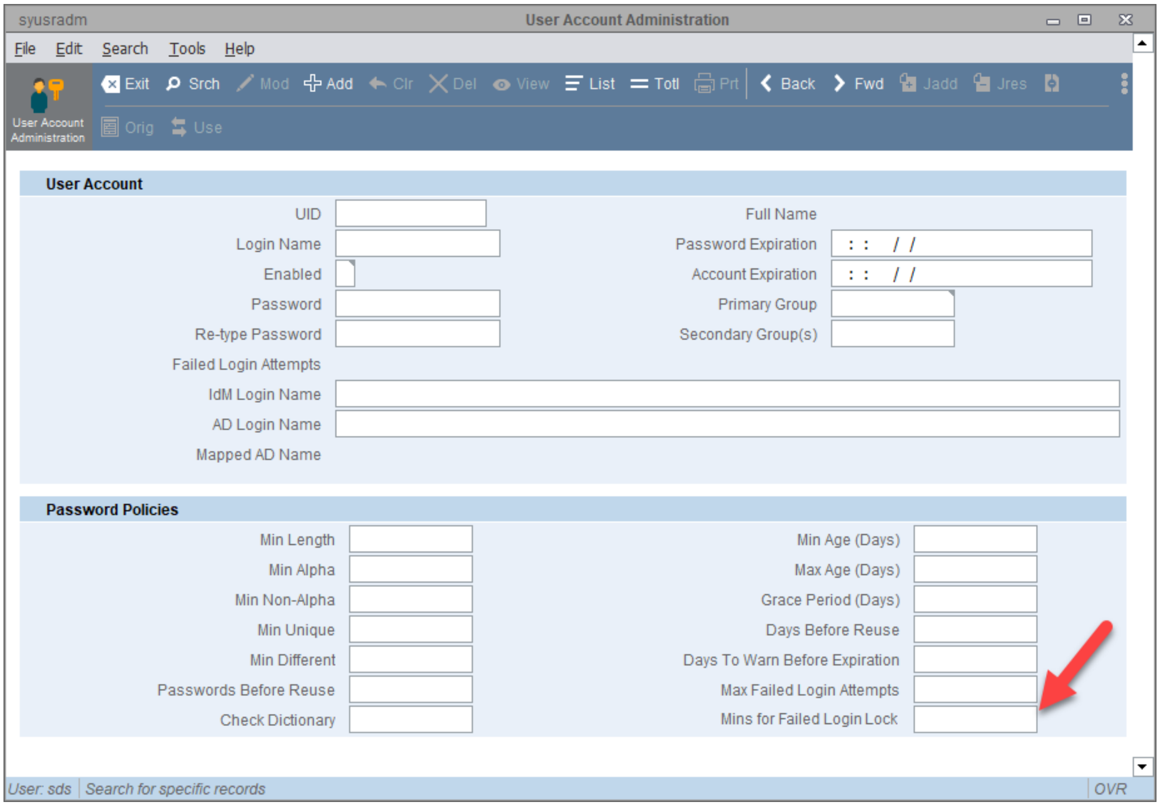
From the manual entry screen, you can also click **View QR Code** to return to the QR code screen and use your mobile device for registration instead.

1.4.3
Failed Login Time Threshold

In 2024.4 we are releasing a Failed Login Time Threshold Feature. Now, when a user exceeds the threshold of consecutive failed logins within the minutes specified in the **Mins for Failed Login Lock** field, the user account will be locked. A system administrator or authorized administrator must unlock the users account, it cannot be automatically unlocked as per CJIS Security Policy 5.9.3 AC-7.

NOTE: If an agency is using Active Directory Integration, these fields are ignored.

Figure 6: Updated User Account Administration Field



This setting is configured from the **User Account Administration (syusradm)** screen where we added a new field, **Mins for Failed Login Lock**. New sites are defaulted to CJIS requirements 15 minutes. Existing sites are defaulted with the `OFF` keyword.

The **Max Failed Login Attempts** field is used in conjunction with the **Mins for Failed Login Lock** field. If the **Mins for Failed Login Lock** field is set to `OFF`, the user's account is locked once the number of **Max Failed Login Attempts** is reached. There is no time limit.

If the **Mins for Failed Login Lock** field time is set to `OFF` or `0`, the original process of account locking of the system occurs; no timer is used.

For example, if the **Max Failed Login Attempts** field is set to `5` and the **Mins for Failed Login Lock** field is set to `15`, the following happens:

Table 2: Scenario Descriptions

Scenario	Description
1	Between 10:00AM and 10:05AM, the user makes four consecutive failed attempts to login to Flex. At 10:06AM, the user makes the fifth failed attempt to login to flex. That user account will be locked as they had **five** failed login attempts in a **six** minute period.
2	Between 10:00AM and 10:05 AM, the user makes four consecutive failed login in attempts. At 10:20AM, the user makes a 5th failed attempt to login to Flex. That user

Scenario	Description
	account will not be locked because only **one** failed attempt occurred within a **fifteen** minute period.
3	Between 10:00AM and 10:05AM, the user makes **four** consecutive failed login attempts to Flex. At 10:06AM the user successfully logs in to Flex. At 10:10AM, the user again has a failed login attempt, their account would not be locked as it is not a consecutive failed login attempt.

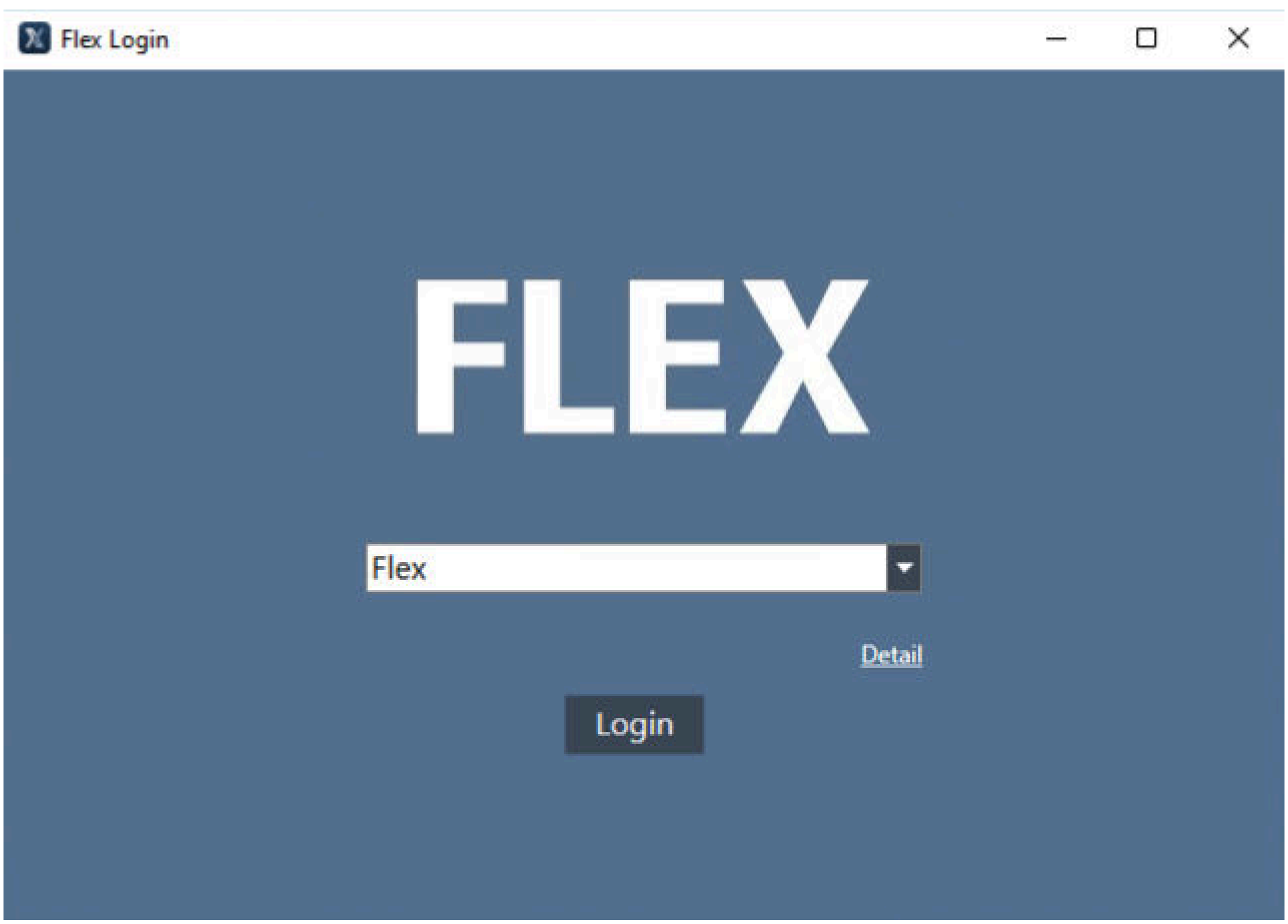
NOTE:
Administrators can configure the number of consecutive failed logins and the time threshold used, but CJIS Security Policy recommends 5 failed attempts within 15 minutes.

For more information about how to change system defaults, refer to "Modifying the System Defaults File" in the *Flex Administrator Manual*.

1.4.4
Updated Flex Login Screens

The Flex login screens were updated as part of an initiative in 2024.3. Now, when you log into Flex, the first thing you are asked is your server name.

Figure 7: Updated Flex Login Screen



When logging in, you can enter your username. Depending on agency settings, your login process may change. For more information on logging in to Flex with TOTP enabled, see the *Flex Records Management System (RMS) User Manual*.

1.4.5
Admin: Updated SMTP Server Options

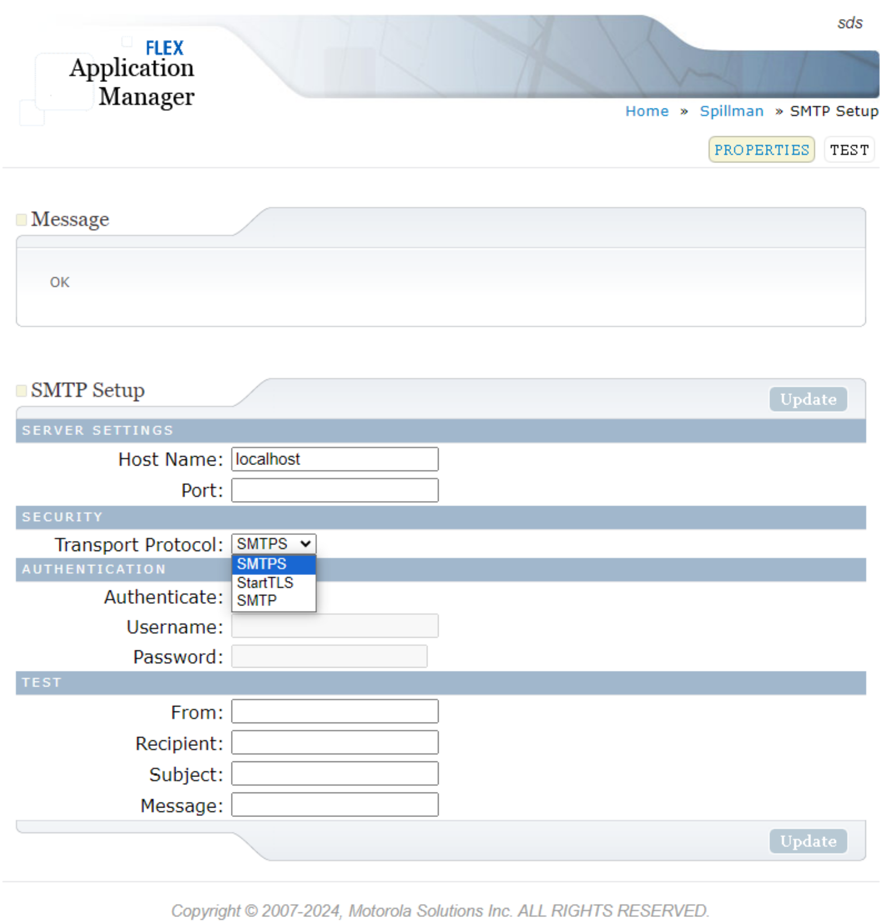
In the Flex Application Manager, the new **Transport Protocol** drop-down list box replaces the **Use SSL** option to expand the SMTP server connection options and enable connections via the TLS/StartTLS protocol.

Administrators can also test the SMTP configuration.

The **Security** setting of the **SMTP Setup** screen has three options:

- **SMTPS** – Simple Mail Transfer Protocol Secure secures email transmissions with encryption.
- **StartTLS** – Start TLS protocol command enables Flex servers to connect through TLS 1.2 and 1.3 if it is required by the SMTP relay provider. This selection supports email connections to Microsoft 365, Office 365, and Google Mail.
- **SMTP** – Basic SMTP with without encryption or other security measures.

Figure 8: New Transport Protocol Options



These options allow agency administrators to connect their Flex application to a preferred SMTP provider.

The new **Test** section enables administrators to test the email protocol configuration with the **From**, **Recipient**, **Subject**, and **Message** fields. The **Test** button a the top right of the screen launches the test on the **Transport Protocol** setting.

1.5 Records

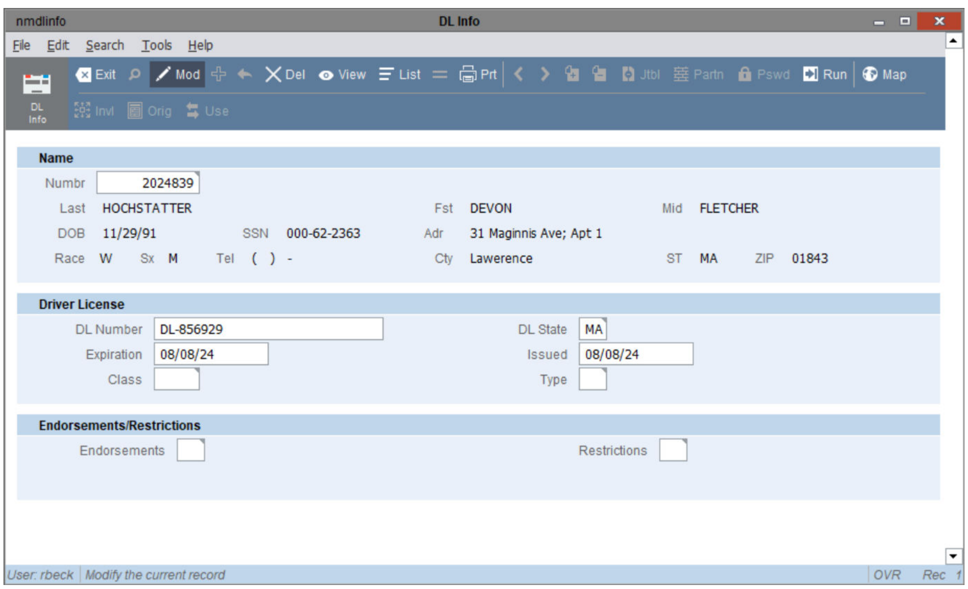
1.5.1 Added Drivers License Issued Date Field

As of the 2024.4 release, we added the **Issued Date** field to the following locations:

- **DL** tab of the **Add Name Record Mobile Names** screen
- **DL Info** screen (nmdlinfo)
- **Mobile Names** screen

This field provides a place to store the Driver's License Issued Date in Flex.

Figure 9: Issued Field on DL Info Screen



1.5.2 Added Incident Summary Field to Law Screens

We added an **Incident Summary** field to all law screens. Now, when an agency requires a summary of the incident, a field is available on part of the narrative section. This allows users to prepare public-facing summaries for media inquiries, as well as OPRA and FOIA requests.

We added the **Summary** field in the **Narrative** area of the **Law Incident** screen. It now displays on the following screens:

- **Law Incident** screen on Flex Desktop
- **Law Incident** screen on Flex Mobile
- Mobile Field Incident Report

We also added an **Add Summary** button to the **Mobile Law Incident** screen on Flex Mobile.

NOTE: Similar to Narratives, you can only add one Incident Summary per Incident.

You can add templates to the Summary field through the application cue card (apccard) setting. For more information about this process, see "Adding Application Cue Cards" in the *Flex Administrator Manual*.

1.5.2.1
Admin: Configuring the Incident Summary Setting

If you do not want an Incident **Summary** entry to be automatically added to the narrative section on the **Mobile Law Incident** screen, you can disable it from **adminutil**.

Procedure:

1. To open **adminutil** from the Flex command bar, enter `adminutil`
2. Navigate to **Module** → **Module.FR** → **Module.FR.AutoAddSummaryToIncident**.

Table 3: Module.FR.AutoAddSummaryToIncident Setting

Setting	Description
AutoAddSummaryToIn-cident	Determines if an empty summary record is automatically added to law incidents on the **Mobile Law Incident Edit** screen. If set to **TRUE**, an empty incident summary is automatically added to the narrative section on the **Mobile Incident Edit** screen, allowing the officer to enter a short incident summary. The **Add Summary** button is disabled because a summary is already present. There can only be one summary per incident. If set to **FALSE**, an empty incident summary is **NOT** automatically added to the narrative section on the **Mobile Incident Edit** screen. The **Add Summary** button is enabled on the **Mobile Incident Edit** screen. There can only be one summary per incident.

1.5.3
Cloud Integration of the Traffic Accident Table

We integrated the Traffic Accident table (acmain) into the Cloud, enhancing feature parity between Flex Insight and Multi-Agency Search in the Cloud. This enables crash records to be queried for services such as Multi-Agency Search and in the future, CommandCentral Reporting.

1.6
IBR

1.6.1
Enhancement Checkbox for Offenses and Victims

We enabled the ability for users to **NOT** send records to IBR using the **AllowSelectedOffenseVictimNotSendToIBR** setting that was documented in 2023.2 and 2024.2.

This setting is now available in 2024.1 Utah; 2024.2 Maine and Pennsylvania; 2024.4 North Carolina, Vermont, Arkansas, Mississippi, New Hampshire, New Mexico. This setting may become available for more agencies the future.

1.6.2

State-Specific Updates

The following are state-specific IBR updates:

Table 4: State-Specific IBR Updates

State	Description	Flex Version
TX, OR	New Feature that allows multiple offense codes per statute and ability to upload state spreadsheets to update tblaw.	2024.1
MS,NH, NM, NC, VT, AK, ID, USVI	Mutually exclusive / Lesser inclusive feature turned on for MS,NH, NM, NC, VT, AK, ID, and USVI.	2024.4
NV, AZ	UOF FBI Standard turned on for NV and AZ Allow collection of data but no reporting until states start collecting data.	2024.1
IA, IN, NE, CA, KS	Statute updates for IA, IN, NE, CA and KS	No version for these cloud updates

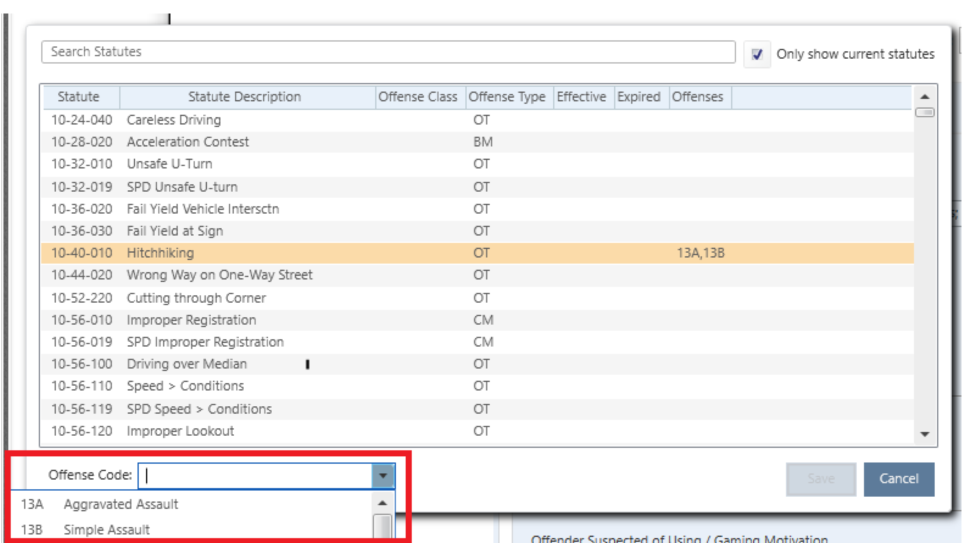
1.6.3

Statute Import Tool Update

As of the 2024.1 release, once enabled, Oregon and Texas users can more easily assign an offense code to a statute when a statute has multiple offense codes.

Previously, if a statue had multiple offenses, users had to manually enter the statute multiple times reflecting the different offense codes. Now, when a statute with multiple offense codes assigned to it is selected, the **Offense Code** drop-down box appears. Once expanded, users can select which offense and finalize their selection by clicking **Save**.

Figure 10: Offense Code Drop-down Menu



1.6.3.1

Updating Oregon IBR Statutes

You can update the statutes by using the IBR statute import tool.

Procedure:

1. Open the Flex webapp.
2. Click the **IBR Statute Import Tool** link.
3. Click **ORIBRProcessor**.

   The **ORIBRProcessor Properties** page opens.

4. Click on **Update Statutes**.
5. Click **Browse**.
6. Select the file from the state that you want to upload.
7. Click **Update Statutes**.
8. Review the changes.
9. To save changes, on the bottom, click **Submit**.

1.6.3.2

Updating Texas IBR Statutes

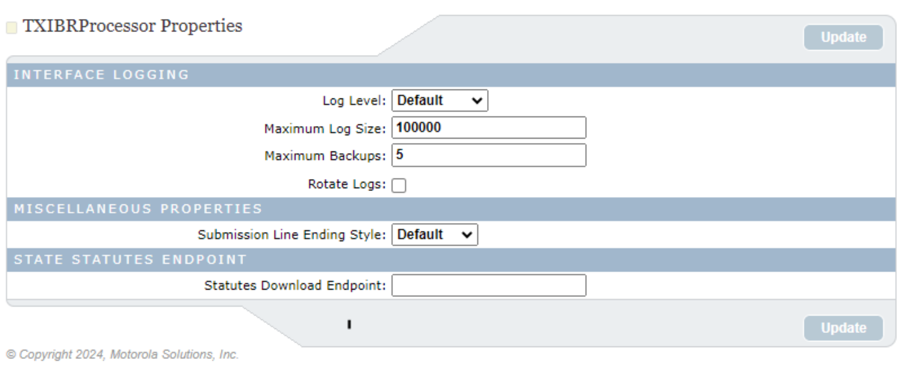
You can update the statutes by using the IBR statute import tool.

Procedure:

1. Open the Flex webapp.
2. Click the **IBR Statute Import Tool** link.
3. Click **TXIBRProcessor**.

   The **TXIBRProcessor Properties** page opens.

   Figure 11: TXIBRProcessor Properties Page

4. In the **Statutes Download Endpoint** field, enter `https://www.dps.texas.gov/ucr/documents/txucroffensecodetable.xlsx`
5. Click **Update**.

   Once the page is saved, you can download the statute page.

1.6.4
Use of Force in Arizona and Nevada

For Arizona and Nevada, you can now collect Use of Force reports through Sentryx Flex IBR.

In IBR, a Use of Force (UOF) incident consists of the following:

- Incident level UOF data element
- One or more Officers.
  - You can add officer roles as needed.
- One or more Subjects.
  - You can add subject roles as needed.

The UOF incident tab collects the incident level Use of Force Data elements and is on the Persons tab.

1.7
Jail

1.7.1
Flex Jail Scanner Application Login Update

For Flex versions 2024.3 and later, we have updated the login process for the Flex Jail Scanner application to reflect the updated Flex Login process and become compatible with Time-Based One-Time Passwords (TOTP).

If a Flex server is on version 2024.3 and above, users must first select their Flex server before they can enter their login credentials. The system then checks if TOTP is enabled for the server. For more information about TOTP, see Time Based One Time Password (TOTP) Integration on page 66.

If TOTP is enabled, users are prompted to either set up TOTP for the first time, or log in using an authenticator application.

NOTE: It is highly recommended that users setup TOTP for the first time using the Flex Desktop or Mobile application for ease of setup.

If TOTP is not enabled, you can enter your login credentials and click **Sign On**.

For more information on enabling TOTP and managing your agency's authenticated devices, see the *Flex Administrator Manual*.

1.7.1.1
Logging into the Flex Jail Scanner Application

Procedure:

To log into the Flex Jail Scanner Application, perform one of the following actions:

Table 5: TOTP Functionality

If...	Then
If your agency has not updated to the 2024.3+ release,	you will not be able to sign in or set up TOTP yet, but the login process has changed. **a.** On the Flex **Login** screen, select your Server and then press **Login**

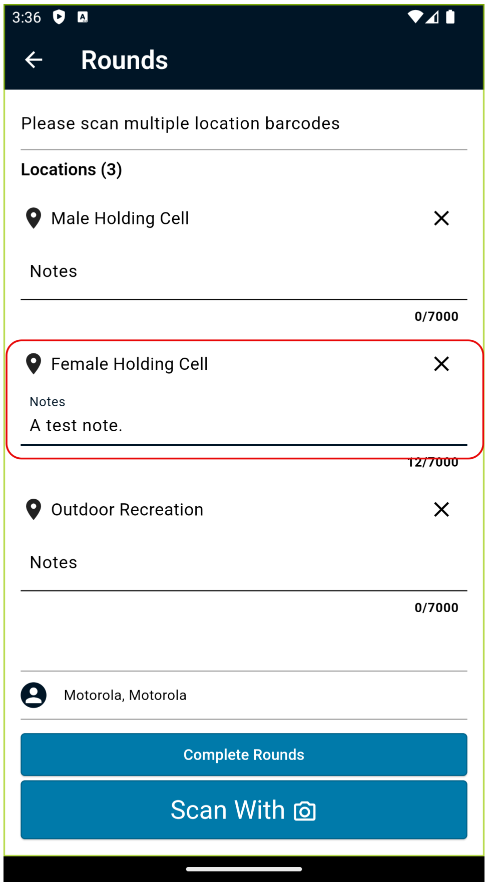
If...	Then
	b. In the **Username** field, enter your username. **c.** Press **Next**. **d.** In the **Password** field, enter your password. **e.** Press **Next**. **f.** Click **Continue to Flex**. **NOTE:** Once your agency updates to the 2024.3+ release, you can add TOTP authentication to Flex.
If you are logging in using your smartphone device for the first time after your agency has enabled TOTP,	we highly suggest that you attempt to sign in using the Flex Desktop application for ease of setting up TOTP.
If you are logging in after you have completed TOTP setup for your account,	complete the following steps: **a.** On the Flex **Login** screen, select your Server and then press Login **b.** In the **Username** field, enter your username. **c.** Press **Next**. **d.** In the **Password** field, enter your password. **e.** Press **Next**. **f.** Under the text stating `Enter the 6-digit code generated by your authentication app.`, enter the code that your authentication application displays for Flex. **g.** Press **Next**. **h.** Click **Continue to Flex**.

1.7.2
Flex Jail Scanner – Add Notes to Rounds

Users of the Flex Jail Scanner Application can now add notes for each location as they complete their round checks. The notes appear in the Flex Jail client.

After the Rounds feature opens in the Flex Jail app, a **Notes** field appears for each location barcode. An officer can enter a note for a location but is not required to do so. In the following example, a test note is placed in the **Female Holding Cell** location.

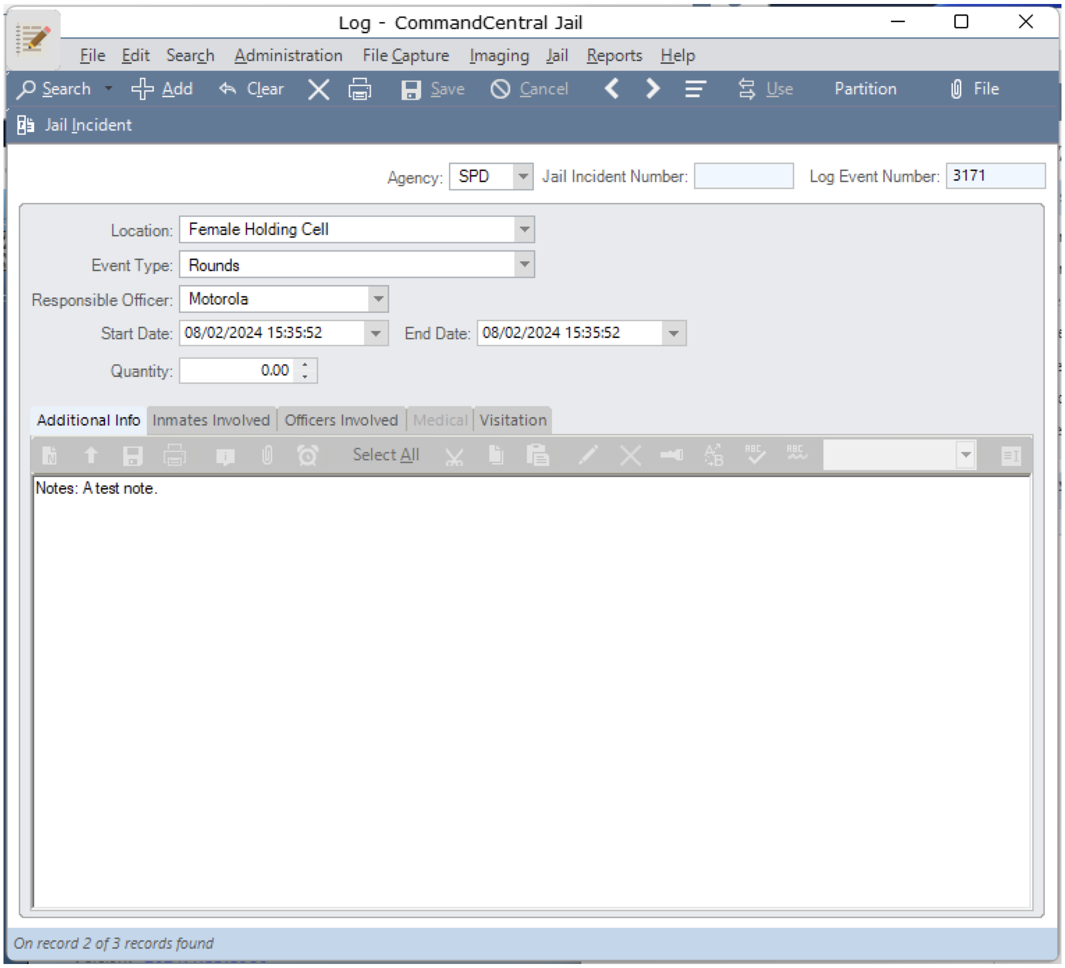
Figure 12: Flex Jail Scanner Application Rounds Notes



In the **Log** window, the Flex Client user can view all locations of completed rounds by filtering the **Event Type** parameter and selecting **Rounds**.

The **Additional Info** tab displays the note entered at the Flex Jail app for each location.

Figure 13: Flex Jail Client Application Rounds Additional Info Tab



1.7.3

Multiple Jails in P1 Booking Integration

As of the 2024.3 release, if enabled by administrators, users can select which jail they send bookings through the PremierOne to Flex Booking Integration.

The Multiple Jails feature allows for the destination Flex Jail to be selected on PremierOne at the moment of transferring the booking. For complete functionality, the PremierOne agency that is sending information to your agency must also have this update.

After this setting is enabled, an officer in PremierOne can select a destination agency without having to navigate and change settings on the P1BookingInterface **Configuration** screen.

For this functionality to be enabled, administrators must select the new **Enable Multiple Jails** check-box under the **Properties** screen for P1BookingInterface. This feature only functions when the booking direction is set to PremierOne sends bookings to Flex.

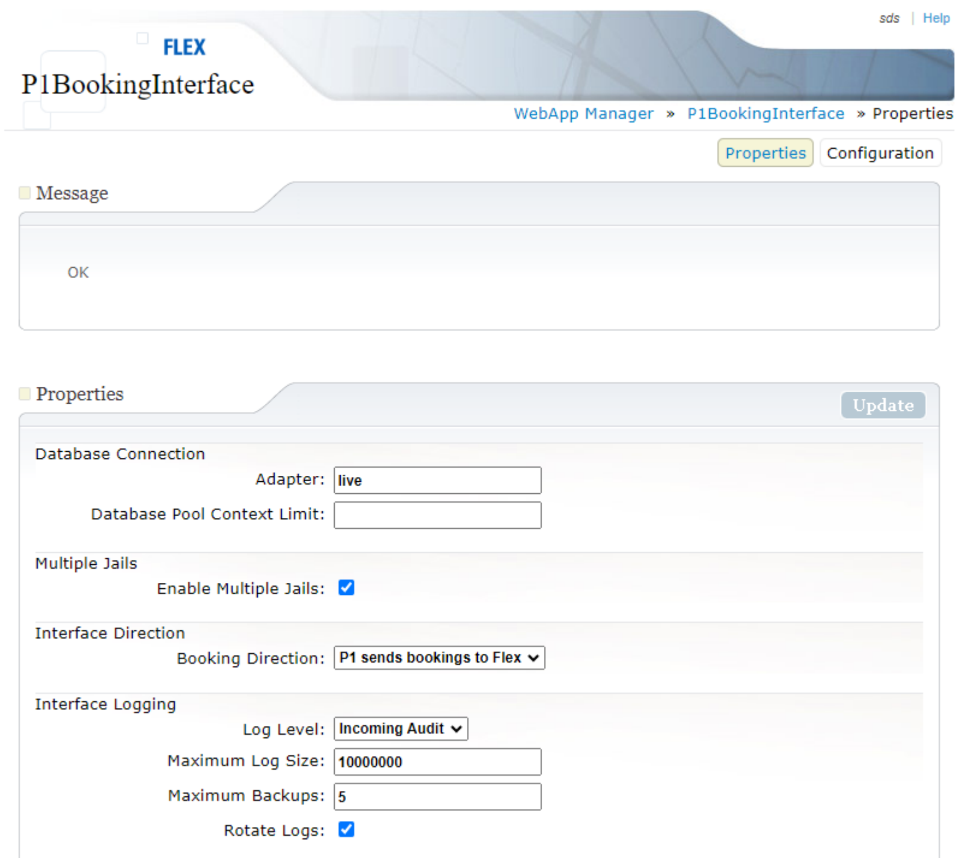
1.7.3.1 Enabling Multiple Jails in P1 Booking Integration

As of the 2024.3 release, the PremierOne to Flex Booking Integration supports agencies configured with more than one jail.

Procedure:

1. Open the Flex web application.
2. Click the **P1BookingInterface** link.
3. On the **Properties** screen, check the **Enable Multiple Jails** check-box.

   Figure 14: P1BookingInterface Properties Page

   If you already have the P1BookingInterface set up, this setting works when the booking direction is set to PremierOne sends bookings to Flex.
4. Click **Update**.
5. At the bottom of the screen, click the **Test** button.

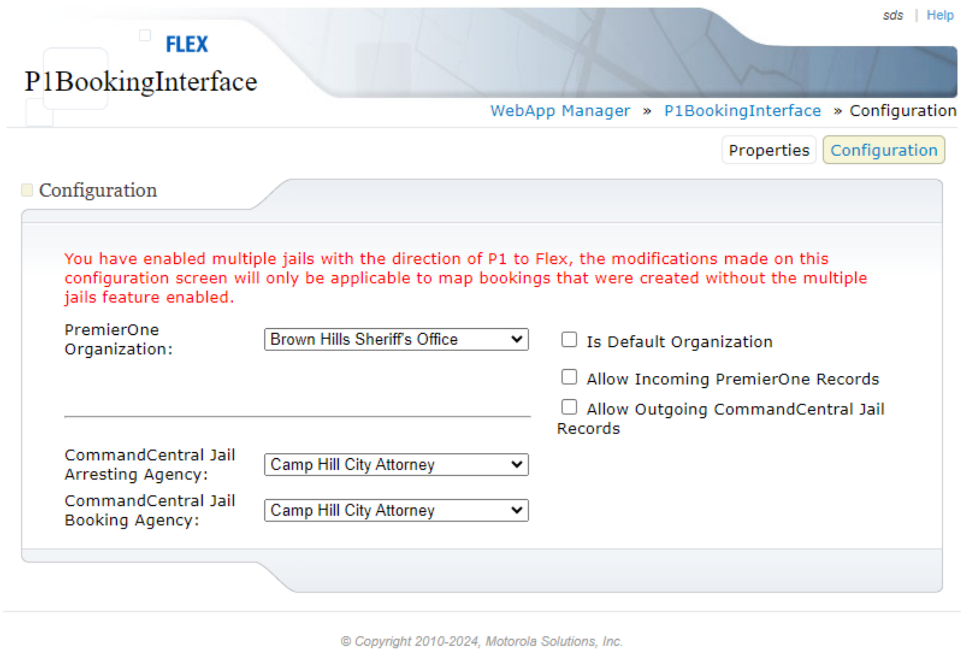
   If configured correctly, a `Authentication Successful!` message appears in green.

   If you go to **Configuration** screen after this setting is enabled, a message similar to the following appears:

```
You have enabled multiple jails with the direction of P1 to Flex, the
modifications made on this configuration screen will only be applicable to
map bookings that were created without the multiple jails feature enabled.
```

If you have multiple jails enabled for PremierOne to Flex and you change the information present on the **Configuration** screen, the changes made are only used for bookings created before you had multiple jails enabled.

Figure 15: P1BookingInterface Configuration Page



1.7.4
Other Enhancements

The following updates have also been completed for Flex Jail:

Table 6: Jail Enhancements

Description	Jail Version
Property bag locations and inmate number added to inmate list	2024.2
Expired flags showing on inmate list - fixed	2024.1

1.8 StateLink

1.8.1 State-Specific Updates

The following are state-specific updates:

Table 7: State-Specific Statelink Updates

State	Description	Version
AZ	NLETS Parsing Updates	2024.3
ID	DQ Nlets Region Codes Update	2024.2
	EM/EPO OLS Updates	2024.3
GA	GLEMS Migration	2024.4
FL	FDQ/DQ State Change/Updates	2024.1
	EMN State Change/Updates	
	EMJR State Change/Updates	
IA	IA TraCS Response Sharing	2024.4
CO	Vehicle Registration Import to Flex	2024.1
NV	Nevada StateLink 2.0	2024.1

1.9 Interfaces

This section lists the issues resolved for Interfaces.

Table 8: Interfaces Update Resolutions

Jira Ticket	Issue	Issue Resolved
CRJINTERFACE-910	Odyssey Warrant Bidirectional Failed to get Warrant. Unable to execute DEx query. The interface was not able to execute Dex query based on the list option selected in the drop down list.	Deploy the new interface `war` file and reload it.
CRJINTERFACE-895	NJCrashSubmission Fails State Validation - Missing Boxes 83-95 In the `XML` file. Some vehicles information were not addressed correctly	Update `war` file.
CRJINTERFACE-835	CitationInterface - CAPS - Arkansas eCite - ArkECiteWebService.java:119 - Citations were not pulling from the web service after the library update on the Flex side.	Deploy the new interface `war` file and reload it.

Jira Ticket	Issue	Issue Resolved
CRJINTERFACE-798	Odyssey Arrest Export TRN/TRS issue Unable to link Tyler ChargeID with Flex Offense.	The API request is now meets the customer needs.
CRJINTERFACE-781	Minnesota DataWorks Livescan referring to incorrect field.	Deploy the new Livescan3 interface `war` file and reload it.
CRJINTERFACE-780	Remove the Minnesota DataWorks Livescan standalone attribute from the xml header to facilitate the xml file submission to 3rd party.	Deploy the new Livescan3 interface `war` file and reload it.
CRJINTERFACE-776	TN Fusion Center No Incident only data and Arrest Official is not available Request for separate activity crime case for each offense and also for the officer name to be split into first and last name.	Deploy the new `war` file and reload the interface.
CRJINTERFACE-775	NJCrashSubmission Fails for NJCREDS submission at Null. Missing validation fields.	Implemented additional validations.
CRJINTERFACE-728	Null Field Errors (FBI / SSN) - Odyssey Arrest interface - Receiving API error for empty xml elements.	Deploy the new `war` file and reload it.
CRJINTERFACE-726	NJCrashSubmission Fails for Lat/Long and Other items during validation. Lat/Long, Total Killed, and Total Injured validation error.	Deploy the new `war` file and reload it.
CRJINTERFACE-699	Odyssey Arrest Export TRN/TRS issue. Arrest Export was not sending TRN and TRS fields due to lack of permissions on API call.	Implemented a new workflow that calls a specific API for the TRN and TRS. This specific API call should work for all customers without permission issues.
CRJINTERFACE-630	Swanson Interface not sending data. Soap requests were failing to send due to Soap action header missing in the request.	The soap action header was added in the request. Deploy the new interface war file and reload it.
CRJINTERFACE-348	NY TRACS ctmain.dtissue should be mapped from ArrestTransactionDate tag. Field was not populating in the Citation screen in Flex client.	Deploy the new interface `war` file and reload it.

1.9.1 GEARS Accident Import Update

As of the 2024.2 release, the GEARS Accident Import for Georgia agencies has been updated to take advantage of hybrid architecture. Agencies can once again bring their Accident data into Flex from the new GEARS system.

The existing legacy SFTP process used for extracting crash data from the GEARS and sending it back to the agency is being replaced by a web service utilizing an Application Programming Interface (API). The SFTP process is being retired to better align with data security measures that mitigate risk associated with file sharing. The new API method of data transfer will provide the agency with a more complete set of data and will provide greater data security.

The Hybrid Flex Adapter WAR file should be deployed on the Interfaces-Server Tomcat.

This interface contains applications running in the Cloud and On-premise:

Table 9: Cloud and On-premise Applications

Type	Description
Cloud	Services responsible for retrieving data from GEARS APIs, transforming and sending to OnPrem.
OnPrem	Component receives translated data from Cloud and imports it into Flex.

1.9.1.1 Admin: Managing On-Premise Settings for HybridFlexAdapter

Procedure:

1. Log into Tomcat Interface's server.
2. Deploy `HybridFlexAdapter` WAR file.
3. Configure the following settings:

Table 10: HybridFlexAdapter Fields

Field	Description
Adapter	Adapter name for the FLEX database
Username	Username for FLEX database
Password	Password for FLEX database
Temporary Folder	Folder to temporarily store the attachment files
IDM Server Port	Motorola Identity Management (IDM) server port
IDM Server Path	IDM server URL
Client Id	Client ID for querying IDM
Client Secret	Client Secret for querying IDM
SAS Service Hostname	Hostname for the SAS service
SAS Service Port	Port for the SAS service
SAS Service Base URL	Base URL for the SAS service
Log Level	Logging level for the interface
Maximum Log Size	Maximum number of logs that are stored
Maximum Backups	Maximum number of backups that are stored
Rotate Logs	Check-box, if selected, that allows logs to be rotated.

4. Click **Update**.

1.9.2

TN Fusion Interface

We created the new TN Fusion Interface which allows you to connect to the Tennessee Fusion system and submit incident information to the state.

You can use the TN Fusion Interface to collect and export data about an offender's arrest associated law incident. You can also use the interface to perform the following actions:

- Schedule the interface to automatically initiate data queries and exports to the third party within a set timeframe, ensuring that both new and altered data are regularly sent to the data warehouse.
- Use the interface to export data on the offenses related to an arrest, gathering the vital details required by the third party.
- Transform the data you retrieve from Data Exchange into the GJXDM format, which is compatible with the Fusion Center system's Webservice. This facilitates successful data uploads. Once in the correct format, you can send the GJXDM messages directly to the TN Fusion Center Webservice.
- Read the log on the **Logs** page of the interface web application.

Installation requires the same hardware and OS as other Flex products as well as the standard Flex software setup with the Sentryx Server and the Interfaces Server.

1.9.2.1

Admin: Installing the TN Fusion Interface

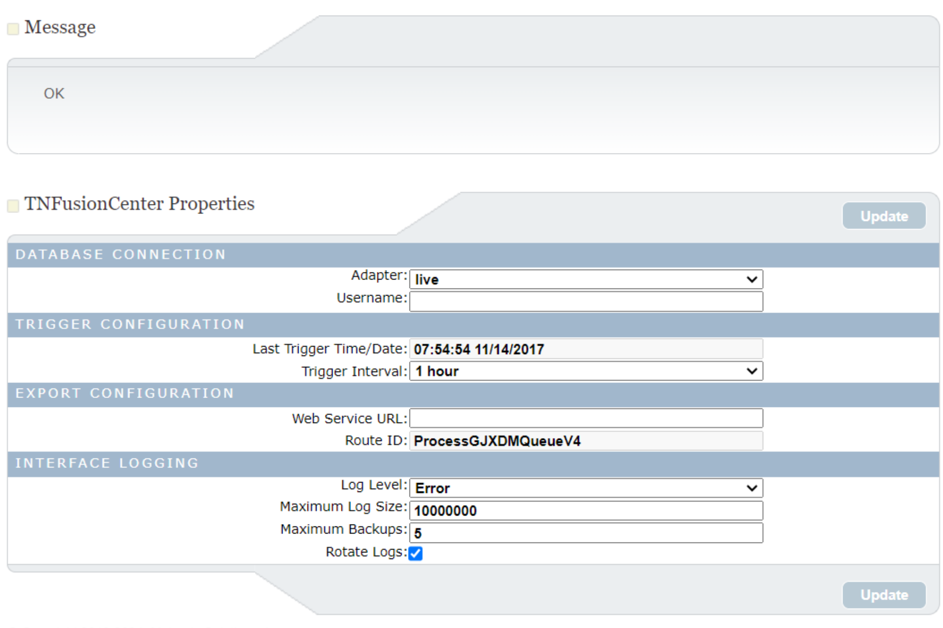
You must deploy the `.war` file of the interface on the Interfaces Server. You can do this through the Application Manager web application which is also typically deployed on the Interfaces Server.

Procedure:

1. Deploy the `TNFusionCenter.war` file directly from the application server.

   The webapp opens and displays the **Properties** page.

   Figure 16: TNFusionCenter Properties Page



2. Complete the following fields:

Table 11: TNFusionCenter Properties Fields

Field	Description
Adapter	The adapter to use for database access.
Username	The username a user uses to query and update database records.
Last Trigger Time/Date	The last time/date when the interface exported data successfully. Read-only field.
Trigger Interval	The interval that the interface triggers
Web Service URL	The URL to the TN Fusion Center Web Service (training Web Service URL https://www.tfctraining.tn.gov/LEIE/Service.asmx)
Route ID	The route ID was provided by the agency. Read-only field. The default value is `ProcessGJXDMQueueV4`
Log Level	The level of information to be stored in the log. The **Error** level provides the least information, while the **Debug** level provides the most.
Maximum Log Size	The maximum size, in megabytes (MB), that a log file can be before creating a new log. The default value is `10,000,000`
Maximum Backups	The maximum number of backup log files to keep. The default value is `5`
Rotate Logs	You can create a new log file when the maximum log size is reached by selecting this check box. This check box is selected by default.

3. Click **Update**,

NOTE:
If you make changes to this setting, you must restart the `.war` file.

You can update this `.war` file by redeploying the latest version.

1.10
Reports

1.10.1
New and Updated Reports

We added new reports, made enhancements to certain reports according to customer feedback, and eliminated errors that were reported to us by users.

Reports beginning with `rp` are accessible by users with appropriate sypriv privileges from the Flex command line by entering the file name without any extension. Example: `rpevchr`

Reports with file names the same as the screen names are accessible by clicking the **Print** button on the respective screens.

Any report with an `.x` extension is printed in a PDF format, and any report with an `.r` extension is printed in a fixed-width text format.

New Reports

- `rpjlasmt.q/.r1` - **Jail Assessment Audit report**
  - As a csv output.
- `rptrdatc.rm1` - **Maine Traffic Stop Report**
  - Report to be used for Maine Profiling Data Collection Law in State of Maine's required format.

Fixed/Updated Reports

- `lwmain.x1/.r1` - **Incident Report**
  - Added the Summary field from the Law screen.
- `rptrdatc.rpd3` - **North Carolina Traffic Stop Report**
  - Updated to reflect passenger info correctly.
- `rpjlbilld.x1` - **Detailed Multi Agency Billing**
  - Fixed query so that all bookings will show if multiple are present for the same inmate.
- `rpsldump` - **Dump System Log Records**
  - Added the uuid in the output per schema update.
- `rpcdanal.q` - **CAD Call Response Times**
  - Added instructions for using the csv format options.

1.11 Touch

1.11.1 Ability for Comments to Auto-Scroll

You can now toggle whether or not the comments on the Flex Touch **Calls** screen auto-scroll or not by using the **Auto-Scroll** toggle in the **Comments** section on the Flex Touch **Calls** screen.

This toggle allows you to prevent the comments area from automatically scrolling to focus on new comments as they are added. You can manage this functionality individually from within each call or you can set a default value of **On**/**Off** in the Flex Touch **Settings** screen.

Figure 17: Touch Screen with Auto-Scroll Toggle

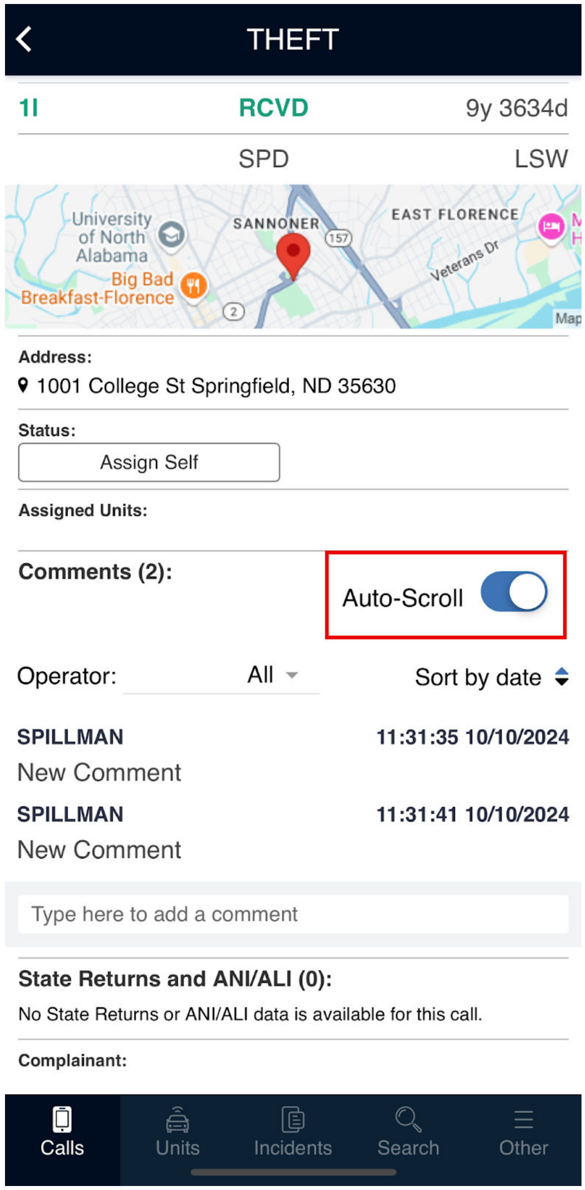


Figure 18: Touch Settings with Auto-Scroll Toggle

1.11.2 Display State Returns and ANI/ALI Data in Touch

If enabled by your agency, State Return data and ANI/ALI data associated with CAD calls now displays in the new **State Returns and ANI/ALI** section on the Flex Touch **Calls** screen.

In order for the data to display, the sypriv **touchstatereturn** must be enabled.

Chapter 2

Release 2024.3

This chapter presents changes made to Flex for the 2024.3 release.

2.1 CAD

2.1.1 CAD Calls: Ability to Quickly Add, List, and Remove Vehicles

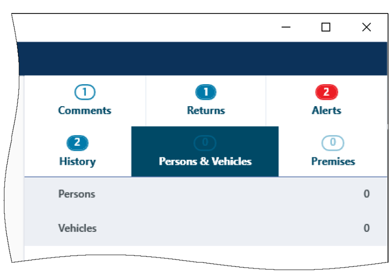
This feature reduces the time and number of keystrokes it takes to handle vehicles related to the incident, and is integrated with the similar ability for persons.

The feature requires the following settings in **adminutil**:

- `Module.CAD.Calltaking.RunNamesFromComments` set at the User level to `Yes`.
  The default value is `No`.
- `Module.StateLink.RemoveAddToCall` set at the World level to `False`.
  `False` is the default value.

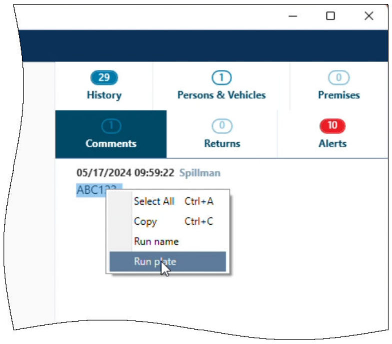
With these settings, after restarting the Flex client application, the **Manage a CAD Incident** screen has a new **Persons & Vehicles** tab.

Figure 19: Persons & Vehicles Tab



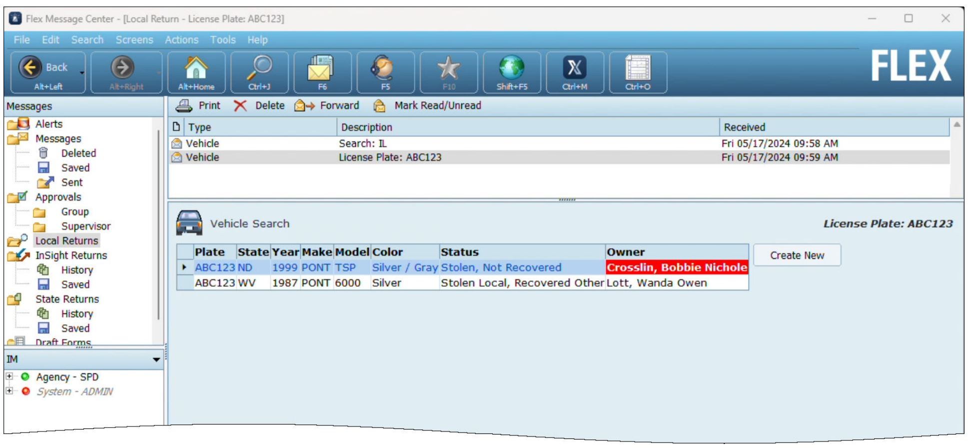
Users of the **Manage a CAD Incident** screen can now highlight person or vehicle information (license plate number) included in the text of a comment and use the right-click context menu to run a query. This way they do not need to go to the command line. The use of the feature for persons was described in Ability to Add Persons to Calls from Comments on page 81. The previous **Persons** tab is now changed to **Persons & Vehicles**. The following focuses on the feature for vehicles.

Figure 20: Run Plate Query Option



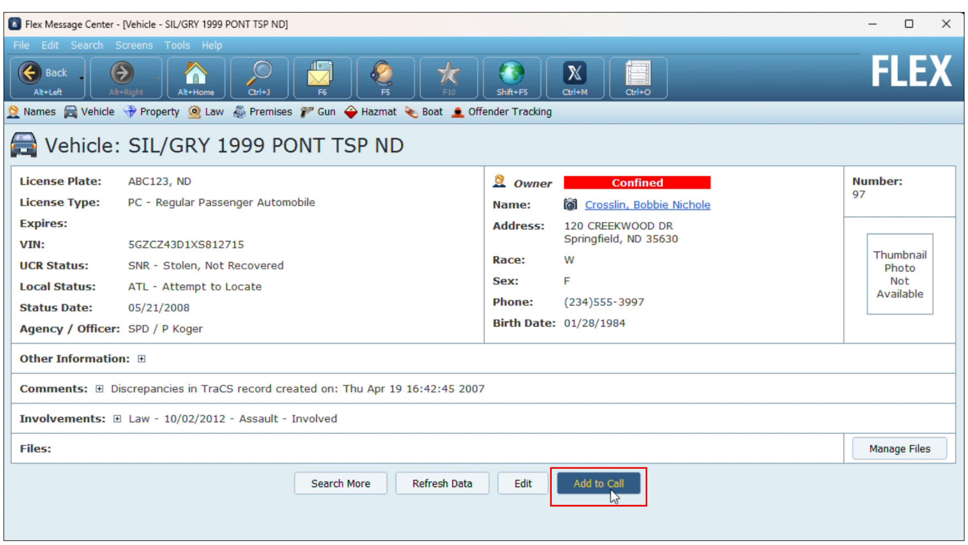
The query results appear in Flex Message Center under **Local Returns** or **State Returns**.

Figure 21: Vehicle Query Results



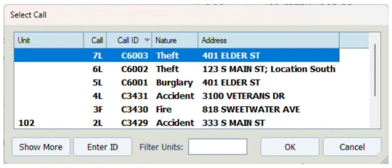
After clicking the right result, users can add the vehicle record to the CAD call by using the **Add to Call** button. The StateLink **Add Return** button is relabeled to **Add to Call**.

Figure 22: Add to Call Button



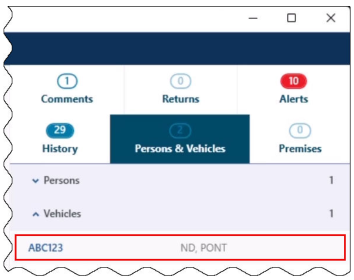
After clicking the **Add to Call** button, in the **Select Call** pop-up window, users should confirm the selection.

Figure 23: Call Selection Window



When confirmed, the query result is sent to the selected CAD call. On the CAD Incident screen, the number of involved persons and vehicles on the **Persons & Vehicles** tab increases. To view the information about the involved vehicles, users should click the **Persons & Vehicles** tab and then the **Vehicles** bar, which expands the list. Each item includes the plate number, state, and the make of the vehicle.

Figure 24: Vehicle Added to the Call

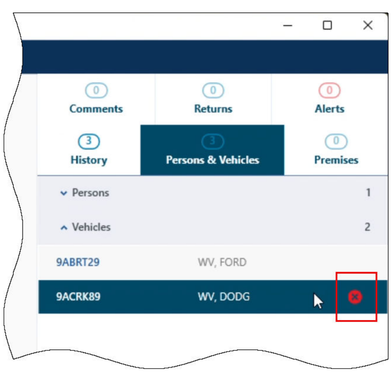


Users can display the whole information about the vehicle by double-clicking the plate number, which opens the vehicle record that is saved locally.

When more vehicles are entered in comments, they can be added in the same way. Both vehicles and persons can be searched directly in Flex Mobile and added to the call with that **Add to Call** button.

If any vehicle (or a person from the **Persons** list) has been added by mistake, users can remove the item from the list by hovering over it and clicking the **Delete** icon shown in the following figure. This operation must be confirmed in a pop-up dialog box.

Figure 25: Delete Icon on a Selected Item from the Vehicles List



2.1.2
Demographics Changes

We made the following changes to the Demographics for Traffic Stops based on the updated requirements from a number of states:

- On the **Traffic Stop** screen, we re-labeled the **Driver's Race** field to **Perceived Driver's Race** and the **Driver's Gender** field to the **Perceived Driver's Sex**.

  NOTE: The label for **Drivers Gender** has always used the **Sex** code table and stored the data in a field labeled, we have just updated the label to match its data.
- On the **Mobile Complete Call** and **Mobile Update Demographics** screens, we re-labeled the **Driver's Race** field to **Actual Driver's Race** and **Driver's Sex** field to **Actual Driver's Sex**
- Expanded the **Reason for Stop** (tbrcrs) field on the **Traffic Stop** and **Incident** screens
- Updated the TS command usage line to describe the fields as `{S/percievedRace perceivedSex stopReason}`
- Created a new code table (rctbrace) for the **Perceived Driver's Race** and **Actual Driver's Race** fields
- Created a new code table (rctbsex) for the **Perceived Driver's Sex** and **Actual Driver's Sex** fields

On the **Traffic Stop** screen, field labels and the 10 code origin table were updated in the following ways:

Table 12: Traffic Stop Screen Changes

Previous Field Name	Updated Field Name	New Table
Driver’s Race	**Perceived Driver's Race**	rctbrace
Driver's Gender	**Perceived Driver's Sex**	rctbsex

We updated the Reason for stop field to adhere to the changes that were made to the 10 code table tbrcrs:

Table 13: Reason for Stop Field Changes

Field	Change
Contact Abbreviation	Expanded field from 4 to 20 character limit
Contact Description	Expanded field from 30 to 100 character limit

2.1.3
LO Command Removal

The LO CAD command is no longer supported as of the Flex CAD 2024.3 release.

The command allowed new dispatchers to log on to CAD without the current dispatcher logging off the software in urgent situations, such as during a busy shift change. Now, dispatchers can only log on as the sole user.

2.2 GeoValidation/Mapping/Quickest Route

2.2.1 ArcGIS Pro 3 Support

Flex now supports ArcGIS Pro 3.3.

IMPORTANT: Updating from ArcGIS Desktop to ArcGIS Pro is a major update, which requires models and locators to be rebuilt. Please review the *Flex Hardware and System Requirements* for more information and contact your administrator or Motorola Representative about updating to ArcGIS Pro.

ArcGIS Server 10.9.1 is compatible with ArcGIS Desktop 10.8.2, ArcGIS Pro 2.9, and ArcGIS Pro 3.3. ArcGIS Server 10.9.1 is the last version to support ArcGIS Desktop.

Features in ArcGIS Pro 3.3 that require a newer ArcGIS server version than 10.9.1 will not work until a newer version of ArcGIS is supported by Flex.

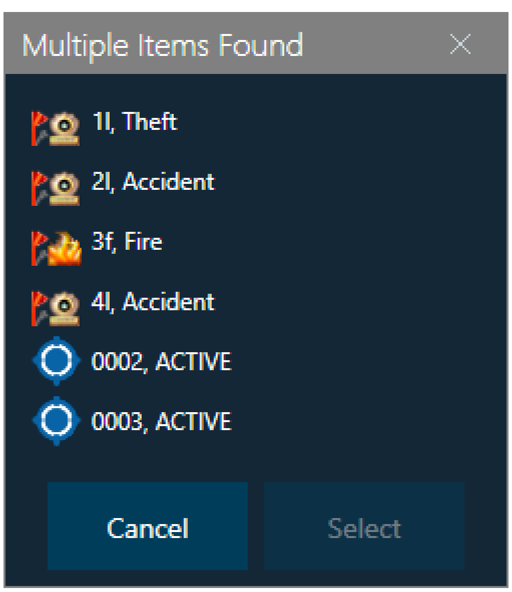
In addition, ArcGIS Pro 2.9 will be retired by ESRI on June 1, 2025.

2.2.2 Mapping Updates

As of the 2024.3 release, we made the following changes to Flex Mobile Map:

- The sidebar now uses traditional collapse and expand functionality. It stays expanded or collapsed until toggled. You can collapse or expand the sidebar by clicking any of the icons on the sidebar that would otherwise expand it.
- When you select an option to expand or collapse the sidebar, the whole map and navigation now shifts over. This prevents the covering of vital data. The state of the sidebar is now saved to the client.
- You can now show and hide both incident and unit labels and icons.
- You can now display a list of the nearby incidents and units in an area of the map with many incident and unit overlapping icons.

Figure 26: List of Multiple Incidents and Units



2.3 Hub/Platform

2.3.1 Time Based One Time Password (TOTP) Integration

As of the 2024.3 release, Flex now supports Time-Based One-Time Passwords (TOTP) for agencies that want or need to enable two-factor authentication at login. Authentication applications that have been tested to work with Flex are listed below.

TOTP functions on the Flex Desktop, Flex Mobile/Message Center client, Flex Touch, Flex Jail Scanner, and the Flex Web Application Admin. TOTP will be coming to the Flex Evidence Scanner app by Q4 2024, it is suggested to deactivate TOTP for users that use the Flex Evidence Scanner until this feature is available.

Agencies and admins can turn TOTP on or off using the new adminutil **Module.MFA.TOTP** setting. Once this setting is set to **TRUE**, no other action is required to enable this feature. With this setting enabled, administrators can add, update, and remove authenticated devices for their agency/agencies using the Login Management webapp.

TOTP can be enabled per agency or for all users on a Flex server. Once TOTP is enabled, users must add an authenticator device to their account the next time they log in. This can be done by scanning a QR code in the authentication application. Every subsequent login requires them to verify their username and password with a TOTP code.

TOTP Setting Management

Once TOTP is enabled, in the **Help** menu of the Flex desktop and mobile clients:

- Administrators can add, update, and remove authenticated devices for other users from the **Authentication Management** option.
- Users can manage their own devices from the **Authentication Management** option in the Flex desktop and mobile **Help** menu.

Motorola has tested the following Authenticator apps with Flex TOTP. This list is not exhaustive and Motorola does not suggest one Authenticator app over another.

- Microsoft Authenticator
- Google Authenticator
- Okta Verify
- LastPass Authenticator
- Duo Mobile (Cisco)
- Twilio Authy Authenticator

2.3.2 Flex Remote Support Link in Flex Help Menus

A link to Remote Support is now included in the Flex Help menus. Flex users can now quickly and easily access the web portal for remote support through the respective Help menu in Flex Desktop, Flex Mobile, or Flex Jail screens without having to remember or manually type in the URL for Remote Support.

NOTE: This link should only be used when you are on an active support call with Motorola Technical Support and have been given an active session code from the support team.

Figure 27: Link to Remote Help in the Flex Desktop Application

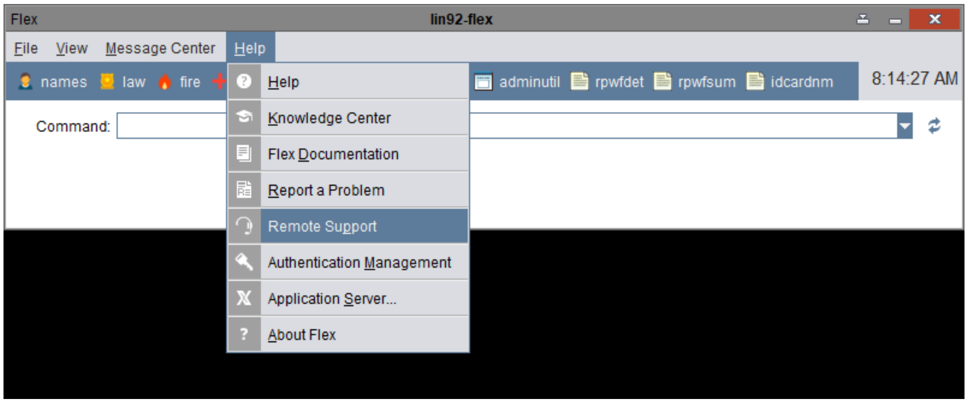


Figure 28: Link to Remote Help in the Flex Mobile Application

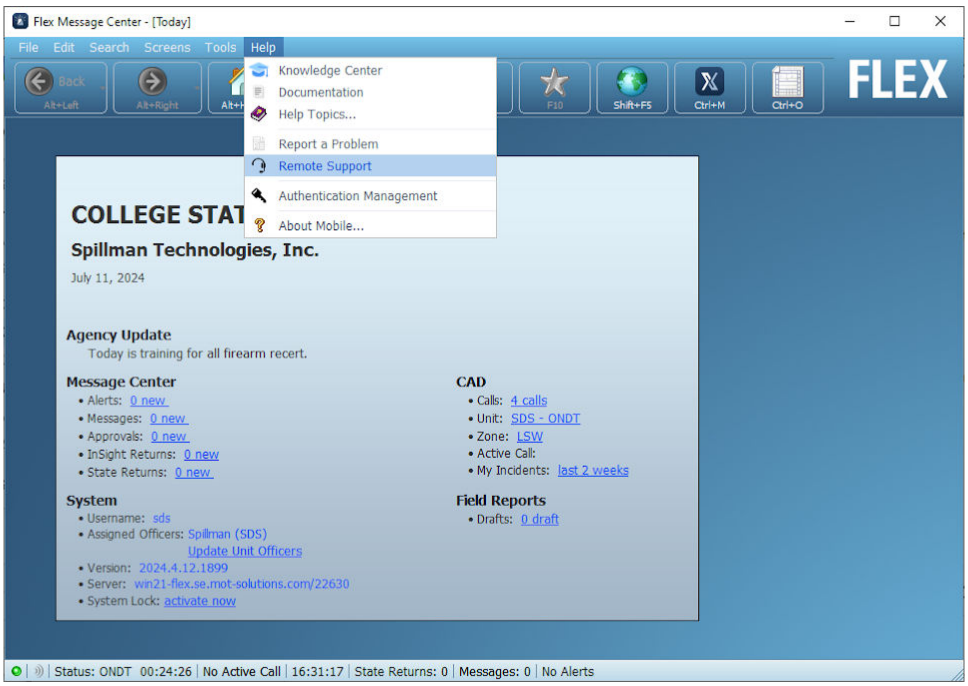


Figure 29: Link to Remote Help in the Flex Jail Application

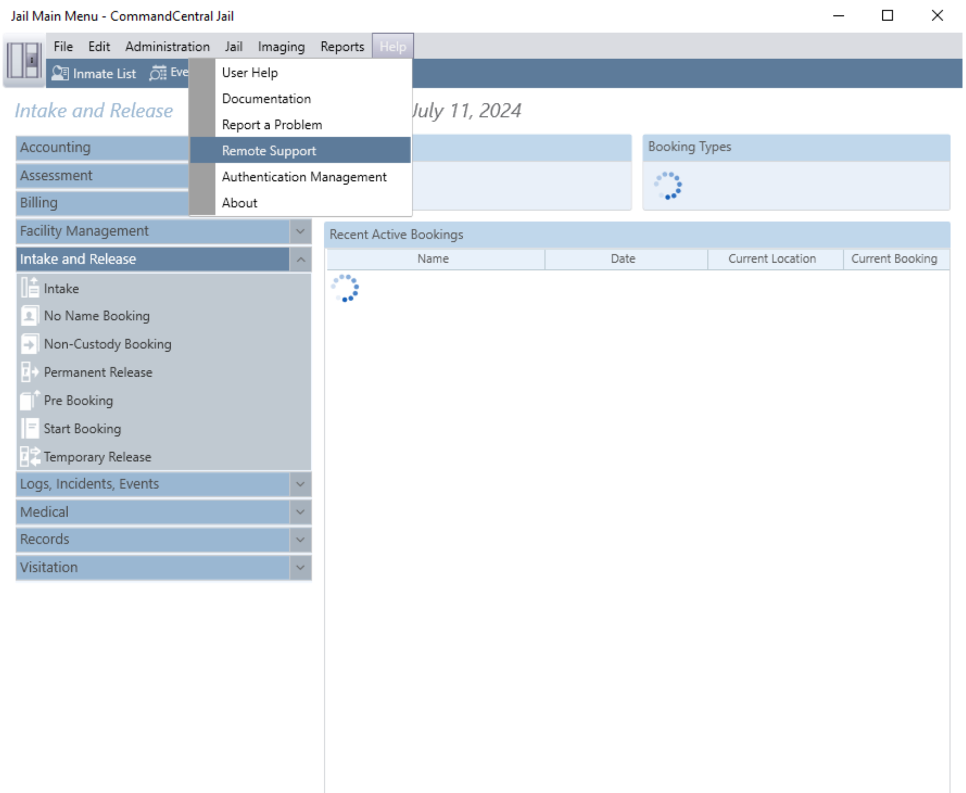
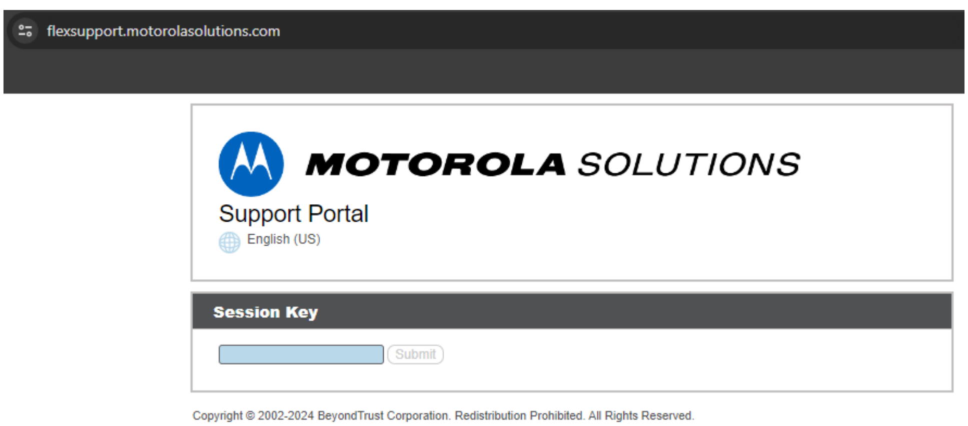


Figure 30: Flex Remote Support Portal



2.4
IBR

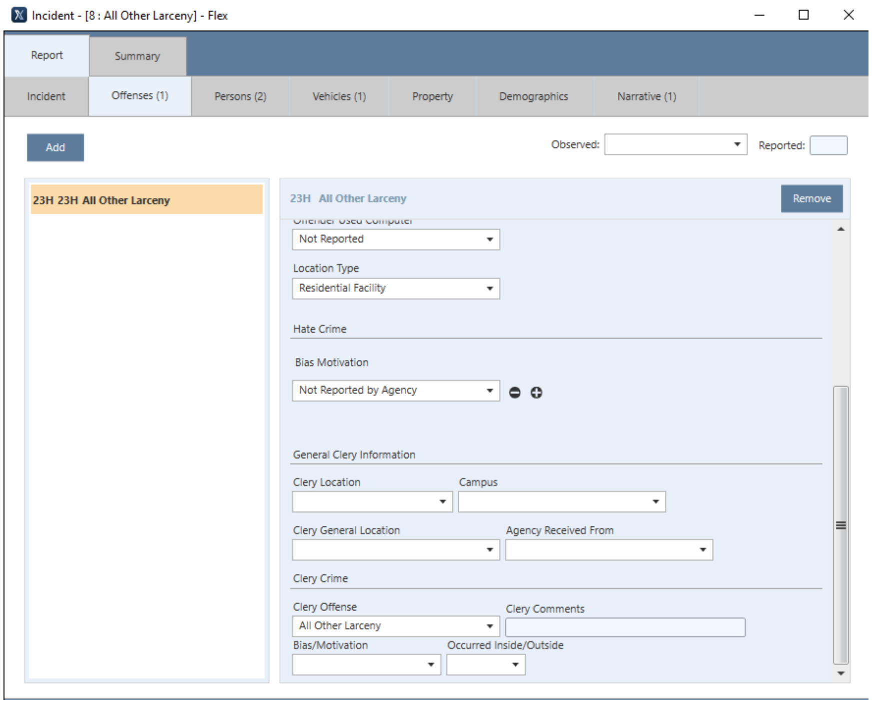
2.4.1
Clery Reporting Updates

We have implemented the following improvements for Clery reports:

- We added a Clery Offense drop-down menu that allows users to record if they are reporting that offense.

- We added a **Clery Explanation** text box next to the Clery offense so that users can explain if they modify the offense for Clery.

Figure 31: Clery Offense Information



2.4.2
State-Specific Updates

The following are state-specific IBR updates:

Table 14: State-Specific IBR Updates

State	Description	Flex Version
Nevada	Improved statute update tool	2024.1
Illinois	Statute updates	2024.1
New Jersey	Domestic Violence Time Spent - added drop downs to calculate formula	2024.1
All	Clery – Added ability to add notes and change offense codes	2024.1

2.4.3
More Verbose IBR Server Errors

We enhanced some of the IBR Server Errors. Now the Server Error message draws from the XXIBRProcessor.log and lists the specific error without the need for hovering.

For example, if an agency code is missing, you will see a message similar to the following:

```
java.lang.IllegalArgumentException: Agency field on the incident is invalid for
IBR, please update it on the incident or create an IBR Agency record for it from
the apagncy screen.
```

2.5
Jail

2.5.1
eSign for Incident Report and Releases

Flex Jail now includes the ability to use eSign for the following types of reports:

- Medical Screenings
- Assessment Report
- Hold Harmless Agreement

2.5.2
Jail Scanner Updates

We renamed the CommandCentral Jail Barcode Scanning mobile app to Flex Jail Scanner.

We added the following updates:

- A lock icon in the upper right corner to visually indicate if your connection is encrypted or unencrypted. Note that this does not take into consideration any encryption that occurs through a VPN tunnel.
- An easier to understand error message that appears if the BarcodeScanner webapp is not deployed or activated on your server.
- The server options screen automatically defaults to the standard encrypted port for the barcode scanner application.
- By default, the application will attempt to connect through an encrypted connection and if that fails, it will automatically fall back to an unencrypted connection.

NOTE: We will remove the ability to connect through an unencrypted connection in a future release.

We rewrote the Flex Jail Scanner App from the ground up. It now resolves some functional/foundational issues, preventing them from occurring in the future.

We have resolved the following issues:

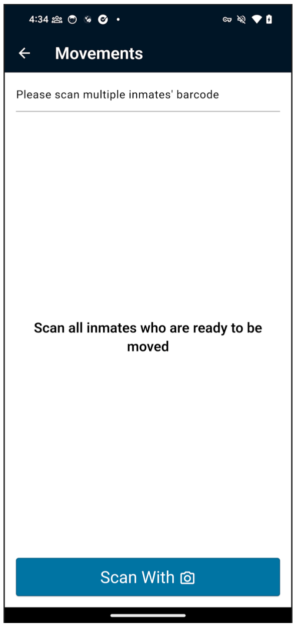
- If you press a button in the UI multiple times, the action will not be re-performed without ensuring that the first action was completed.
- Better performance of caching and uploading data from the app when it is offline.

2.5.3
Camera Scanner Feature

The Camera Scanner feature in the Flex Jail Scanner mobile app enables users to scan barcodes by using their Android smartphones running this application, eliminating the need for dedicated barcode scanners.

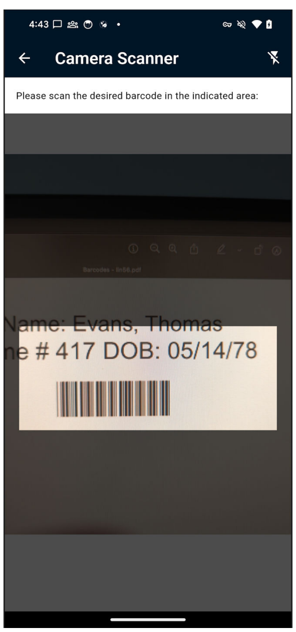
The **Movements**, **Cell Check**, and **Rounds** screens on your compatible Android smartphone will include the **Scan With** tab with a camera symbol.

Figure 32: Scan With Tab with a Camera Symbol on the Movements Screen



To scan an inmate barcode, you should tap the **Scan With** tab and point your phone's camera at that barcode.

Figure 33: Barcode in the Viewing Area



When the barcode is in the viewing area of the screen and is recognized, you will immediately get a confirmation and the inmate name will appear on the screen.

Figure 34: Confirmation of Successful Barcode Scanning

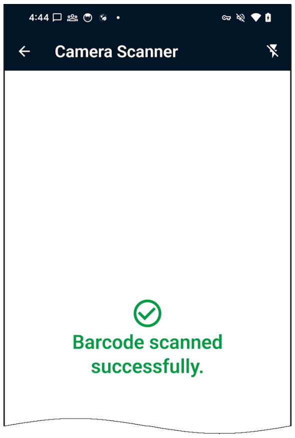
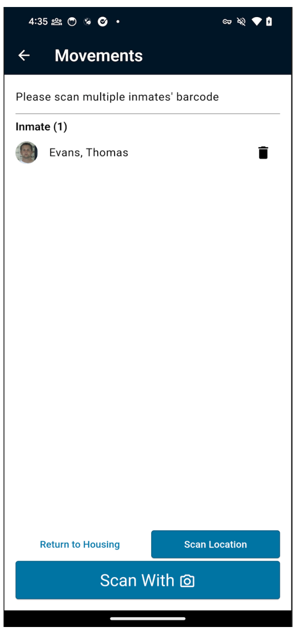


Figure 35: Scanning Result on the Movements Screen



Similarly, you can scan barcodes of other inmates or locations, in any of the **Movements**, **Cell Check**, and **Rounds** screens.

2.6 Reports

2.6.1 New and Updated Reports

We added new reports, made enhancements to certain reports according to customer feedback, and eliminated errors that were reported to us by users.

Reports beginning with `rp` are accessible by users with appropriate sypriv privileges from the Flex command line by entering the file name without any extension. Example: `rpevchr`

Reports with file names the same as the screen names are accessible by clicking the **Print** button on the respective screens.

Any report with an `.x` extension is printed in a PDF format, and any report with an `.r` extension is printed in a fixed-width text format.

New Reports

- `evtblctn.x1` – **Evidence Location barcode label**
  - Users will now be able to print evidence location barcodes directly from the **evtblctn** table
- `rpjltor.x2` – **Total Offenses Report, by Officer with Statute**
  - Added Arrestee Information
- `rpjltor.x5` – **Total Offenses Report, by Officer with Crime Class**
  - Added Crime Classification
- `rpnmalrt.x1` – **Name Alert Summary Report, by Code, Name Number**
  - x1 - Name alerts - namerep menu
- `rpnmcsr.x1` – **Critical Notices Summary Report, by Code, Name No**
  - Critical Notices Summary Report, Expiring Within 30 days

Updated Reports

- `rpcdanal.rems` – **EMS Incident Response Time Analysis**
  - Updated unit links
- `rpcdanal.rfir` – **Fire Incident Response Time Analysis**
  - Updated unit links
- `rpcdavrp.r3` – **CAD Average Response Times Detail**
  - Corrected column totals and headers
- `rpcdavrp.x3` – **CAD Average Response Times Detail**
  - Corrected column totals and headers
- `rpevch.r1` – **Property Inventory Report**
  - Added new section with evidence item specifics
- `rrevchr.x1` – **Property Inventory Report**
  - Added new section with evidence item specifics
- `rptdatc.rpd3` – **North Carolina Stop Report Data Export**
  - Final version

2.7
Records

2.7.1
Demographics Changes

We made the following changes to the **Demographics Summary** (rcmain) and Mobile **Demographics** screens that apply to Mobile and Desktop:

New Fields and Reorganization

- Added **Perceived Ethnicity**, **Perceived Color**, and **Perceived Gender** fields to the **Demographics Summary** (rcmain) and **Mobile Demographics** screen
- Reorganized **Demographics** area fields to group together perceived and actual demographics

NOTE: Actual Drivers Color will be available in 2024.4

Increased Character Limits

Increased the character limits for the following fields on the **Demographics Summary** screens and their accompanying code tables to enable agencies to conform with state guidelines.

Table 15: Demographic Summary Module Field Changes

Area of Demographic Summary	Field	Change
Reason for Stop	rcreasdl.abbr	Expanded to 20
	tbrcshbs.code	Expanded to 10
	tbrcshbs.descrpt	Expanded to 100
Result of Stop	tbrcoc.abbr	Expanded to 10
	tbrcoc.desc	Expanded to 100
	rcocdl.abbr	Expanded to 10
Citation/Warning	tbrcctwn.code	Expanded to 10
	tbrcctwn.descrpt	Expanded to 100
	rccitwrn.citwrn	Expanded to 10
Basis for Search	tbrcshbs.code	Expanded to 10
	tbrcshbs.descrpt	Expanded to 100
	rcsrchbs.basis	Expanded to 10
Arrest Based On	tbrcarbs.code	Expanded to 100
	tbrcarbs.descrpt	Expanded to 100
	rcarstbs.arstrsn	Expanded to 10
Type of Stop	tbrcstop.code	Expanded to 10
	tbrcstop.descrpt	Expanded to 100
	rcmain.stoptyp	Expanded to 10
Passenger / Group Member	tbrcpass.abbr	Expanded to 10

Area of Demographic Summary	Field	Change
	tbrcpass.desc	Expanded to 100
	rcpassdl.abbr	Expanded to 10
Violations Observed	rcvioobs.action	Expanded to 10

Created Demographic Summary-specific Code Tables

Created Demographic Summary-specific code tables for sex, ethnicity, gender, race and color so that users can choose from specific codes as per their state's traffic stop reporting requirements that may differ from normal Federal NCIC or State's IBR code tables, Please note that data from existing Demographic Summary records will be automatically migrated to the new code tables.

By default, we are automatically populating the new demographic summary specific code tables with values from the existing code tables. It is up to your SAA to modify these new code-tables for your agency's needs.

The new code tables are as follows:

Table 16: Demographic Summary-Specific Code Tables

Code Table	Description
rctbrace	Demographics Race
rctbsex	Demographics Sex
rctbclor	Demographics Color
rctbgen	Demographics Gender
rctbethn	Demographics Ethnicity

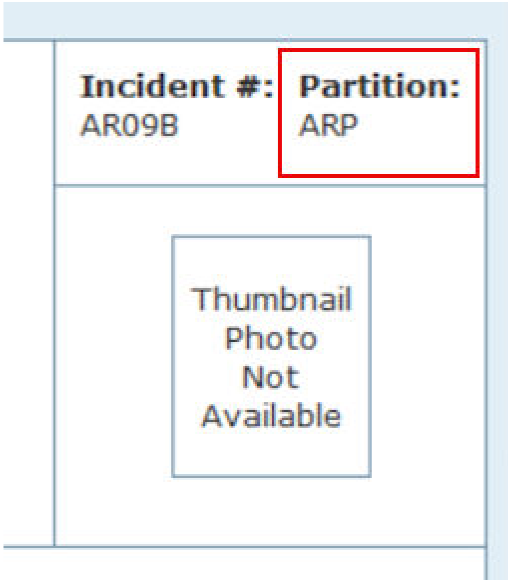
2.7.2
Display Partition Information on Mobile

The **Mobile Law** screen now displays a record's partition, allowing users to quickly determine whether or not a given record is in a partition.

Partitions now functions in the following ways:

- If a partition exists on a given law incident record, the **Mobile Law** screen displays the partition
- If no partition exists, the **Mobile Law** screen displays the **Partition** label and it is blank

Figure 36: Partition Information on Mobile



2.7.3
File Capture Screen Enhancements

We completed the following enhancements for the **File Capture** screen, in three areas.

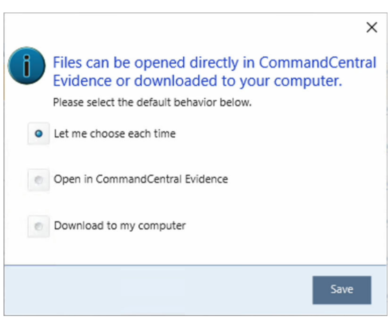
2.7.3.1
Ability to Open Files Directly in CommandCentral Evidence

For agencies that are using CommandCentral Evidence, a records clerk or patrol officer has the ability to open digital files directly in CommandCentral Evidence without having to download the file to their computer.

- A new `Module.FileCapture.downloadBehavior` adminutil setting allows agencies to control how users open files by allowing users to choose their preference, or forcing users to either download files to their computer or open them directly in CommandCentral Evidence.

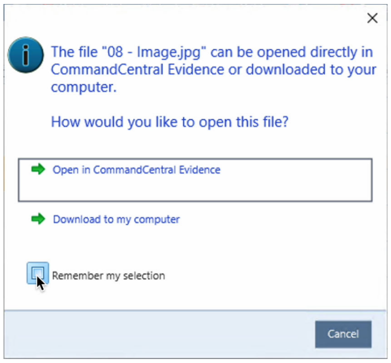
  For more information, see the *Flex Administrator Manual*.
- Users who are allowed to choose their preference have the ability to remember their preferred choice by selecting and saving the appropriate option (**Let me choose each time**, **Open in CommandCentral Evidence**, or **Download to my computer**).

  Figure 37: Default Behavior Options



When users choose the **Let me choose each time** option and do not want to manually select an option each time, they can update the default behavior by double-clicking a file from the **File Capture** screen, selecting the preferred choice, and remembering it.

Figure 38: File Opening Options



For more information, see the *Records Management System (RMS) User Manual*.

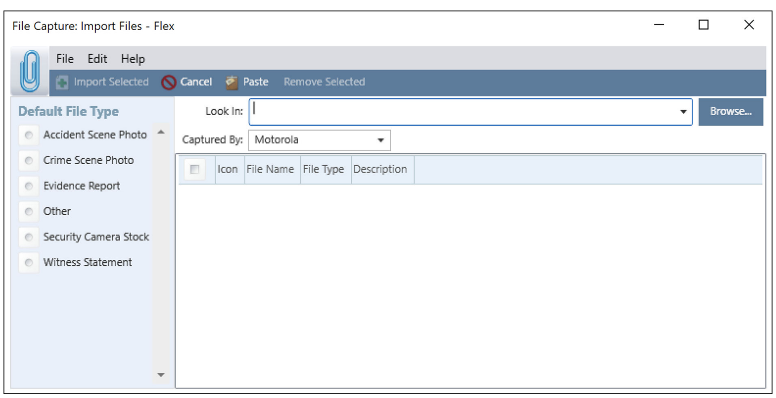
2.7.3.2

Quick Import Optionality

Thanks to customer feedback, we have created a new adminutil setting.

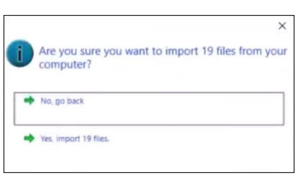
This `Module.FileCapture.EnableQuickImport` adminutil setting allows agencies to hide the **Quick Import** button from the **Import Files** screen by selecting the `False` value. Without that button, the batch import of multiple files by default is not available, and users should consciously choose only the required ones. By default, the `Module.FileCapture.EnableQuickImport` setting is set to `True`.

Figure 39: File Capture Screen Without the Quick Import Button



If the **Quick Import** button is not hidden and users click that button and then the **Import Selected** button, a pop-up dialog warns them about the number of files they are going to import.

Figure 40: Import Confirmation Dialog



If users quickly press ENTER on their keyboard while the warning message is shown, they select the first `No, go back` option, so that no file is imported. To import only the required ones, users should deselect unnecessary files from the whole list, click the **Import Selected** button again, and confirm the import of the files that remained selected.

For more information, see the *Records Management System (RMS) User Manual*.

2.7.3.3 Retroactively Populated File Capture Fields

Now when opening the **File Capture** screen, the new fields recently added (`CreatedTime`, `CapturedBy`, `Retention`, and `Storage Location`) will now be retroactively populated for files that existed prior to us adding these additional columns.

2.8 StateLink

2.8.1 State Specific Updates

The following are state-specific updates:

Table 17: State-Specific Updates

State	Description	Version
Oregon	Oregon StateLink 2.0	2024.1

2.9 Touch

2.9.1 TOTP Integration for Flex Touch

As of the 2024.3 release, Flex now supports Time-Based One-Time Passwords (TOTP) for agencies that want or need to enable two-factor authentication at login. Authentication applications that are compatible with Flex for TOTP include Google Authenticator, Microsoft Authenticator, and other apps that follow the same standard as those two.

For more information about authenticator applications see Time Based One Time Password (TOTP) Integration on page 66.

Chapter 3

Release 2024.2

This chapter presents changes made to Flex for the 2024.2 release.

3.1 Security

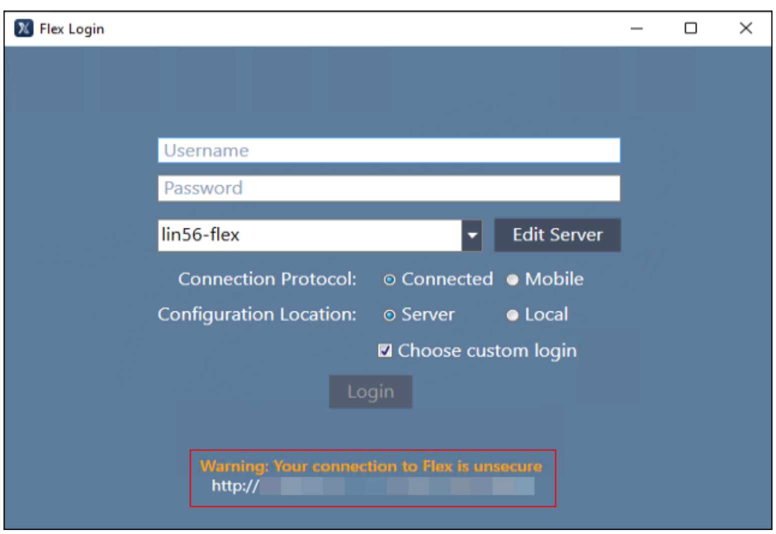
3.1.1 Admin: Security Enhancements

The Flex login security process was enhanced during the 2024.2 release by implementing the following updates:

- If SSL certificate validation cannot be verified, the Flex Client login for both Mobile and desktop fails. This action is taken to ensure all Flex data is encrypted in transit.
- When the connection to Flex is not secure and if encryption is not checked off in the connection settings, a warning message now appears on the Flex Login screen and notifies you of this.
- Administrators can now use Motorola Flex CertCheckerUtil, a lightweight script that checks the integrity of your SSL certificate and network before updating Flex to 2024.2+.

  NOTE: The CertCheckerUtil script is not intended to be run on servers. If it is run on servers, it will provide incorrect results.

Figure 41: Unsecured Flex Login



3.1.1.1
Admin: Motorola Flex CertCheckerUtil

As of the 2024.2 release, we are distributing a powershell script which verifies the integrity of your SSL certificate and network configuration, called CertCheckerUtil.

NOTE: The CertCheckerUtil is not intended to be run on Windows Servers, only Windows Clients. If CertCheckerUtil is run on Windows Servers, it displays incorrect results.

CertCheckerUtil is a lightweight script that can be used to check the integrity of your SSL certificate and network before updating Flex to 2024.2+. This script works on machines with or without Flex.

This utility is placed on all Flex clients in the `%ProgramData%\Spillman` folder, and on the Flex server at `sds\app\force\tools\CertUtilChecker`.

When you schedule an upgrade, the upgrade technician will contact you and provide you with the CertCheckerUtil as part of the prepatch process. During this pre-patch process, you or the technician must run the CertCheckerUtil. For more information about running the Motorola Solutions CertCheckerUtil, see Admin: Using the Motorola Flex CertCheckerUtil on page 80.

3.1.1.2
Admin: Using the Motorola Flex CertCheckerUtil

NOTE: The CertCheckerUtil is not intended to be run on Windows Servers, only Windows Clients. If CertCheckerUtil is run on Windows Servers, it displays incorrect results.

Procedure:

1. Open Windows Explorer to the following location: `%ProgramData%\Spillman`
2. Right click on the **CertCheckerUtil.ps** file and select **Run as Powershell**.
3. Enter your Flex server host name found in the certificate manager at the prompt.

   You must enter a host name, not an IP address. IP addresses cannot be secured via SSL certificate.
4. Press **Enter**.
5. Enter the port you want checked.

   You can enter any port that Flex uses. The default port is `4443`
6. Press **Enter**.

   The script runs and checks if the various components are configured correctly, such as network, certificates, and install packages.

   The CertCheckerUtil ensures that your Client, Network and SSL Certificate are properly configured by performing the following actions:

Table 18: CertCheckerUtil Checks

Check	Description
Performs DNS reverse lookup	Confirms that the hostname has a valid IP address in the DNS server.
Checks DNS resolution against all DNS servers locally	Confirms that all of the DNS servers that your network adapter connects to are able to communicate with the host name.

Check	Description
Obtains the registry value from mobile and compare it with the resolved common name	Compares the hostname in Flex Mobile with the hostname entered from the certificate manager to ensure that they are the same.
Attempt to establish SSL connection to the primary tomcat	Confirms that a valid ssl connection can be made to port 4443.
Attempt to establish an SSL connection to the interfaces server tomcat	Confirms that a valid ssl connection can be made to port 4444.
Attempts to establish an SSL connection to usgov.commandcentral.com	Ensures that a connection to CommandCentral can be established, this is used for IBR validation as well as hybrid features such as CC Evidence.
Attempts to establish SSL connection to cdb.usgov.commandcentral.com	Ensures that a connection to CommandCentral can be established, this is used for IBR validation as well as hybrid features such as CC Evidence.
Attempts to establish SSL connection to idm.imw.motorolasolutions.com	Ensures that a connection to CommandCentral can be established, this is used for IBR validation as well as hybrid features such as CC Evidence.
Tests the port list for Flex	Tests the connections between the Flex client and the Flex server. These ports are listed in *Flex Hardware and System Requirements* document.
Tests required packages exist	Confirms the proper .NET and other dependencies are properly installed.
This test validates the number of CPU cores	Confirms that the system has the Flex minimum requirement of 4 cores in the CPU.
This test validates the amount of RAM that is installed on the client	Confirms that the system has the Flex minimum requirement of 4 GB of ram, but its suggested that the clients have 8 GB of ram.
This test validates the download speed of the network connection	Confirms that the system has the Flex minimum requirement of high-speed internet connection.

7. To exit, press **Enter**.

3.2
CAD

3.2.1
Ability to Add Persons to Calls from Comments

This feature reduces the time and number of keystrokes it takes to add persons involved in the incident.

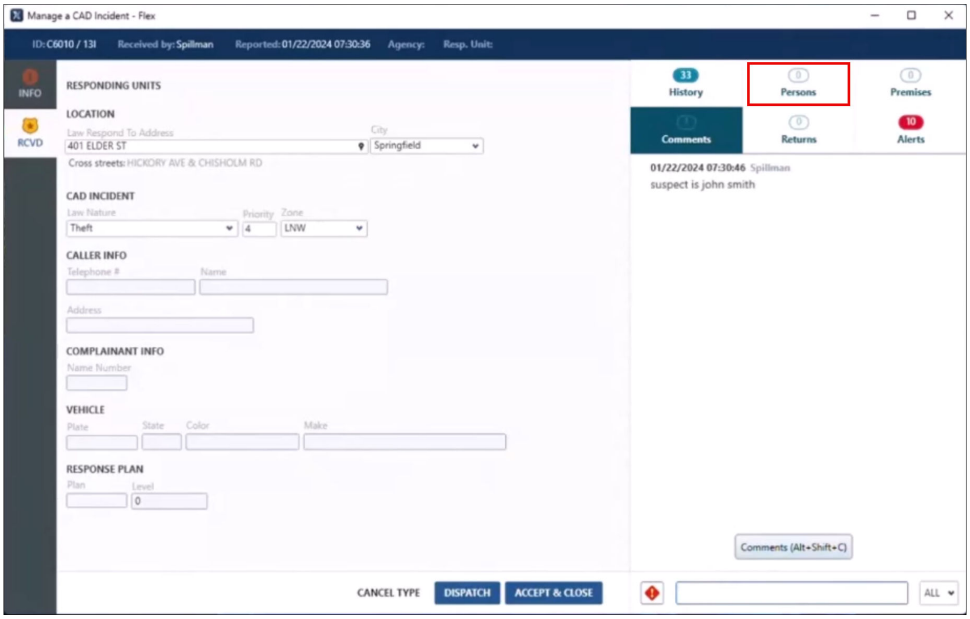
The feature requires the following setting in **Adminutil** at the user level:

`Module.CAD.Calltaking.RunNamesFromComments` adminutil setting is set to `Yes`.

The default value is `No`.

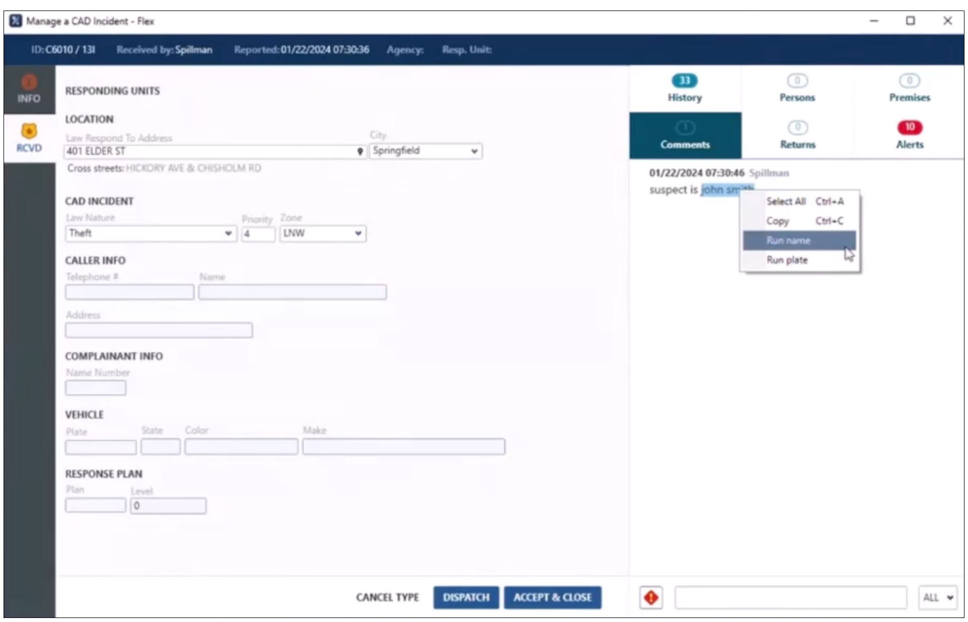
With this setting set to `Yes`, after restarting the Flex client application, the **Manage a CAD Incident** screen has a new **Persons** tab.

Figure 42: The Persons Tab



Users of the **Manage a CAD Incident** screen can now highlight person information included in the text of a comment and use the right-click context menu to run a query by selecting **Run name**. This way they do not need to go to the command line.

Figure 43: Run name Option from Comments



The query results appear in Flex Message Center under **Local Returns** or **State Returns**.

Figure 44: Local Name Match

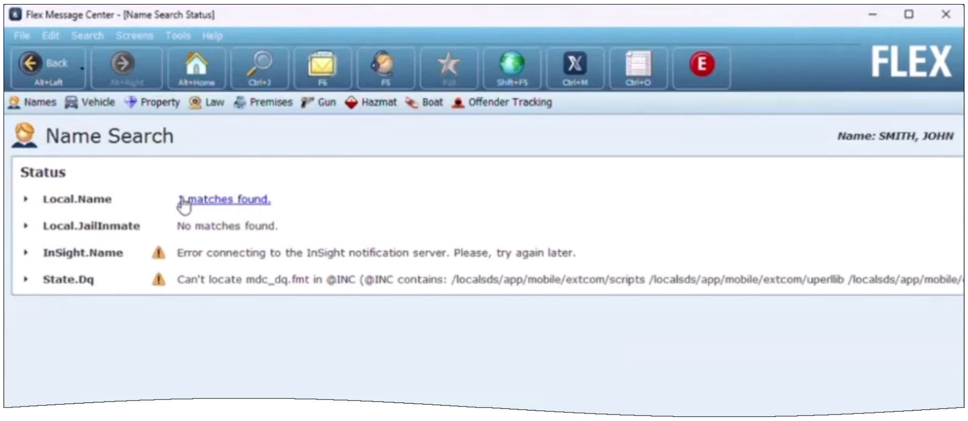
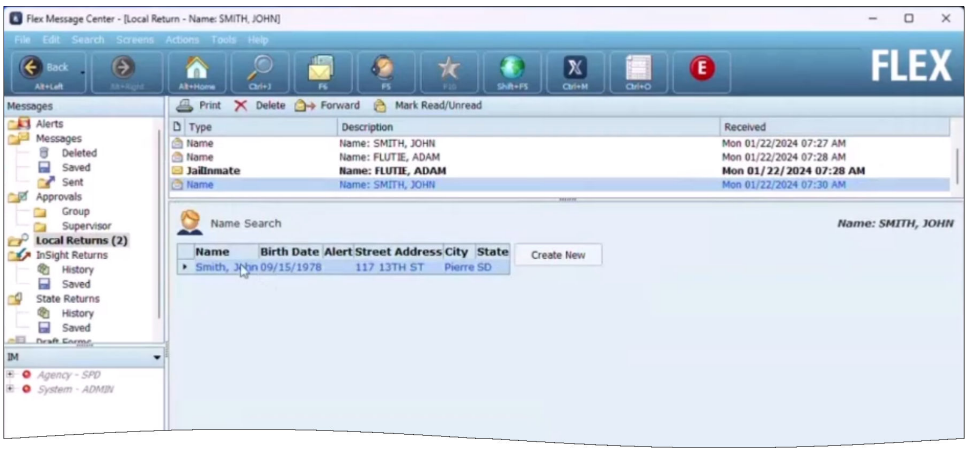
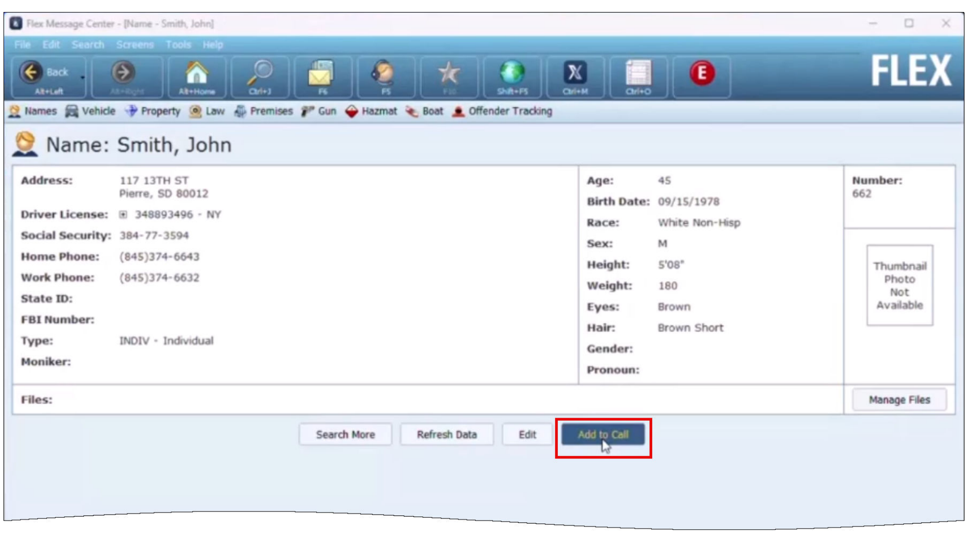


Figure 45: Local Name Return



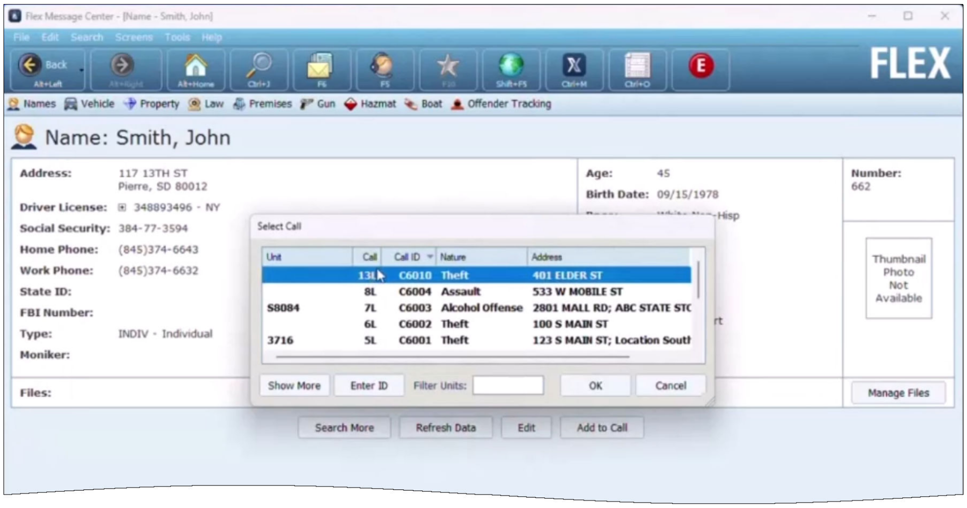
After clicking the result, users can add the person record as an involved person on the CAD call by using the new **Add to Call** button. The StateLink **Add Return** button is relabeled to **Add to Call**.

Figure 46: Add to Call Button



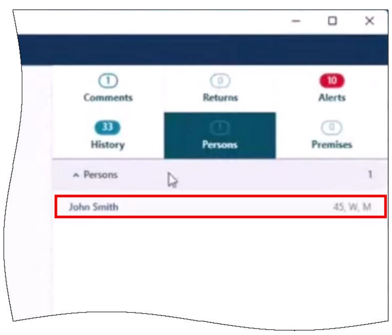
After clicking the **Add to Call** button, in the **Select Call** pop-up window, users should confirm the selection.

Figure 47: Select Call Window



When confirmed, the query result is sent to the selected CAD call. On the CAD Incident screen, the number of involved persons on the **Persons** tab increases. To view the name(s) of the involved person(s) with extracted information on their age, race, and sex, users should click the **Persons** tab and then the **Persons** bar.

Figure 48: Involved Person Added to the Call



The whole information about a person can be displayed by double-clicking their name, which opens the name record from the Names Table.

When more persons are entered in comments, they can be added in the same way.

3.2.2 Shorter Lists of Recommendation Plans for the Recommended Units

Now, the Level drop-down lists contain only the existing recommendation plans for the zone of the incident.

Previously, in the case of covering zones defined for a zone, unit recommendation plans for the covered zone, and unit recommendation plans for the covering zones, the lists might be excessively long.

When an incident occurred in the covered zone, the lists of items listed in level drop-downs contained not only the unit recommendation plans for the zone of the incident, but also unit recommendation plans for the zones covering the zone of the incident.

Currently, the drop-down lists are limited to show only recommendation plans for the zone of the incident.

This update is associated with the elimination of the following adminutil settings:

- `Module.CAD.FlexUnitRecommendations.EnableCoveringZones`
- `Module.CAD.FlexUnitRecommendations.CoveringZonesByAliasKind`

The software continues to operate as though these settings are `True`. More information on this is available in the relevant manuals: *Flex CAD Administrator Manual*, *Flex CAD User Manual*, and *Flex Response Plans Manual.*

3.2.3 Window Positions of CAD Incident Screens Remembered

Now, Manage a CAD Incident screens automatically reopen in the same positions the logged-in user closed them in.

The positions are remembered between sessions of the same user when in **File** → **Configure...** → **General Settings** the **Remember Window Positions** option is selected. Otherwise, the positions are remembered during the current session. This feature is similar to the anchor functionality for Classic screens, but does not require any action on the part of the user.

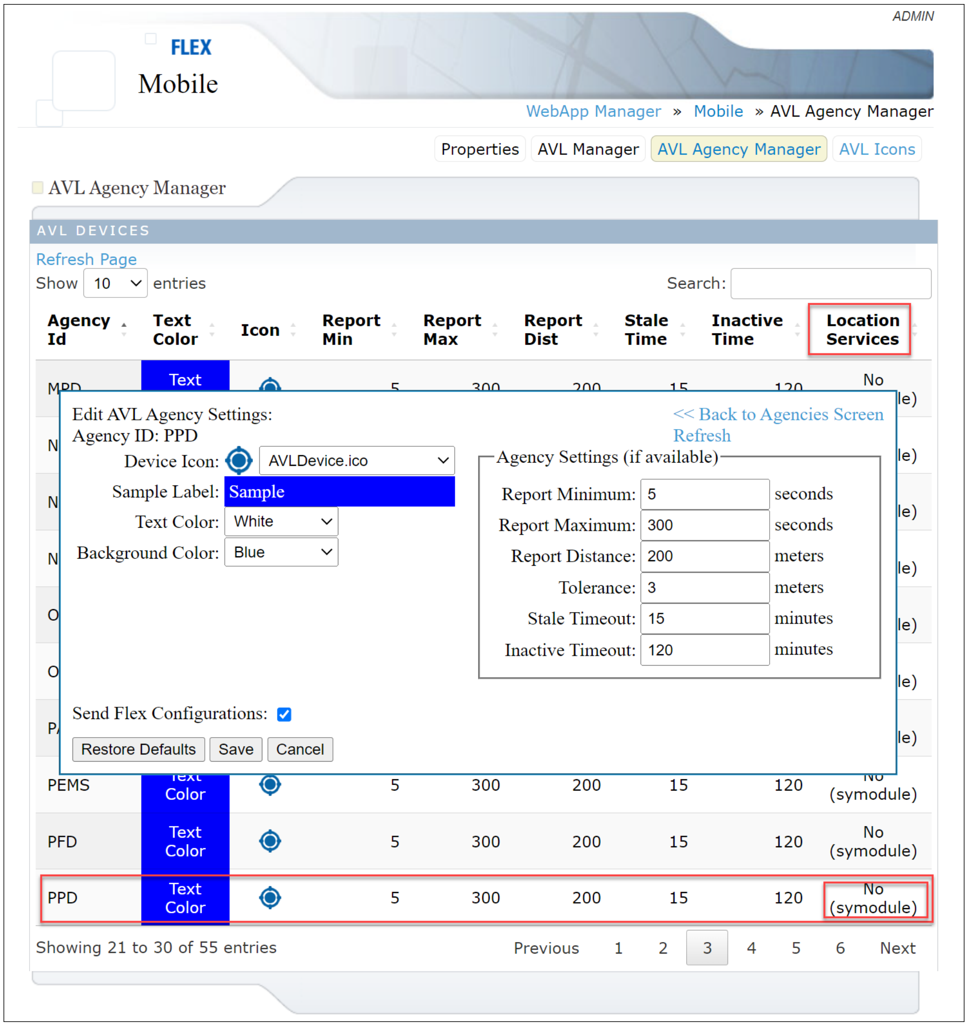
3.3 GeoValidation/Mapping/Quickest Route

3.3.1 Flex AVL Information in CommandCentral Location Services

Flex Automatic Vehicle Location (AVL) information can be forwarded to CommandCentral Location Services. This feature allows users of Flex CAD Web Client and CommandCentral Aware to display Flex units with AVL devices on CommandCentral maps. How the devices show in CommandCentral is based on the setup in CC Admin, under Unit Management.

This feature requires configuration for designated agencies in the Flex Application Manager. See the following examples for the PPD agency.

Figure 49: AVL Agency Manager Page

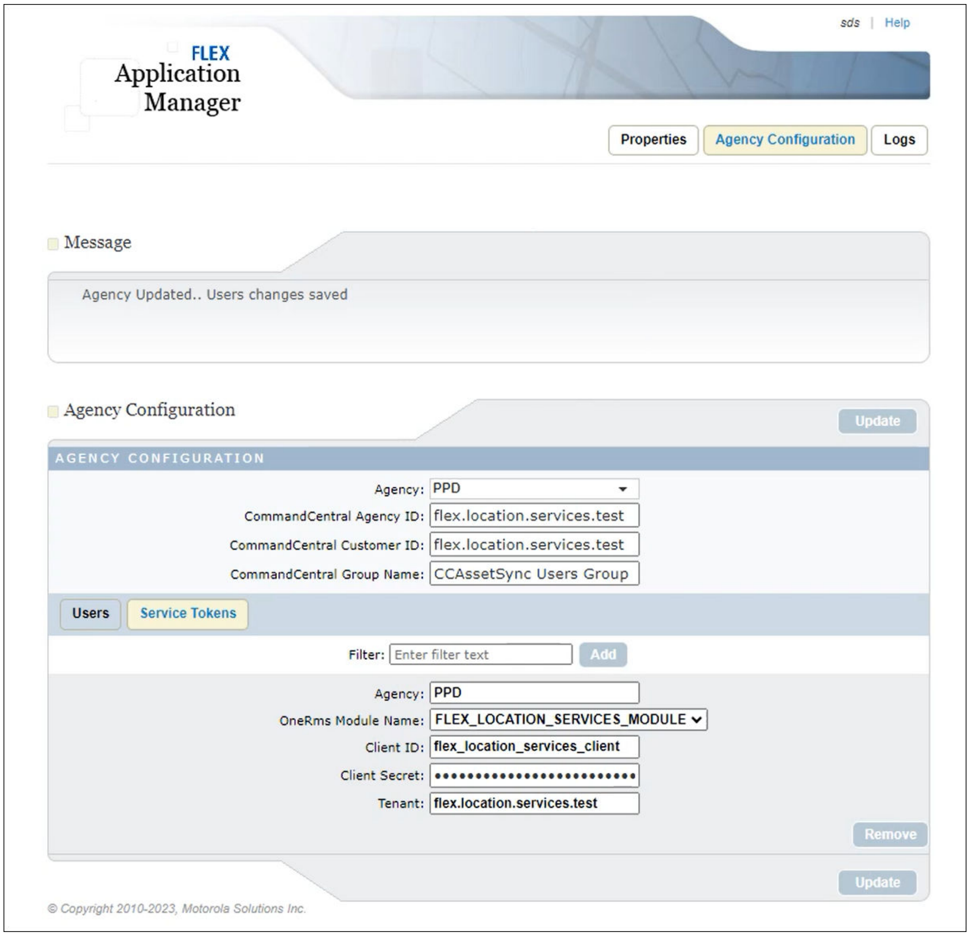


The **AVL Agency Manager** page contains new column: `Location Services`. If the Location Services feature is not set up for an agency, it indicates `No (symodule)`. If the symodule is enabled, it will indicate if that agency has been set up or not in OneRmsConfiguration, and will have a link to OneRms. The values of the status can include:

```
Yes
No
No (invalid)
No (symodule)
```

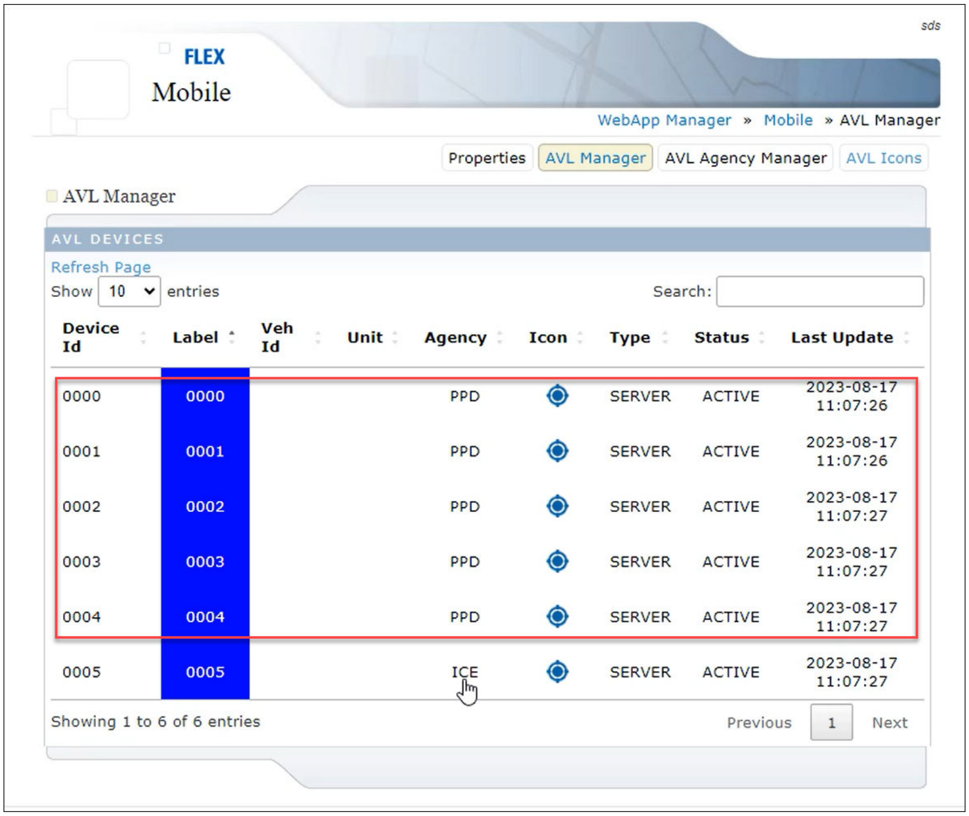
The agency configuration requires setting up **Service Tokens**.

Figure 50: Example Setup of Service Tokens for Forwarding Flex AVL Information to CommandCentral Location Services



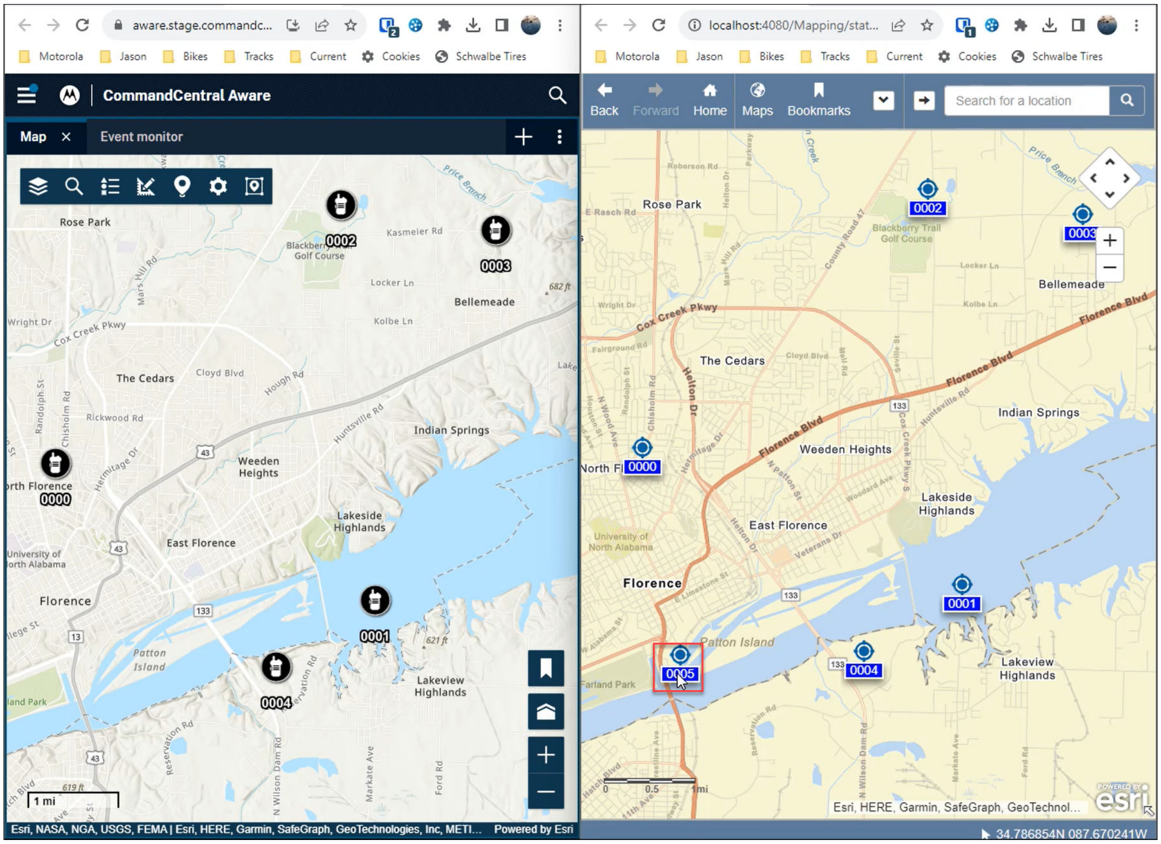
The PPD agency has five active AVL devices. The following list in the Flex Mobile AVL Manager also shows another AVL device (`0005`), however it belongs to a different agency, ICE.

Figure 51: Active AVL Devices



The units with the five active AVL devices can be seen not only on a Flex map, but also on a CommandCentral map, for example on the CommandCentral Aware map.

Figure 52: Flex Units displayed on the CommandCentral Aware and Flex Maps



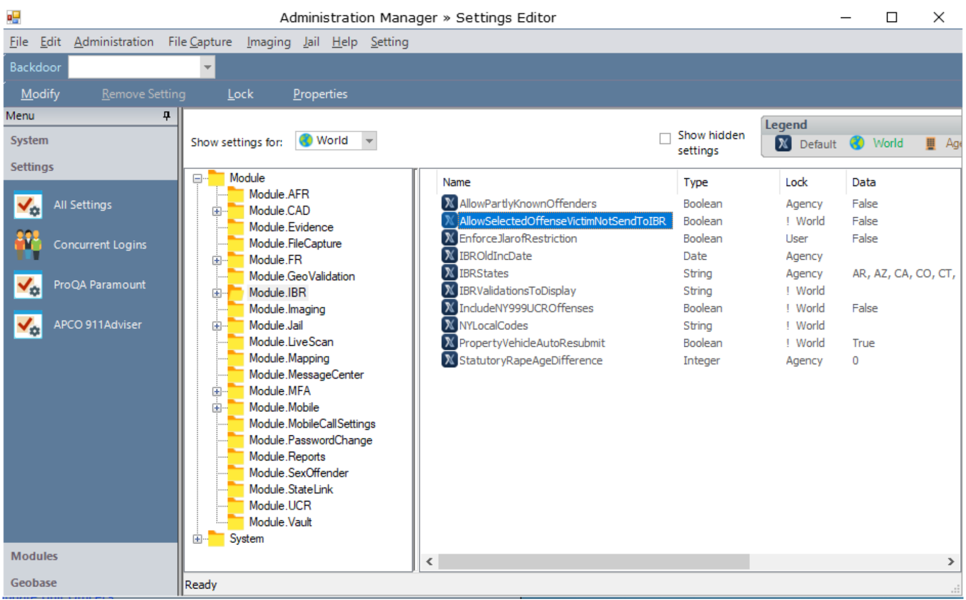
You can notice that the unit `0005` only appears on the Flex map (on the right). The reason is that the feature has not been configured for the ICE agency.

3.4
IBR

3.4.1
Ability to Choose to Submit Lesser Inclusive or Mutually Exclusive Offenses

Maine and Pennsylvania agencies can now allow users to **not** send lesser inclusive crimes to IBR using the `AllowSelectedOffenseVictimNotSendToIBR` setting. Previously, users had to send lesser inclusive crimes to IBR.

Figure 53: AllowSelectedOffenseVictimNotSendToIBR Setting in Adminutil

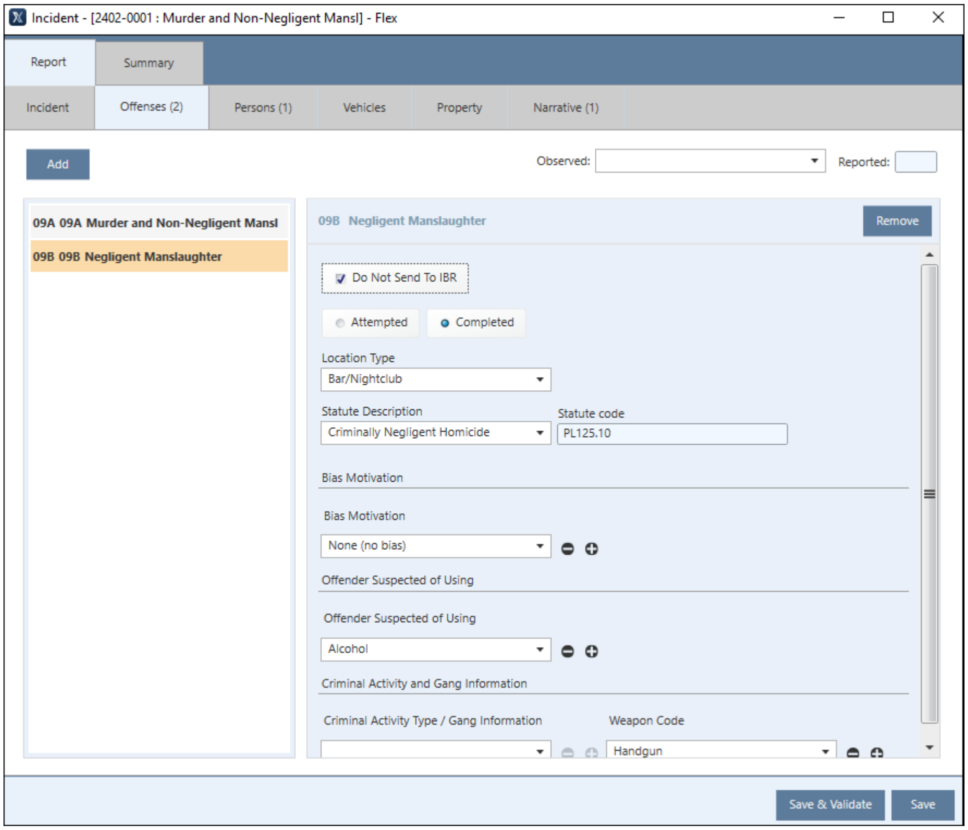


Mutually Exclusive Crimes Check Box

We added a **Mutually Exclusive Crimes** check box on the **Offense** screen when the `AllowSelectedOffenseVictimNotSendToIBR` option is enabled.

Users can select which mutually exclusive offense they want to report by toggling the **Mutually Exclusive Crimes** check box on the offense.

Figure 54: Mutually Exclusive Crimes Check Box



For more information about mutually exclusive and lesser included offenses, see *2019.2.2 National Incident-Based Reporting System Extensible Markup Language Developer's Guide.*

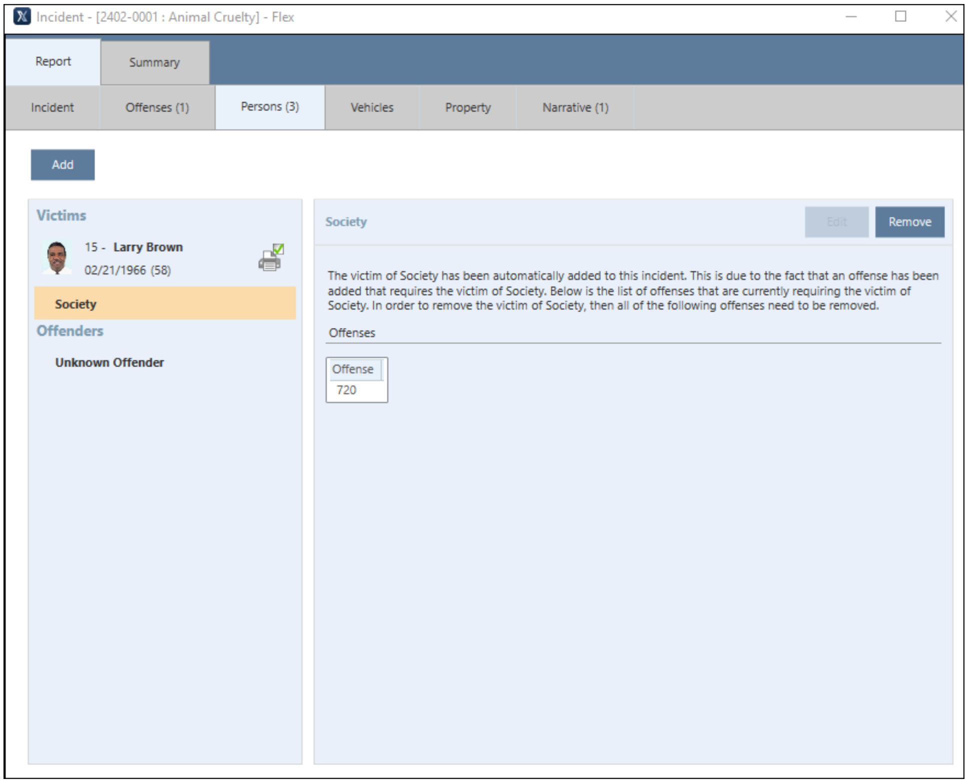
NIBRS

Now when submitting a NIBRS report, users can now add victims to society crimes without reporting to NIBRS. This update aligns Flex reports to NIBRS standards.

Previously when adding a person, the report would error and not validate.

Flex reports now also display a victim, but Flex sends **Society**.

Figure 55: NIBRS Society Crime



3.4.2

State-Specific IBR Release Updates

We implemented the following state-specific IBR updates:

Table 19: State-Specific IBR Updates

State	Description	IBR Version
Washington	State updates	N/A
Alabama	Statute update tool	2023.4
Louisiana	Statute updates	N/A
Nebraska	Statute update tool	2023.3
Maine	Updated state to 2021.1	2023.3
California	Statute updates	2023.2
Ohio	Statute updates	2023.2

3.5
Mobile

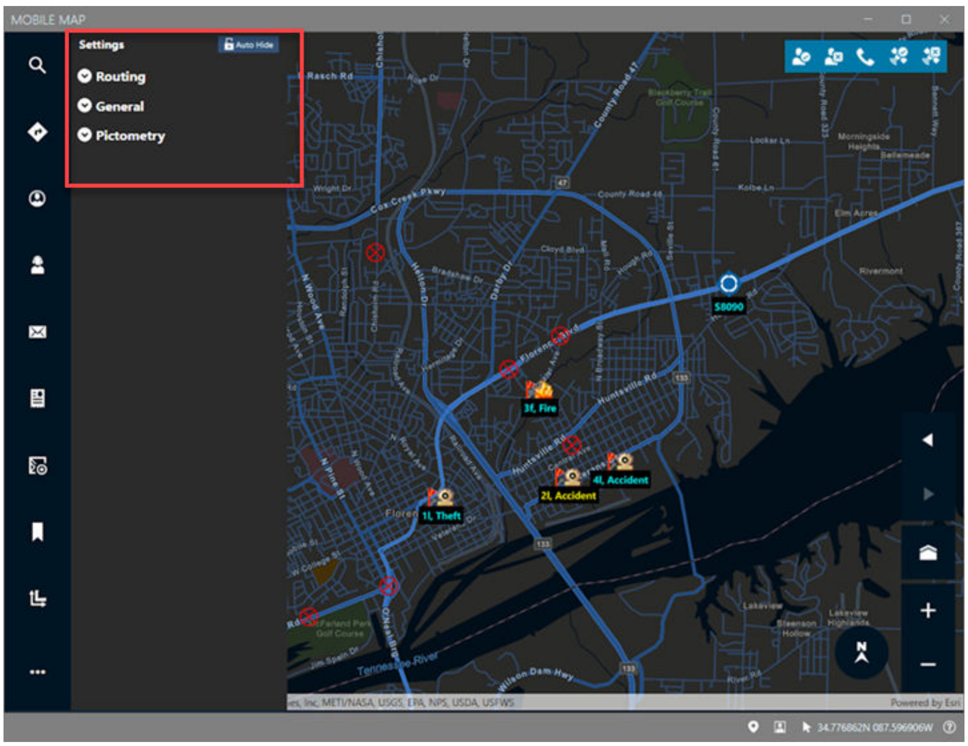
3.5.1
CAD Mapping Settings Reorganization

The existing **Mobile Mapping Settings** menu has been reorganized to list options within specific categories.

The categories include:

- **Routing**
- **General**
- **Pictometry**

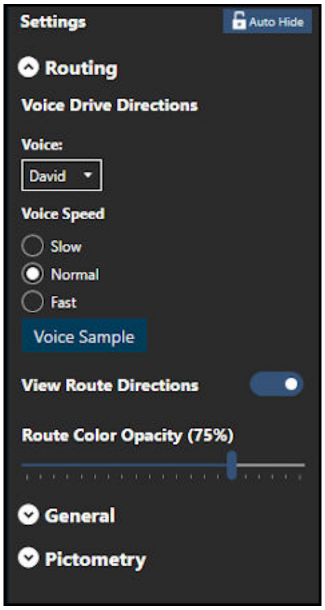
Figure 56: Updated Settings Menu and Categories



The **Routing** option contains the following settings:

- **Voice**: Users can select which voice to use from the drop-down menu.
- **Voice Speed**: Users can select how fast or slow the voice speaks by selecting the **Fast**, **Normal**, or **Slow** check box. Users can also tap the **Voice Sample** button to hear a brief example of how the voice sounds.
- **View Route Directions**: Users can select this option to turn on or off the ability to see route directions displayed on the map.
- **Route Color Opacity**: Users can use the sliding scale to adjust the opacity of the route color on the map.

Figure 57: Routing Option Menu



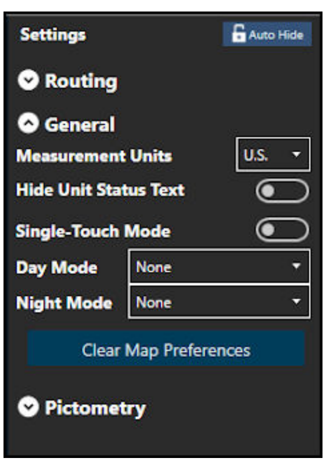
The **General** option contains the following settings:

- **Measurement Units**: Users can select which unit of measurement to use from the drop-down menu.
- **Hide Unit Status Text**: Users can turn on or off the option to view Unit Status Text on the map.
- **Single-Touch Mode**: Users can turn on or off the option to use Single-Touch Mode.
- **Traffic Data**: Users can turn on or off the option to track traffic data from the third-party HERE database.

  NOTE: The **Traffic Data** toggle only appears if your agency has purchased HERE.

- **Day Mode**: Users can choose which Day Mode to use on the map from the drop-down menu, or select **None** to choose no option.
- **Night Mode**: Users can choose which Night Mode to use on the map from the drop-down menu, or select **None** to choose no option.
- **Clear Map Preferences**: Users can choose to clear some map settings and set them to their default. The following settings are cleared: Map layer selections (defaults to showing all layers), Look up markers, Route and directions, and Unit/Call Filters (defaults to Show All).

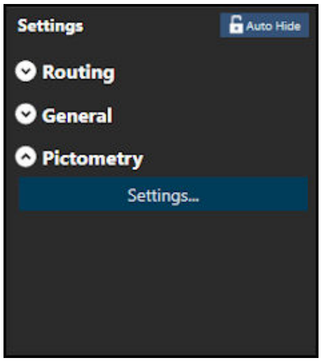
Figure 58: General Options Menu



The **Pictometry** option contains the following setting:

- **Settings**: Users can tap this button to navigate to the **Pictometry Settings Window**.

Figure 59: Pictometry Option Menu



3.6
Records

3.6.1
Agency Filterable Law Circumstances

We added the **Agency** field to the Law Incident Circumstance Codes (`lwtbcirc`) table.

The **Circumstances** field on the **Law Incident** and **Mobile Law Incident** screens is now easier to maintain and use.

Using the **Circumstances** field, you can now filter and display circumstances that are relevant for your specific agency.

By selecting the **Show All** button under the **Circumstances** field, you can view all circumstances, regardless of agency.

3.6.2
Automatic Workflow Initiation after Creating an Evidence Record in Mobile Law Incident

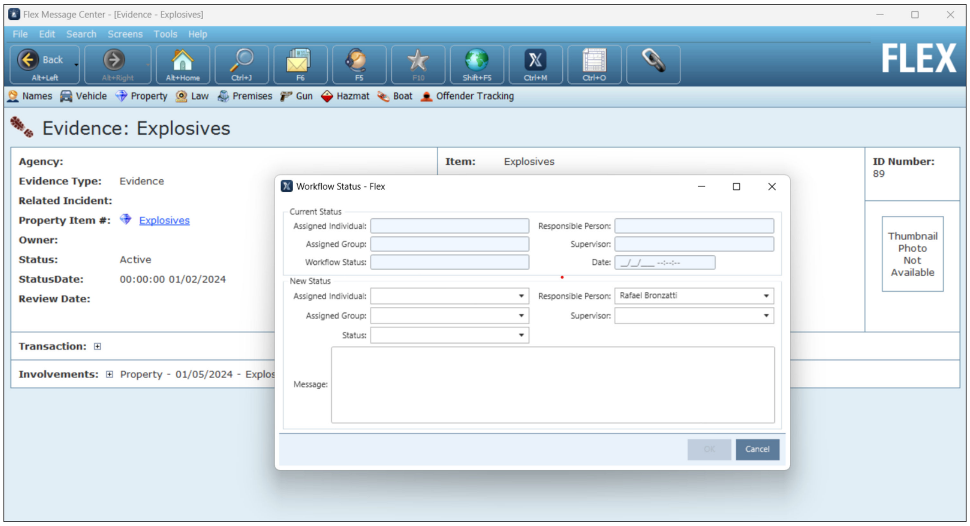
Previously, if configured, workflow for evidence would automatically initiate only if an evidence record was created in Flex Desktop. Now, evidence records created through a Mobile Law Incident form will automatically initiate workflow as well.

To ensure workflow is initiated automatically, your administrator must add the following `wfcfg` entry for Evidence in the Application Parameters table (apparam):

```
evmain evmain.number A
```

With this setup in place, when you create a new evidence record through the Mobile Law Incident form, you can see that the workflow is automatically initiated and the Evidence Technician is notified.

Figure 60: Example of Automatically Initiated Workflow



3.6.3

External CAD ID Field in the PremierOne CAD to Flex RMS Interface

We added a new **External CAD ID** field to the **Law Incident** (`lwmain`), **Fire Incident** (`frmain`), and **EMS Incident** (`emmain`) screens.

This field is activated by administrators in the P1CADtoFlexRMS web application with the use of the **Import P1 CAD data into Flex CAD** setting.

The PremierOne CAD to Flex RMS interface (P1CADtoFlexRMS) can now put the P1 CAD ID in the new **External CAD ID** field in the Law, EMS and Fire incident records. Other integrations can use this field for external CAD Incident numbers.

This allows users to tie reports back to CAD incidents. The **External CAD ID** field can be auto-populated on the **Law Incident** (`lwmain`), **EMS Incident** (`emmain`), and **Fire Incident** (`frmain`) screens for agencies that are using the P1CADtoFlexRMS interface.

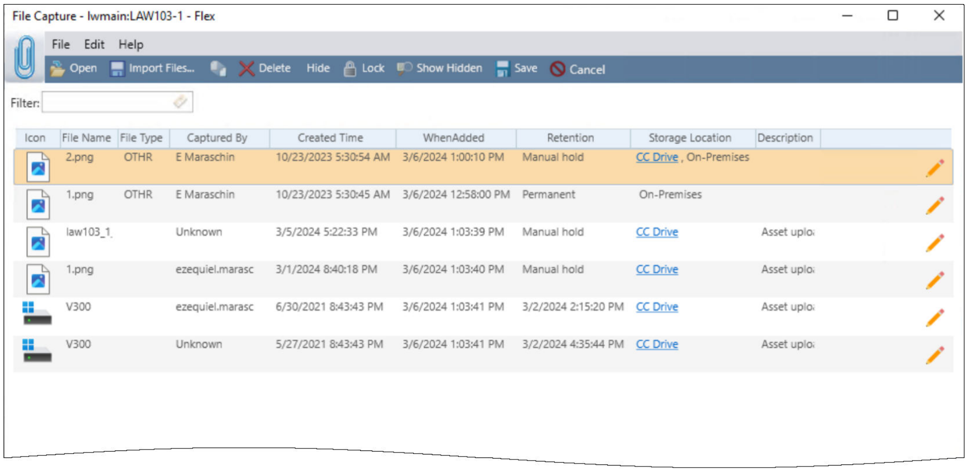
3.6.4

File Capture Screen Enhancements

We completed the following enhancements for the **File Capture** screen:

- Added a **Retention** field. If the file is stored in CommandCentral Evidence, the field shows the retention expiration time of the asset, or `Manual hold`. If the file is stored in Flex, it shows `Permanent`.
- Added a **Storage Location** field that shows the location of the file: `On-Premises`, or `CC Drive` (where CommandCentral Evidence data is stored). If the file is located in CC Drive, the user can view the file directly in CommandCentral Evidence by clicking the `CC Drive` link.
- For digital assets added from CommandCentral Evidence, the **Captured By** field now displays the name of the user from the CommandCentral Evidence record. A future release will expand the **Captured By** field to show the full email address of the CommandCentral Evidence user.

Figure 61: Enhanced File Capture Screen



3.6.5

tbcourt Judge Field Expansion

The **Judge** field on the `tbcourt` screen can how hold up to 50 characters, which is the same as the **Clerk** field.

3.6.6

Updated CommandCentral ID and Email Fields

The **CmdCentral ID** and **CmdCentral Email** fields (added to apnames in 2024.1) can now be populated with the CommandCentral UUID and email address associated with a user's account in CCAdmin.

When the user's email address is updated in either Flex or CommandCentral, the **CmdCentral Email** field automatically updates.

The Flex Application Manager Agency Settings page now includes a sync button **Force Sync with CCAdmin** which allows users to force a synchronization with CCAdmin to ensure any email address updates are synchronized. This should rarely be used.

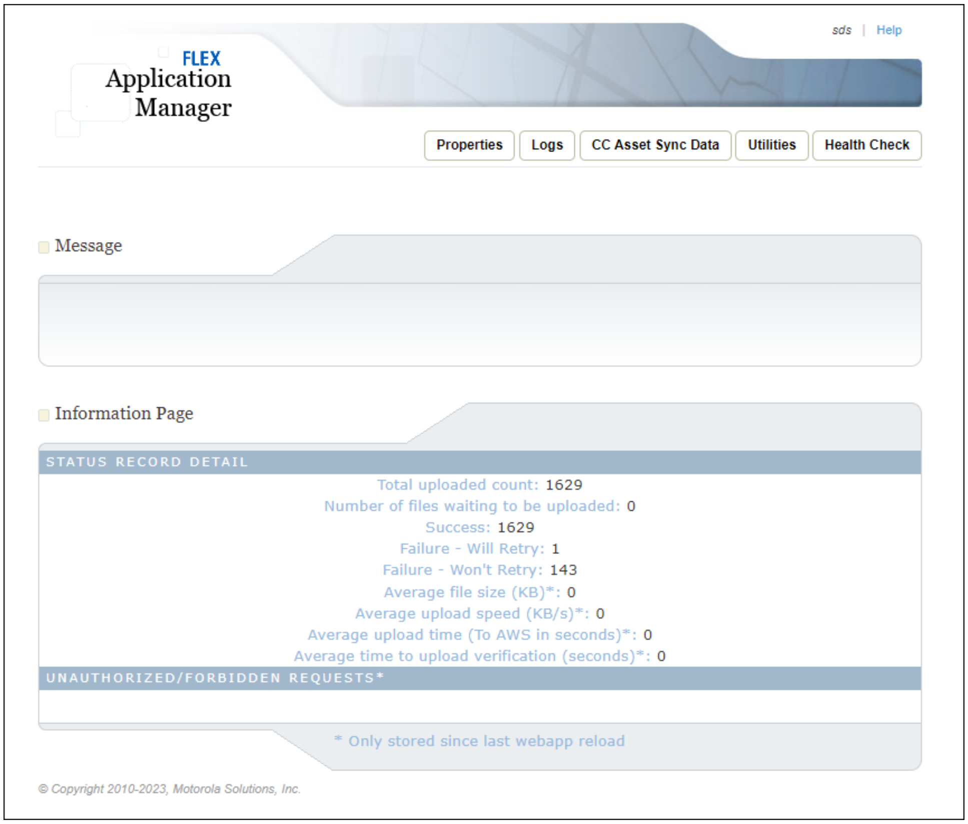
3.6.7

Admin: View Access to CCAssetSync Information Page by a System Privilege

We created a new system privilege **ccasinfo** which you can use to allow users access to the CCAssetSync **Information Page** without their needing to be an administrator or super user. You can set this system privilege at the user, group, agency or world level.

Users with this privilege are not able to modify any CCAssetSync settings or configurations, but can view the CCAssetSync synchronization status. They will still need **su** or **admin** permissions to modify any CCAssetSync settings.

Figure 62: CCAssetSync Information Page



3.7
StateLink

3.7.1
State Specific Updates

The following updates have been completed for the following states:

Table 20: StateLink Updates

<table>
<tr><th>State</th><th>ID</th><th>Description</th><th>StateLink Version</th></tr>
<tr><td>ME</td><td>SLT-9036</td><td>ORI Updates</td><td rowspan="4">2.0</td></tr>
<tr><td>NC</td><td>SLT-9630</td><td>Image Returns</td></tr>
<tr><td>MT</td><td>SLT-9983</td><td>DQ Parsing Updates</td></tr>
<tr><td>CA</td><td>SLT-9977</td><td>CLETS Package - Protective Order</td></tr>
<tr><td>AZ</td><td>SLT-10077</td><td>Multi-owner Return Parsing</td><td>1.0</td></tr>
</table>

Chapter 4

Release 2024.1

This chapter presents changes made to Flex for the 2024.1 release.

4.1
CAD

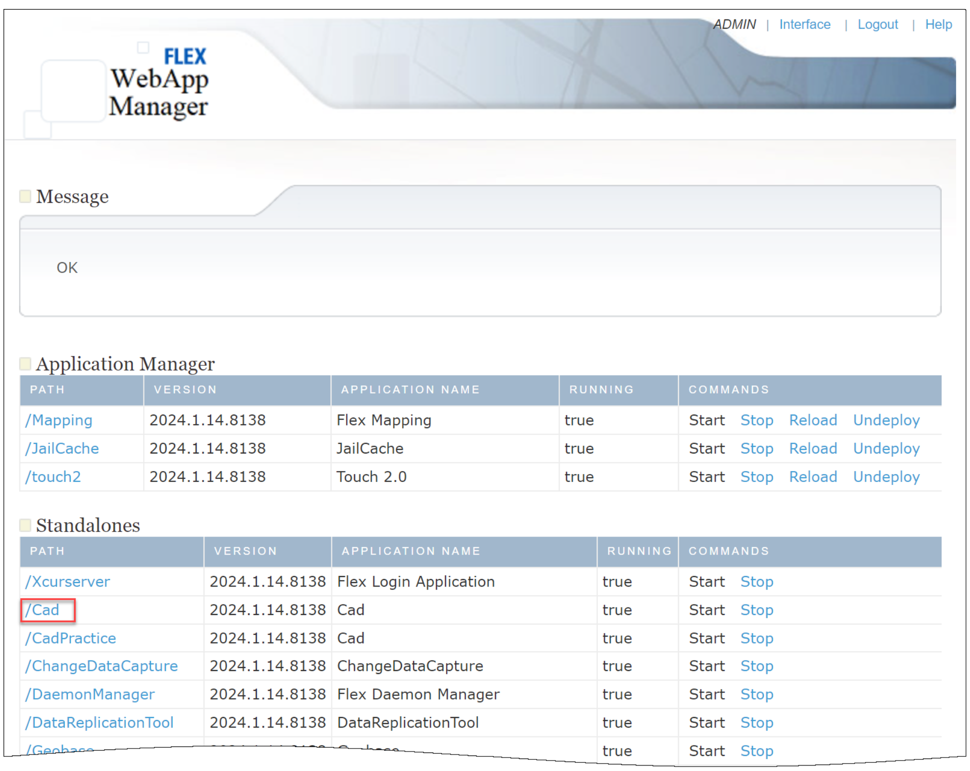
4.1.1
Admin: Clearing the CAD Cache

Administrators may need to clear the cache if any information is out of sync, without restarting the CAD application. By using the **Clear Cache** button, you can ensure that the CAD application has the right information. This should not impact users that are already logged in, since they have their own copy of the cache.

Procedure:

1. Open the Flex WebApp Manager.

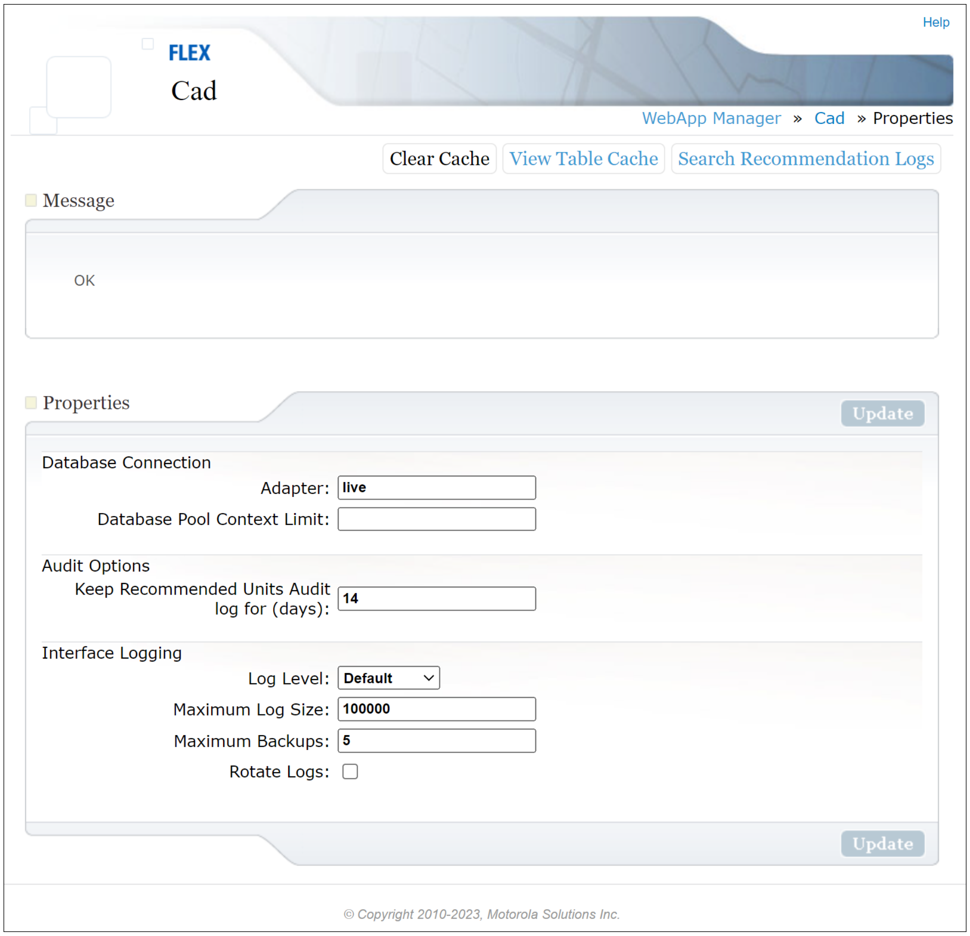
   Figure 63: CAD Link in the Flex WebApp Manager

2. Click the **/CAD** link.

   The Flex Cad Properties screen opens.

Figure 64: Flex Cad Properties Screen



3. Click the **Clear Cache** button, and in the pop-up confirmation box click **OK**.

   In the **Message** area, the `Please wait, clearing cache…` information appears, which finally changes to `Cache cleared!`

   NOTE:
   If any errors occur during that operation, in the **Message** area the relevant information is displayed instead.

   The process flow and results are recorded and can be checked in the Log File Viewer.

4.1.2

Admin: Enabling and Configuring Automatic Unit Status Updates

With automatic unit status updates enabled, some unit statuses can change automatically when a unit leaves a station, arrives on scene, and returns to its assigned station. This is a way to reduce radio traffic. You can now enable this feature for units in your agency in the **Units Table**, with the use of the new **Auto Status**

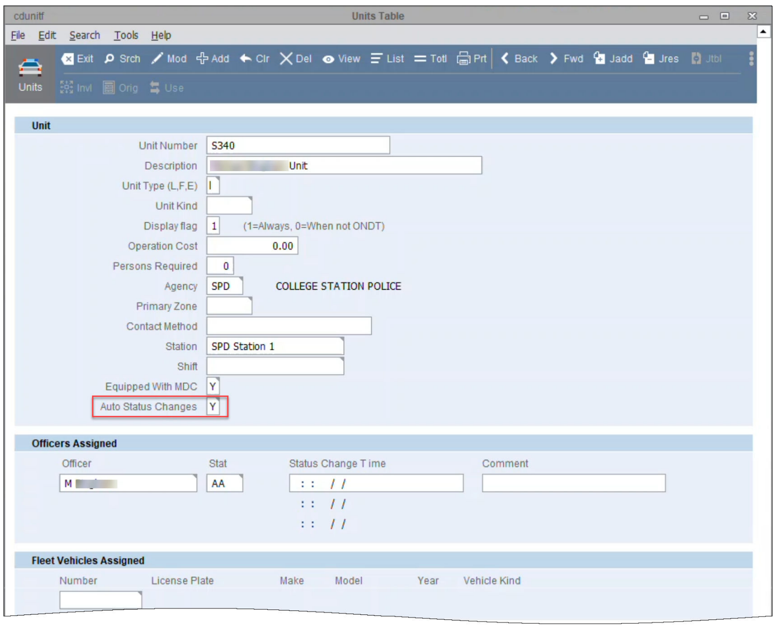
Changes field. In the **Unit Status Ten-Codes** table you must configure criteria that determine when an automatic status change occurs.

NOTE: This feature requires the AVL module and requires that vehicles are feeding their GPS locations to Flex.

Procedure:

1. At the command line, enter `cdunit`
2. In the `cdunit` (**Units Table**), for a given **Unit Number**, set the **Auto Status Changes** field to `Y` (Yes).

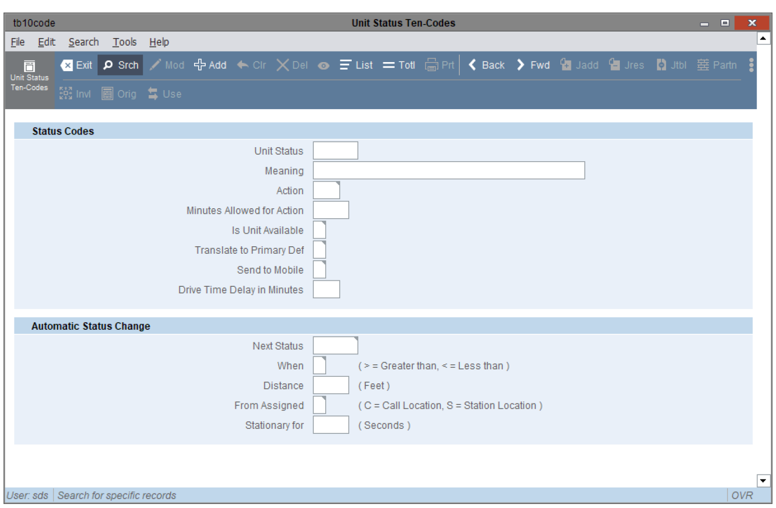
   Figure 65: Auto Status Changes Field

3. To configure criteria that determine when an automatic status change occurs, at the command line enter `tb10code`

   The `tb10code` (**Unit Status Ten-Codes**) table has been extended with the **Automatic Status Change** section with the **Next Status** field and four fields for choosing the criteria.

   Figure 66: tb10code Table with the Automatic Status Change Section

4. In the `tb10code` table, for each **Unit Status** to be automatically changed, in the **Automatic Status Change** section fill in the subsequent fields:

   a. In the **Next Status** field, choose the next status that will be assigned to a unit when the following conditions are met.

   b. In the **When**, **Distance**, **From Assigned**, and **Stationary for** fields, set the required conditions.

      An example sequence of status changes and their conditions:

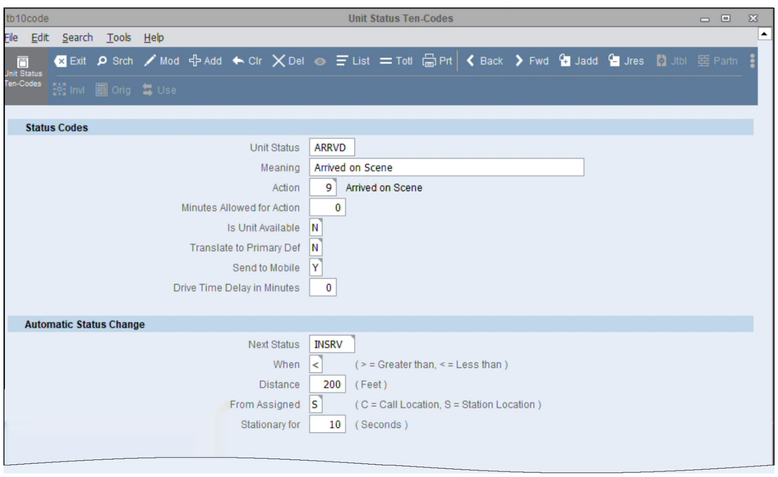
      i. `INSRV` to `BUSY` – when a unit exceeds the distance of 150 feet from the station and is stationary for zero seconds (zero seconds means that the status changes immediately after exceeding this distance). The address of the station must be entered in the `cdstatn` table.

      ii. `ENRT` to `ARRVD` – when a unit is closer than 100 feet to the call and stationary for 10 seconds.

      iii. `ARRVD` to `INSRV` – when a unit is closer than 200 feet from the station and stationary for 10 seconds.

      The following figure shows data entered to automatically change a vehicle status from `ARRVD` to `INSRV` when the distance of the vehicle to the **Station Location** is less than 200 feet and the unit becomes stationary for 10 seconds (**iii**).

      Figure 67: Configuration Example for Automatic Status Change



With the example sequence of status changes and their conditions, when Unit `S340` is responding to a call and then returning to its assigned station, the dispatcher can notice the following changes in the **CAD_1 Unit Status (1)** window:

Figure 68: Initial INSRV Status of Unit S340

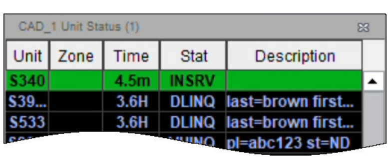


Figure 69: Change to BUSY Status

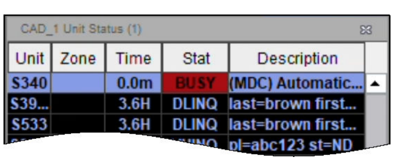
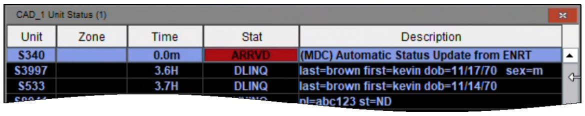


Figure 70: Change to ARRVD Status



In the **Description** column of the expanded window the dispatcher can view the full information about the status change.

Figure 71: Change to ENRT Status

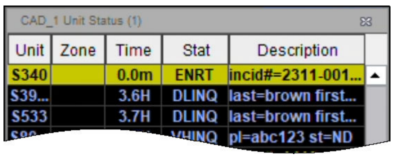
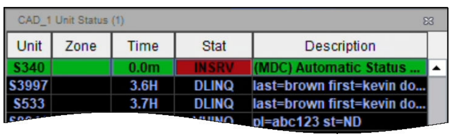


Figure 72: Change Back to INSRV Status



4.1.3 Units Display Order the Same as the Dispatching Sequence

On the CAD Incident screen, responding units are now displayed in the same order they were dispatched, with the responsible unit always listed first.

In the following figures you can see an example with three dispatched units.

Figure 73: Calltaker Screen with a Sequence of Three Dispatched Units

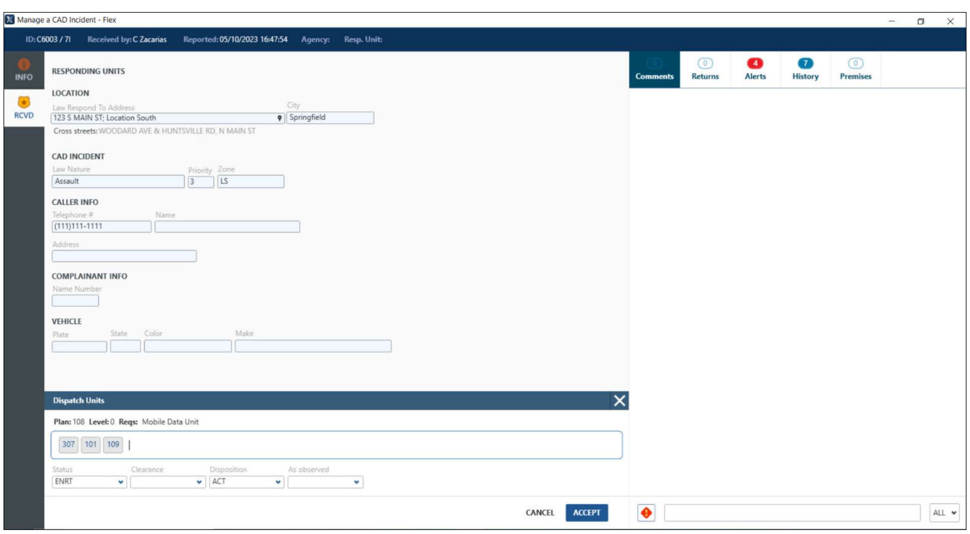
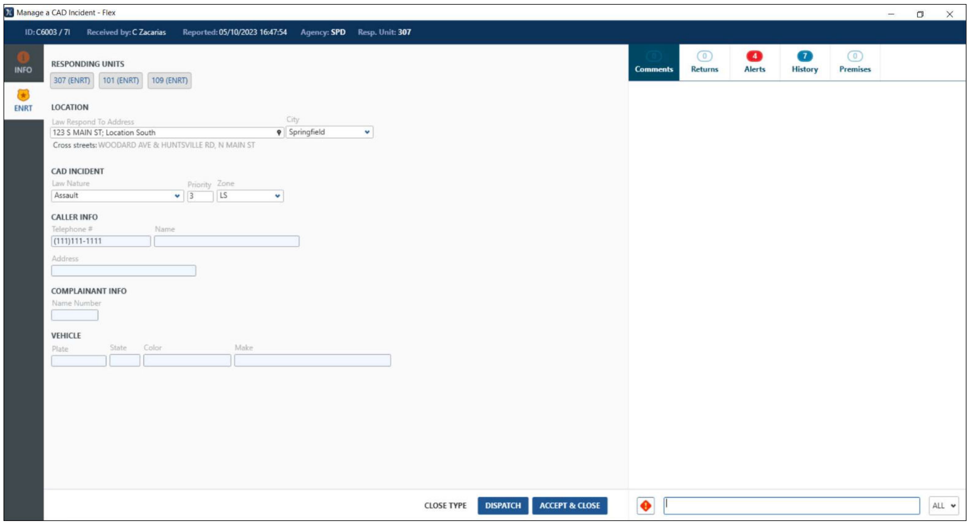


Figure 74: Dispatch Screen with the Dispatch Order Preserved



The same sequence of the dispatched units is preserved in the `Units` column of the **Dispatched Calls** CAD Status window.

4.2 Hub/Platform

4.2.1 Flex Documentation Link in Flex Help Menus

A link to all **Flex Documentation** on the LXP is now included in the Flex **Help** menus. Flex users can now quickly and easily access the most up-to-date **Flex Documentation** on the LXP through the respective **Help** menu in Flex Desktop, Flex Mobile, or Flex Jail screens.

Figure 75: Link to Flex Documentation in the Flex Desktop Application

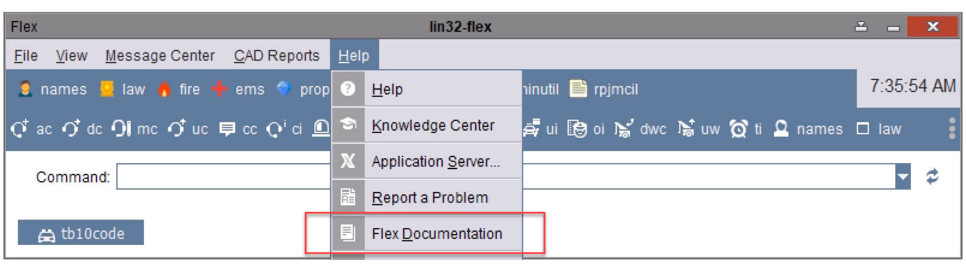


Figure 76: Link to Flex Documentation in the Flex Mobile Application

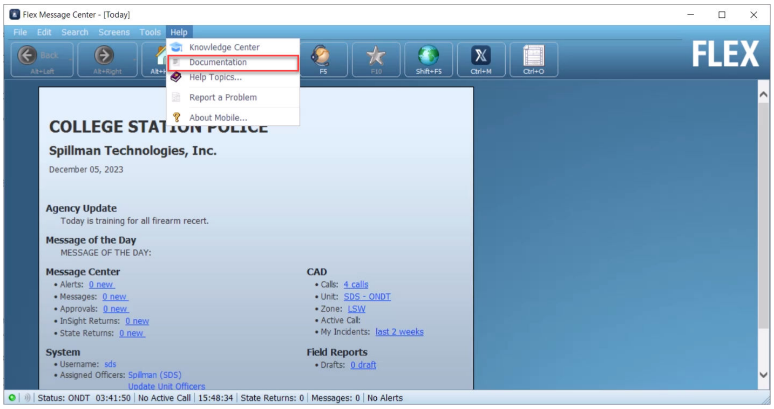


Figure 77: Link to Flex Documentation in the Flex Jail Application

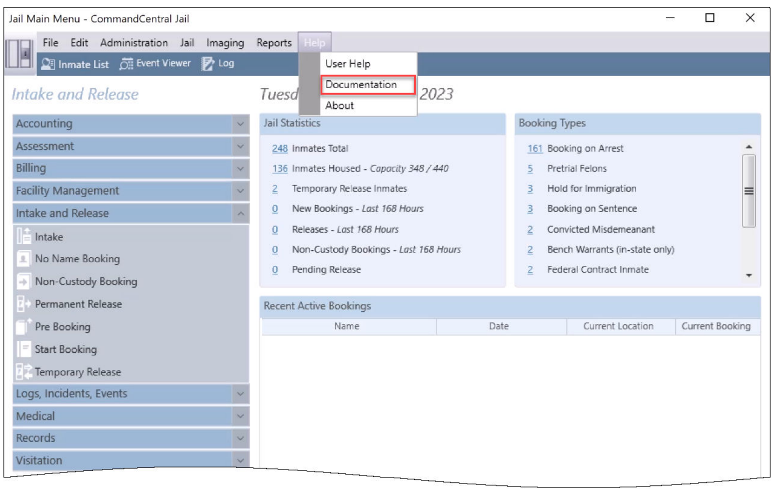
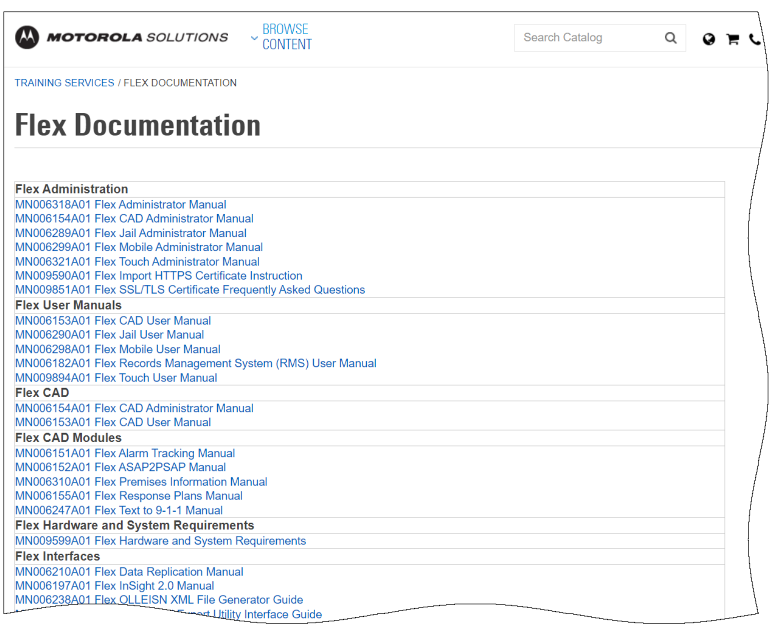


Figure 78: Flex Documentation Page on the LXP



4.2.2
Support for Red Hat Enterprise Linux 9 (RHEL 9)

Beginning with Flex version 2024.1, Red Hat Enterprise Linux 9 (RHEL 9) is a supported Operating System (OS). RHEL 9 OS can now be used for server migrations and new installations.

Due to differences between RHEL 6, 7, 8 and 9, it is not possible to do an in-place upgrade to RHEL 9, and a migration must be performed. Please reach out to Customer Success or Sales for more information.

NOTE: All RHEL installations require an active maintenance contract with Red Hat so that the OS software and security updates can be installed. Up-to-date OS software and all security updates are necessary for CJIS compliance.

4.3
Interfaces

4.3.1
ASAP2PSAP for Wisconsin State

Flex now supports the Automated Secure Alarm Protocol (ASAP2PSAP) for Wisconsin state.

ASAP2PSAP has been successfully tested by an agency in Wisconsin. The feature is released and available for all customers in this state.

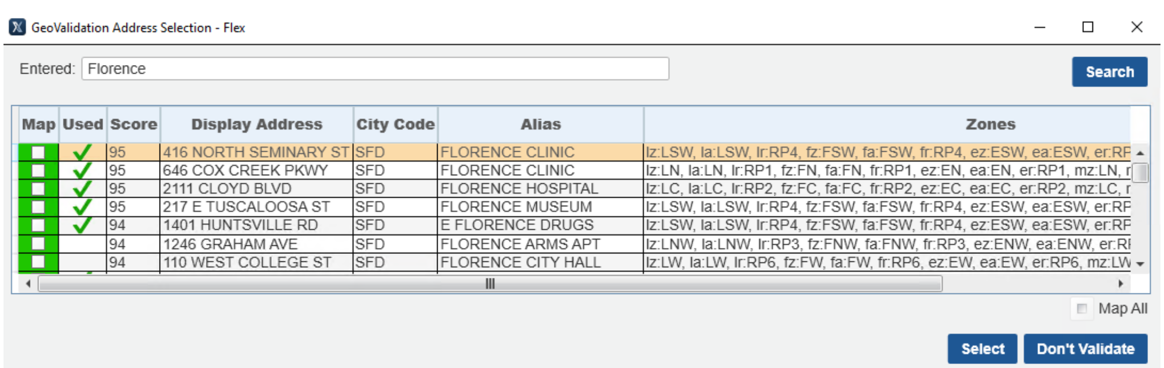
4.4
GeoValidation/Mapping/Quickest Route

4.4.1
Admin: Zone Query Settings for GeoValidation Addresses

Administrators can use the `Module.GeoValidation.QueryCandidateZones` user-level setting to control whether zones are queried for every candidate or the selected candidate addresses in the GeoValidation Address Selection window. Depending on the number of zones returned from the query, this new setting enables less of query load on the GIS server and a shorter query wait time.

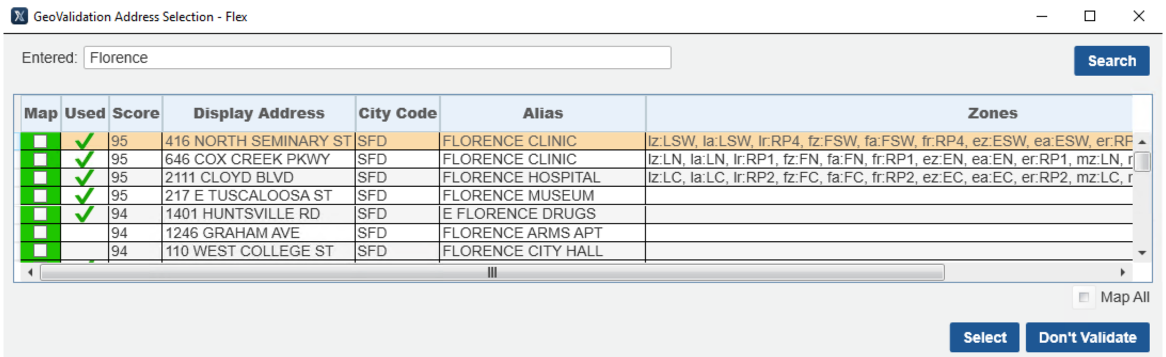
When a Flex user validated an address, earlier Flex releases queried the zones of every candidate from the search. In the current release, the default setting of **True** matches this behavior: that is, all the zones are returned from a query.

Figure 79: GeoValidation Address Query True Setting



When the new `Module.GeoValidation.QueryCandidateZones` setting is set to **False**, only the zones of selected candidates are returned.

Figure 80: GeoValidation Address Query False Setting



NOTE: Regardless of the setting, a zone is returned if the GIS data for the address candidate contains the zone or if the address candidate is an intersection: for example, Fairfax Ave & W 3rd St.

4.5

IBR

4.5.1

State-Specific Updates

The following are state-specific IBR updates:

Table 21:

State	ID	Description	IBR Version
California	IBR-4903	New statute updates	N/A
Colorado	IBR-4839	3611 and 3619 offenses now 90Z per state	N/A
Illinois	IBR-5044	New statute updates	N/A
Indiana	IBR-4983	State statute correction	N/A

4.5.2

Minnesota IBR

Flex IBR is now available in Minnesota.

4.5.2.1

Admin: Setting Up Minnesota IBR

As an administrator, complete the following one-time set up Minnesota IBR by completing the following actions:

Procedure:

1. Add the new **Role** into miscellaneous data (aptbmisc):
   a. At the **tbmitype** table, click **Add**.

   b. Enter `Role` in code and description.

2. Under **apnames**, set up the role description:
   a. Select **Role**.
   b. In the **Description** field, enter a description for the role, such as `Officer` or `Records Clerk`.

   You only need to do this once for all users.

   For example, for any officer in **apnames**, you can select **Misc Info** and open the **aptbmisc**. You can click **Add** and select **Role** from **Misc Code**. You can resolve this by entering role **Value** and clicking **Accept**.
3. Ensure that users must use NCIC values for vehicle makes in **tbmake** and vehicle colors in **tbcolor**.

   NOTE: The Flex client uses the values from the **vhmain** table to send to the state.
4. Under **tbcrime**, users must have the following options:
   - **PM - Petty Misdemeanor**
   - **M - Misdemeanor**
   - **GM - Gross Misdemeanor**
5. Under **tbotype**, assign users to **L - Local Ordinance**.

4.6
Jail

4.6.1
Additional Columns on Inmate List

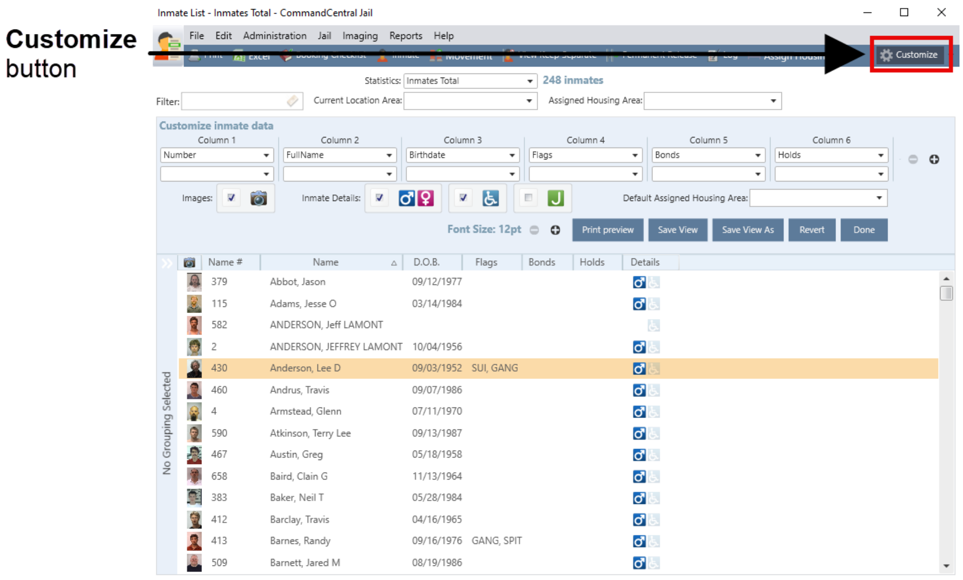
We added additional columns that display the following fields/information to the **Inmate List** screen:

- Flags
- Bonds
- Holds

We added these fields to the **Inmate List** screen to ensure that the information is more visible to corrections officers and reduces the keystrokes and mouse clicks previously used to check for this information.

You can enable these columns by clicking the **Customize** button and selecting which columns you want.

Figure 81: Updated Inmate List Screen



4.6.2
LiveScan 3.0 Bio Option Enablement

As of this release, the Flex **Bio** option is operational in LiveScan 3.0.

If the Administrator activates the Bio option, you can print fingerprint cards and biographical information from the **Names** screen (names). You should use this option to print information in a non-arrest situation such as an employment or a license application.

You have the following options for printing biographical information:

- Printing the biographical information on a fingerprint card, using the agency's fingerprint machine(s).
- Printing the information on a laser printer.

Administrators can configure the Bio option by adjusting the **bioinfo** parameter. The **bioinfo** application parameter determines whether the Bio option appears on the toolbar of the **Names** (nmmain) screen. The parameter also tells the software which custom script to run. Currently the only available script is tpcard.

Admins can make the Bio option available on the **Names** (nmmain) screen by entering the name of the appropriate custom script, such as `tpcard`, in the bioinfo application parameter

Admins can also prevent users from using the Bio option by leaving the bioinfo application parameter blank (the default value).

4.6.3
Texas Monthly Jail Report

You can now print the Texas Monthly Jail Report (rpjltxpop) from the Flex Jail **Texas Jail Population Report** screen (screen name).

Texas requires two jail reports and a cover letter from Jails in Texas. The following report is now in Flex:

- A population summary report

The Texas Monthly Jail Report report is generated by pulling information from the following modules through booking type **jlbktype**:

- Module.Jail.TX.Population.benchWarrant

- Module.Jail.TX.Population.convictedFelCountyJail
- Module.Jail.TX.Population.convictedFelTDCJ
- Module.Jail.TX.Population.convictedMisdemeanant
- Module.Jail.TX.Population.convictedSJFCounty
- Module.Jail.TX.Population.convictedSJFState
- Module.Jail.TX.Population.federalInmates
- Module.Jail.TX.Population.felonsToMisdemeanor
- Module.Jail.TX.Population.othersInm
- Module.Jail.TX.Population.paperReadyGE45
- Module.Jail.TX.Population.paperReadyLT45
- Module.Jail.TX.Population.paperReadySAFP
- Module.Jail.TX.Population.paroleViolatersBW
- Module.Jail.TX.Population.paroleViolatersNC
- Module.Jail.TX.Population.pretrailSJF
- Module.Jail.TX.Population.pretrialClassABMisd
- Module.Jail.TX.Population.pretrialClassCMisd
- Module.Jail.TX.Population.pretrialFelons

Pregnant inmates are identified by pulling through inmate flags.

4.7 Mobile

4.7.1 Assigned Users and Groups by Agency

As of the 2024.1 release, when updating Approvals through the **Update Approvals** or **Update Multiple Approvals** screens, the assigned Individual, Group, Responsible Person, and Supervisor will display by agency if the syparam codefltr is set to `YES`.

4.7.1.1 Admin: Filter Individuals and Groups by Agency

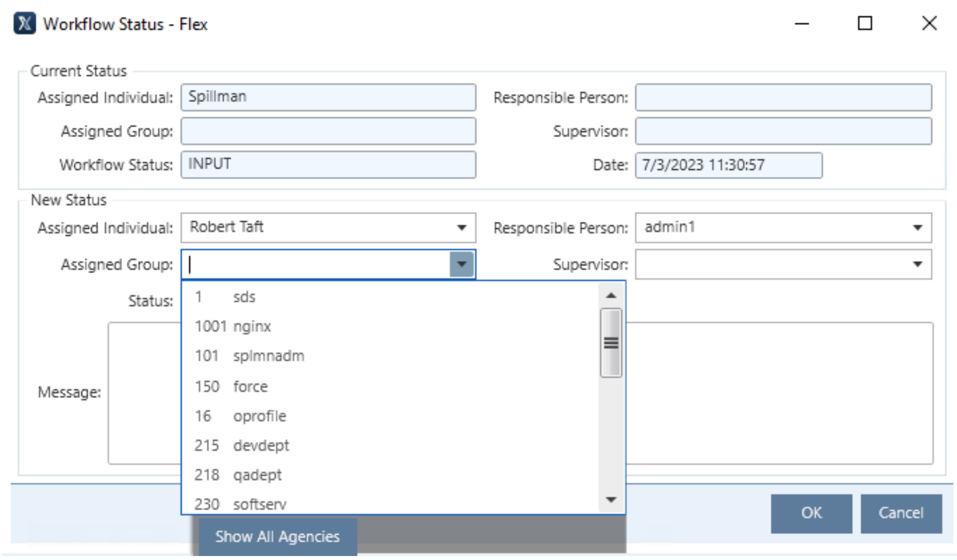
Administrators can now enable Workflow Status drop-down lists to only display individuals and groups assigned to their agency. If there is a need to assign to an individual or group in another agency, the user can select **Show All Agencies**.

When the syparam setting **codefltr** is set to `Yes`, Flex users initially see only users and groups assigned to their agency in the following fields:

- Assigned Individual
- Assigned Group
- Responsible Person
- Supervisor

In the following example, the **Assigned Group** drop-down only shows groups assigned to that user's agency. If the user would like to see all groups, they can select **Show All Agencies**.

Figure 82: Workflow Status Dialog Box



4.7.2
Automatic Unit Status Updates

Depending on agency settings, your unit status may automatically update.

This feature updates based on the following factors:

- Whether or not you are stationary
- Your distance relative to your station or call for service

For more information about configuring the automatic unit status updates, see the *Flex Mobile Administrator Manual* and the *Flex CAD Administrator Manual*.

The following are examples of how automatic unit status updates may function for your agency:

- If you are more than 150 feet from the station and you are in a `PAGED` status, your status automatically changes to `ENRT` (en-route).
- If you are less than 100 feet from a call and are stationary for longer than 10 seconds, your status updates from `ENRT` (en-route) to `ARRVD` (arrived).

4.8
Records

4.8.1
Additional apnames Fields

To increase visibility of a Flex User's CommandCentral account information, we implemented the following changes on the apnames table for email addresses in the 2024.1 release:

- Added the **CmdCentral ID** (**apnames.ccid**) field.

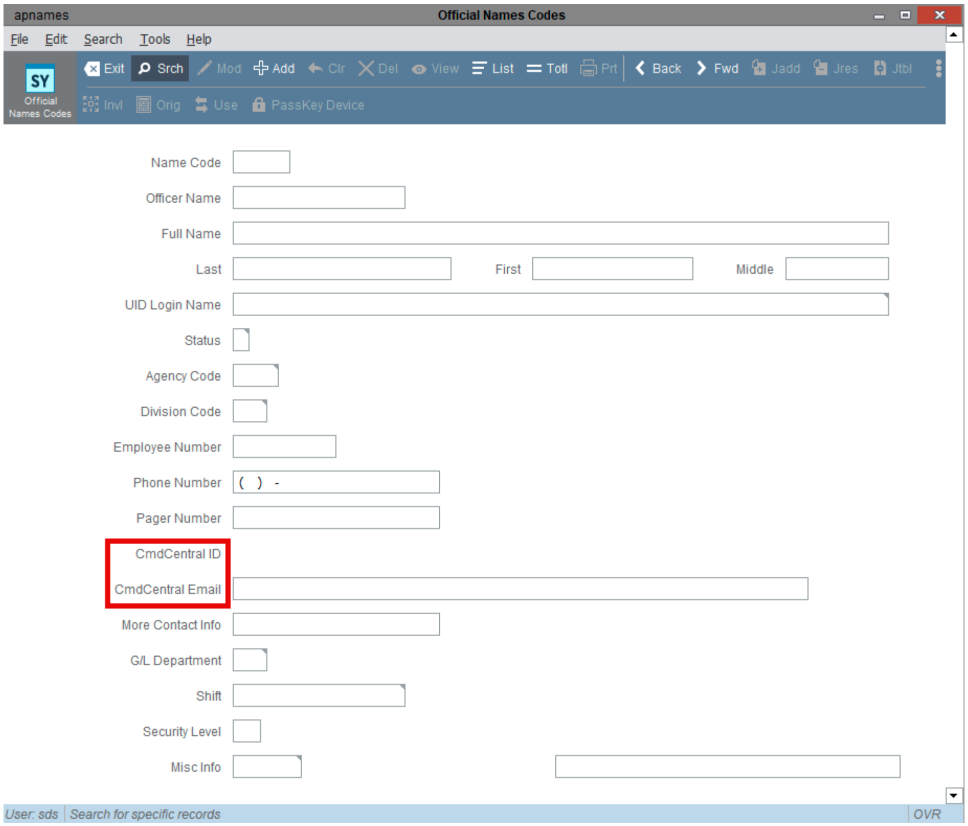
  CmdCentral ID is an ID that uniquely identifies a Flex On-Prem user with their account in CommandCentral. This unique ID cannot be changed or modified, but is displayed for reference purposes.

  This field displays the CommandCentral ID of the user whose information you are modifying.

- Added the **CmdCentral Email** (**apnames.ccemail**) field.

  You can enter users' email addresses for CommandCentral. This field has a 360 character limit.

Figure 83: Added apnames Fields



4.8.2 Assigned Users and Groups by Agency

As of the 2024.1 release, when updating Approvals through the **Update Approvals** or **Update Multiple Approvals** screens, the assigned Individual, Group, Responsible Person, and Supervisor will display by agency if the syparam codefltr is set to `YES`.

4.8.2.1 Admin: Filter Individuals and Groups by Agency

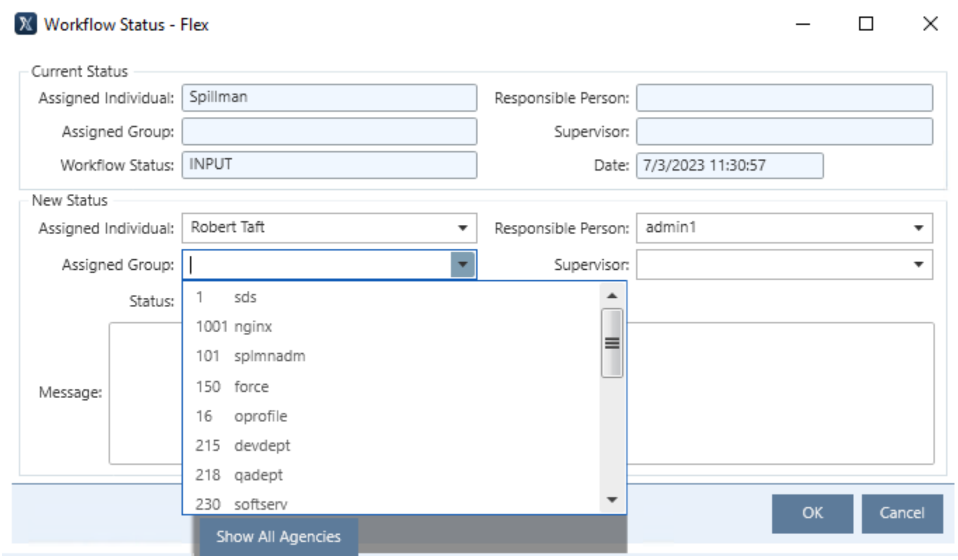
Administrators can now enable Workflow Status drop-down lists to only display individuals and groups assigned to their agency. If there is a need to assign to an individual or group in another agency, the user can select **Show All Agencies**.

When the syparam setting **codefltr** is set to `Yes`, Flex users initially see only users and groups assigned to their agency in the following fields:

- Assigned Individual
- Assigned Group
- Responsible Person
- Supervisor

In the following example, the **Assigned Group** drop-down only shows groups assigned to that user's agency. If the user would like to see all groups, they can select **Show All Agencies**.

Figure 84: Workflow Status Dialog Box



4.8.3
Granular Sync Options for CCAssetSync

We have added additional syncing options to CCAssetSync in the 2024.1 release. These options will allow you to have more control over what digital assets are synced between Flex and CommandCentral Evidence.

Previously, when syncing between Flex and CommandCentral, all digital assets from all tables were synced. Now agencies can choose to only upload files or images from only specific tables. This can be configured per-agency.

We continue to expand the capabilities of syncing digital assets between Flex and CommandCentral, so you can look for additional options in future releases.

One-way Sync from CommandCentral to Flex

- One-way sync from CommandCentral to Flex adds all digital assets that are tagged in CommandCentral Evidence with an incident number to the Flex Incident's **File Capture** window.
- Digital assets are not downloaded from CommandCentral Evidence to Flex, only its metadata.

One-way Sync from Flex to CommandCentral

- One-way sync from Flex to CommandCentral uploads all digital assets from Flex to CommandCentral Evidence based on an agency's chosen table configuration.
- Once digital assets are uploaded, they are queued for removal from the Flex server based upon settings configured by the administrator in `adminutil`. See the "Setup of Deleting Files from Disk in Flex" section in the *Flex Administrator Manual*. Digital assets and their metadata are not downloaded from CCE to Flex. Files uploaded directly to CCE will not display in Flex, even if they are assigned a Flex incident number.

Two-way Sync between CommandCentral and Flex

- Two-way sync from CommandCentral to Flex uploads all digital assets from Flex to CommandCentral based on an agency's chosen table configuration. Once they are uploaded, they are queued for removal from the Flex server based upon settings configured by the administrator in `adminutil`. See the “Setup of Deleting Files from Disk in Flex” section in the *Flex Administrator Manual*.

- All digital assets are tagged in CommandCentral with an incident number and are added to the Flex Incident’s **File Capture** screen.
- Digital assets are not downloaded from CCE to Flex. Only metadata is added to Flex.

4.8.3.1
Admin: Configuring Data Sync for CCAssetSync

To enable data sync for CCAssetSync, complete the following actions:

Procedure:

1. On the WebApp manager, navigate to **/CCAssetSync**.

   A list of agencies missing a sync configuration and that can be configured by CCAssetSync appears.

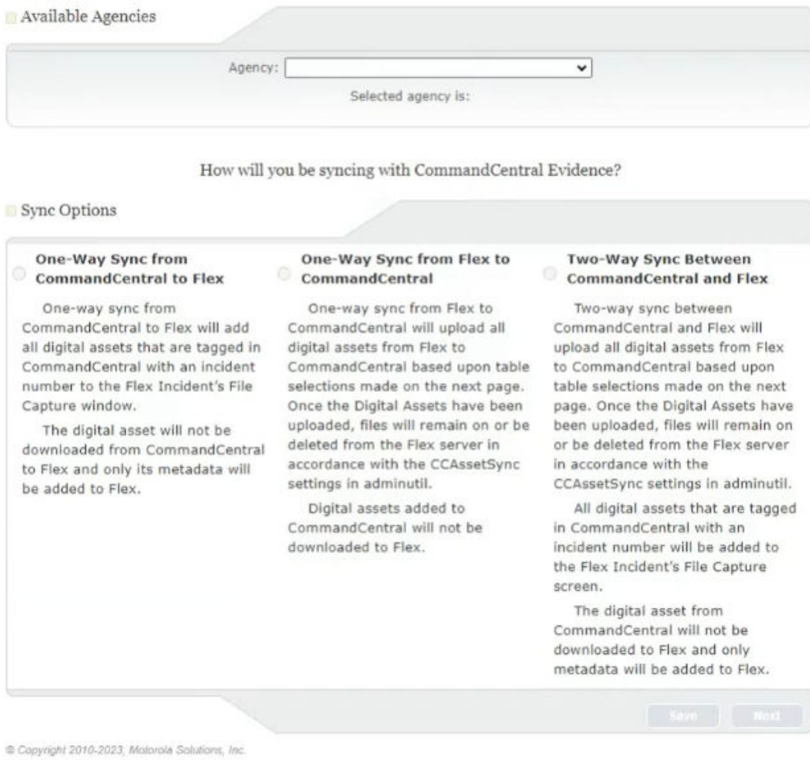
2. Click the **Sync Configuration** button.

   The following sections appear:

Table 22: Sync Configuration Sections

Section	Description
Available Agencies	In this section you can select the agency you want to configure.
Sync Options	In this section you can view the various options for sync configuration.

Figure 85: Sync Configuration Sections

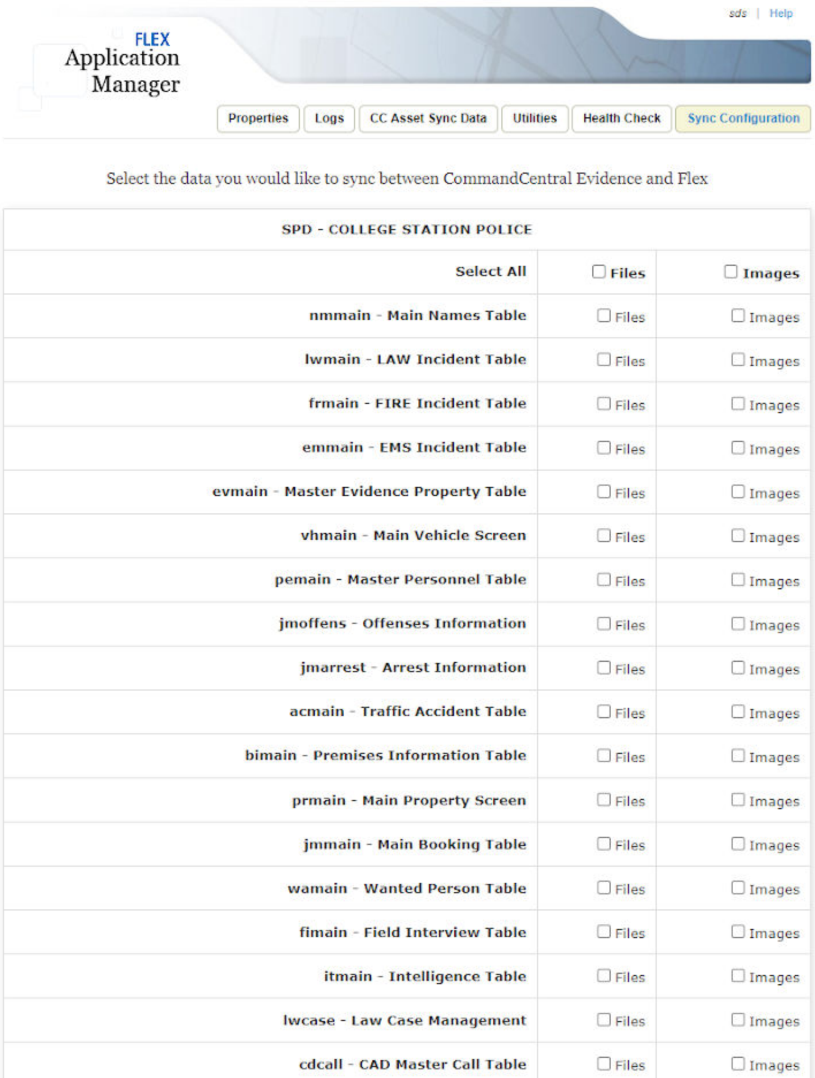


3. Click the **Agency** drop-down menu and select the agency you want to configure.
4. In **Sync Options**, choose one of the options.

If...	Then...
If you want to sync from CommandCentral to Flex,	perform the following actions: **a.** Select **One-Way Sync from Command-Central to Flex**. A pop-up window appears, prompting you to confirm your choice. **b.** Click **OK**. **c.** Click **Save**. **d.** Go to step 6.

<table>
<tr><th>If...</th><th>Then...</th></tr>
<tr><td>If you want to sync from Flex to CommandCentral, or bi-directional sync from Flex and CommandCentral,</td><td>perform the following actions:
a. Choose from:
● Click One-Way Sync from Flex to CommandCentral.
● Click Two-Way Sync Between CommandCentral and Flex.
A pop-up window appears, prompting you to confirm your choice.
b. Click OK.
c. Click Next.
d. Configure which tables you want to sync.
IMPORTANT: If you later stop syncing tables you chose to sync during this step, previously synced information remains shared in CommandCentral.
A list of tables that have files or images attached appears.
e. Select the Image check box to sync the files in the Images screen for the respective table, or the Files check box to sync files in the Files screen for that table.
When configuring a Data Sync setting for a host that includes multiple agencies pushing data to CommandCentral, you cannot select to sync files from the nmmain - Main Names Table. This can only be configured at the host agency level since it is the host agency database that retains all the nmmain records.</td></tr>
</table>

Figure 86: Data Sync Options

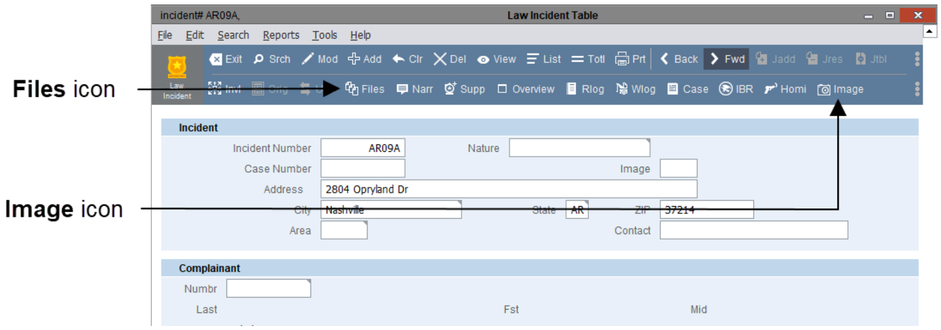


NOTE:
Digital Assets in Flex can be placed in two different screens:

- **Files** screen
- **Images** screen

The **Files** screen can be accessed by clicking the **Files** icon and the **Image** screen can be accessed by clicking **Image** icon.

Figure 87: Law Incident Screen Files and Image Icons



You can add photos, images, and other digital files to the **Files** screen, but only photos and images can be added to the **Image** screen. It is the responsibility of the agency to set expectations and policy as to what should be stored in which location.

5. When you are done making your selections, click **Save** at the bottom of the screen.

   When you configure your sync options for all agencies, the missing sync message no longer displays.

6. To view the data sync status, navigate to the **Status Record Detail by Agency** section at the bottom of the **CCAssetSync Data** page.

   Figure 88: Status Record Detail by Agency

STATUS RECORD DETAIL BY AGENCY

Agency	Uploaded	Remaining	Failure - Will Retry	Failure - Won't Retry	Not Syncing
▴ COLLEGE STATION POLICE - SPD	0	0	0	0	1770
vhmain - Main Vehicle Screen	0	0	0	0	6
bimain - Premises Information Table	0	0	0	0	8
pemain - Master Personnel Table	0	0	0	0	19
fimain - Field Interview Table	0	0	0	0	3
prmain - Main Property Screen	0	0	0	0	8
lwmain - LAW Incident Table	0	0	0	0	1051
cdcall - CAD Master Call Table	0	0	0	0	1
evmain - Master Evidence Property Table	0	0	0	0	12
frmain - FIRE Incident Table	0	0	0	0	39
acmain - Traffic Accident Table	0	0	0	0	105
nmmain - Main Names Table	0	0	0	0	454

* Only stored since last webapp reload

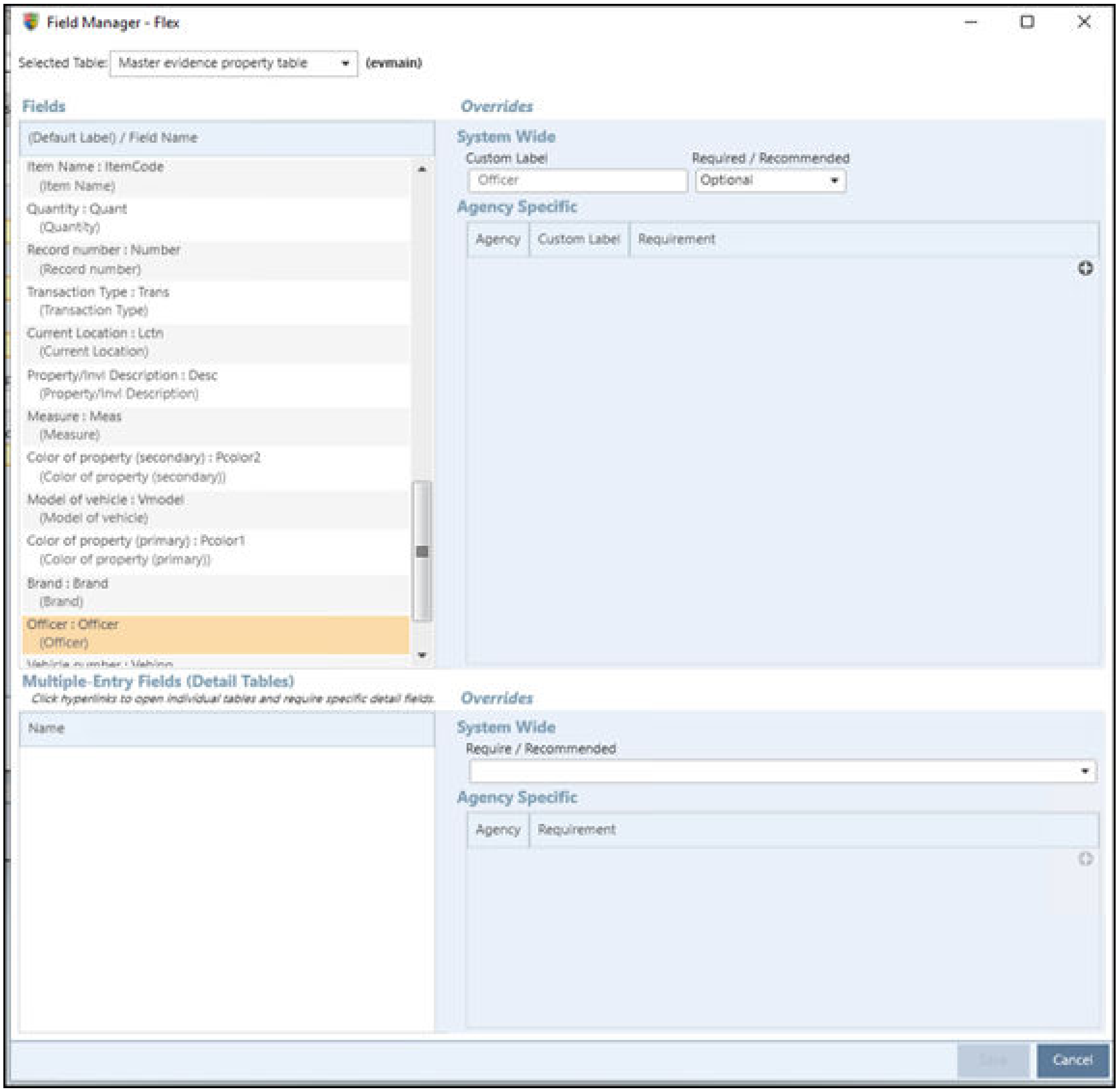
7. To see the status for each table that is being synced, expand an agency.

   NOTE: The number of files under the **Not Syncing** column for the agency reflects all files not being synced, including files from other tables that have not been configured to sync.

4.8.4
Field Manager Enablement for Evidence Table

Fields in the **Evidence** tab (**evmain**) on the **Mobile Law Incident** screen can now be modified using Field Manager.

Figure 89: Field Manager



Field Manager allows administrators to set fields as required or optional. From the Required/Recommended drop-down menu, admins can select **Required** or **Optional**.

Users can also set custom labels for field titles in the **Custom Label** text box.

For more information about using Field Manager, see the *Flex Mobile Administrator Manual*.

4.8.5
File Capture Screen Updates

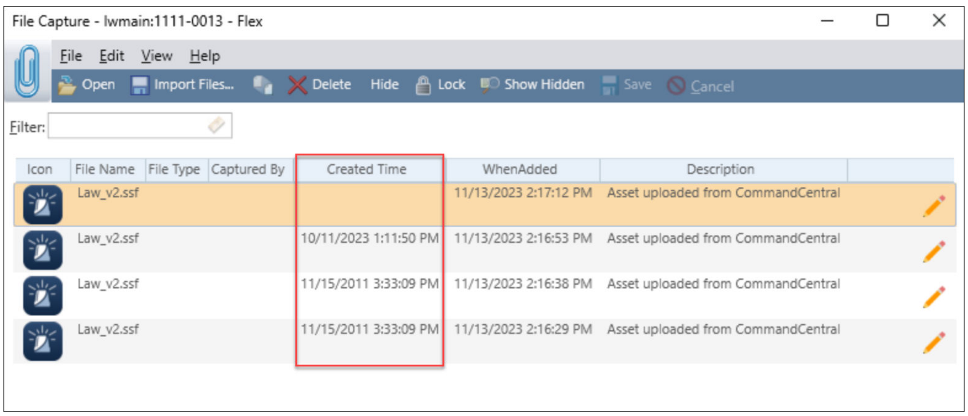
We have enhanced the File Capture Screen with an additional column for `Created Time`.

If a file uploaded through Flex Desktop contains EXIF created time data, that will now be displayed in this column to show the date/time that the file was created, and not just the date/time the file was uploaded to Flex.

For those agencies that are syncing digital assets with CommandCentral Evidence (CCE), the `Created Time` column will display the created date/time of the file from CCE, and the `WhenAdded` column will display the date/time that the file was added to Flex.

We will be adding additional columns in future releases enabling agencies to have a better understanding of their digital assets in Flex.

Figure 90: Updated File Capture Screen



4.9
Reports

4.9.1
New and Updated Reports

We added new reports, made enhancements to certain reports according to customer feedback, and eliminated errors that were reported to us by users.

Reports beginning with `rp` are accessible by users with appropriate sypriv privileges from the Flex command line by entering the file name without any extension. Example: `rpevchr`

Reports with file names the same as the screen names are accessible by clicking the **Print** button on the respective screens.

Any report with an `.x` extension is printed in a PDF format, and any report with an `.r` extension is printed in a fixed-width text format.

New Reports

- `lwcase.x1` – **Case Management Detail Report**
  - Detailed case information for the Case Management table. Includes the Notes section.
- `RPEMCD (.q/.x1f/.x1e/.rcsv)` – **EMS Incident Breakdown**

- Detailed incident report options using the EMS table (.x1e), and the fire table (.x1f). Also there is a csv option using the EMS table (.rcsv).

- `RPJLSMCR (.q/.r1/.x1)` – **State Monthly Confinement Report**
  - Provides daily confinement information including sentencing counts and previous month data.
- `RPEVTRK (.q/.x1)` – **Evidence Tracking Report**
  - Allows a list of evidence based on specified criteria.
- `RPJLOWP (.q/.x1)` – **Jail Event Activity Report**
  - Data from the jllog, breakdown of activity by Officer.

New/Updated Reports

- `RPWARANT (.r1/.x1)` – **Warrant Worksheet Report**
  - Fixed column widths to prevent text overlap. Also fixed translations for SMT section (both formats).
- `RPLWDIR (.x1)` – **Detailed Incident Report**
  - Added incident number to header.
- `RPTINFO (.r1)` – **Report Information Report**
  - Fixed eval from $* to $.

Updated Reports

- `RPTRDATC (.x3/.rpd3)` – **TX Demographic Traffic Stop Report (Sandra Bland .x3)**
  - NC State Traffic Stop Demographic report - formatted for State Submission (.rpd3).
- `RPCDANAL (.rlaw/.rems/.rfir)` – **Response Time Call Detail Analysis**
  - CSV output for response times and detailed incident information.
- `RPCDTCCR (.q/.r1/.x1)` – **Total CAD Calls Received**
  - Updated to reflect the agency in RLMAIN instead of restricted to only incidents when using the agency filter.

4.10 Touch

4.10.1 10-21 Police Phone Dialing Integration

If you have the 10-21 Police Phone application downloaded, you can now select a phone number within the Touch application and call from the 10-21 application instead of using the device's phone number.

This functionality works with any US-based 10-digit phone number and is great for officer privacy.

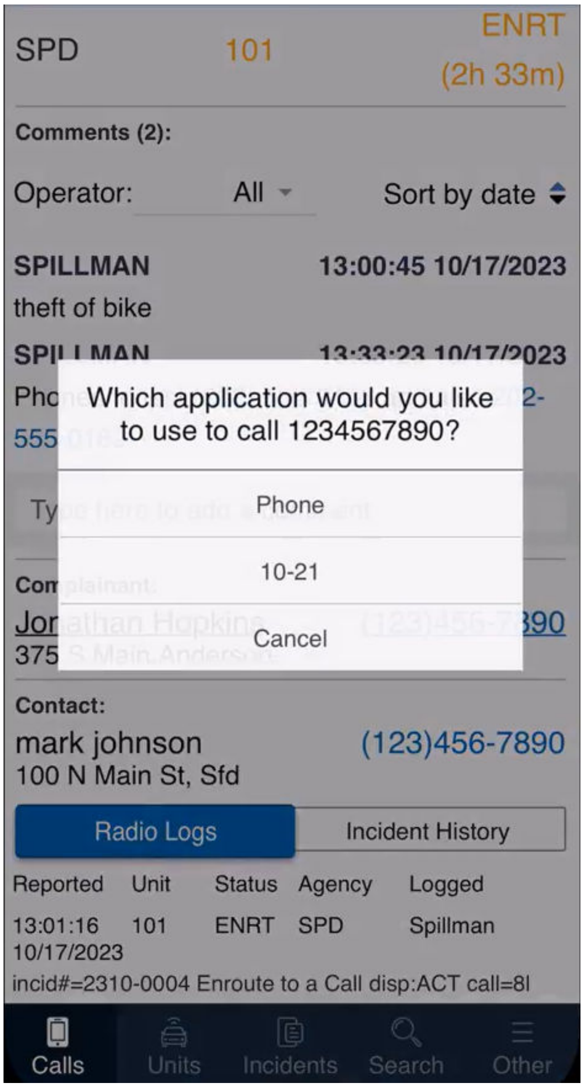
You can call numbers through 10-21 by tapping on any 10-digit number within the Touch application. For more information, see Launching 10-21 Police Phone by Tapping Phone Numbers in Touch on page 122.

4.10.1.1
Launching 10-21 Police Phone by Tapping Phone Numbers in Touch

Procedure:

1. Tap any US-based 10-digital number within the Touch application.
2. Select **10-21**.

   Figure 91: Choosing Application Pop-up Window



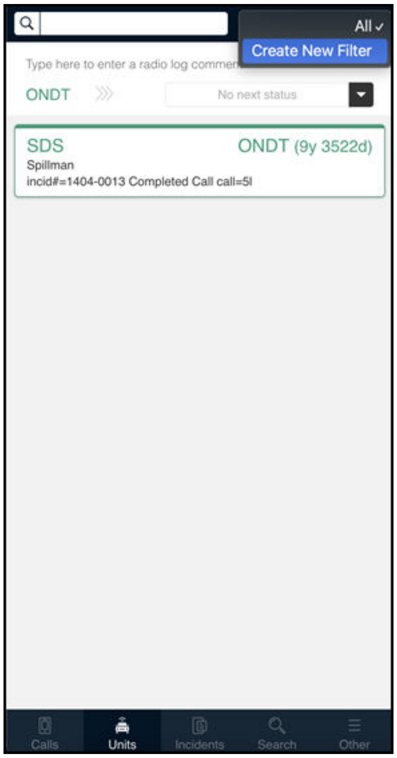
The 10-21 Police Phone application launches.

4.10.2 Custom Filters by Agencies, Zones and Types

Users now have the ability to create, name, edit, and delete custom filters on the **Units** screen.

This ability allows users to filter the units displayed by Agencies, Zones, and Types. Users can create a new filter by tapping **All** on the upper right corner of the **Calls** screen, then selecting **Create New Filter** from the drop-down menu.

Figure 92: Dropdown Menu – New Filter Option



After selecting the **Create New Filter** option, the **Unit Filters** screen displays.

Figure 93: Unit Filters Page

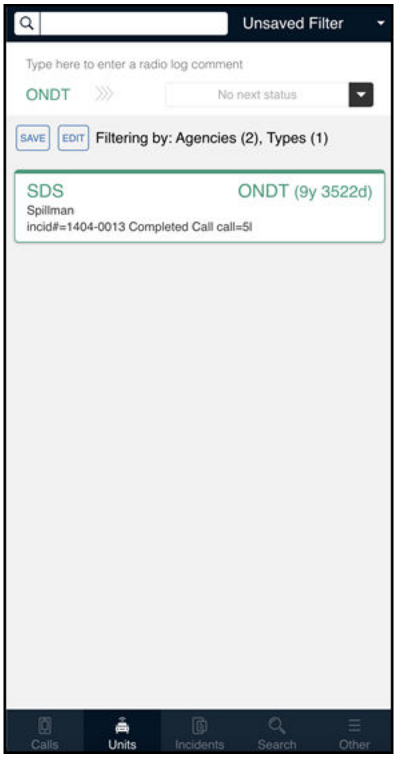
The **Unit Filters** page displays the following sections:

- **Agencies** – Users can tap **Agencies** and select the check boxes next to agencies they want to see on the **Calls** screen. Users can search for specific agencies in the search bar if needed.
- **Zones** – Users can tap **Zones** and select the check boxes next to zones they want to see on the **Calls** screen. Users can search for specific zones in the search bar if needed.
- **Types** – Users can tap **Types** to allow only certain types of calls to appear on the **Calls** screen. Users can select multiple check boxes next to any of the following types:
  - **Law**
  - **EMS**
  - **Fire**
  - **Misc**

To clear any of these filter selections, users can tap **Clear All** at any time. To apply these settings to the **Call** screen, users can tap **Apply**.

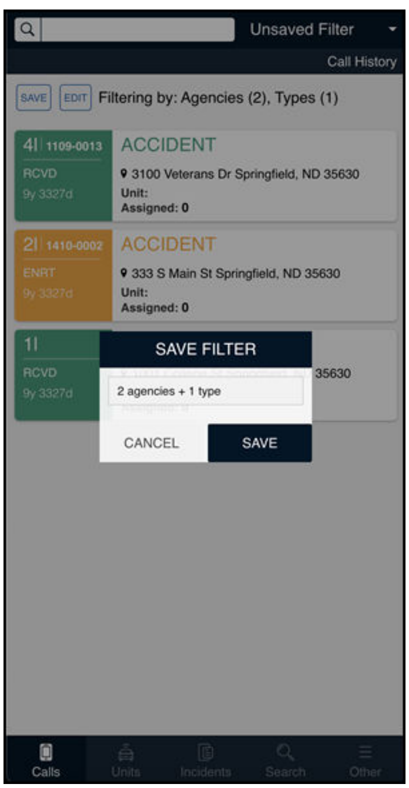
Upon tapping **Apply**, the user returns to the **Call** screen and this new filter displays as **Unsaved Filter** in the top right of the screen.

Figure 94: Calls Screen - Unsaved Filter



To save this custom filter, users can tap the **Save** button. This opens the **Save Filter** window. The user can type a name for the new filter and tap **Confirm** to save it.

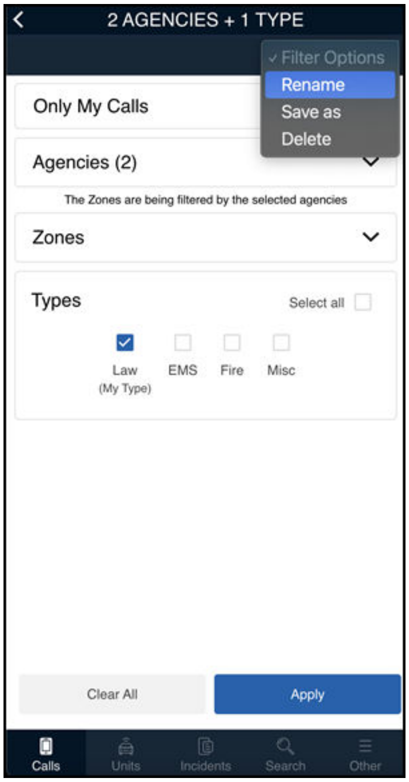
Figure 95: Save Filter Window



This new filter automatically applies to the **Calls** screen and also displays in the drop down menu when the user taps the name of the filter on the top right corner.

To delete, rename, or make adjustments to an existing filter then save it as a new custom filter, users can tap the name of the filter on the **Calls** screen. This opens the screen for the custom filter where users can tap the **Filter Options** button.

Figure 96: Filter Options Menu



To rename a filter, users can tap the **Rename** button and adjust the existing filter name in the text field.

To delete a filter, users can tap the **Delete** button. After tapping the **Delete** button, the **Delete Filter** dialog box displays with a message similar to `Are you sure you want to delete the custom filter?` Users can tap **Confirm** to delete the filter, or **Cancel** to return to the previous screen with no changes.

To make adjustments to an existing filter and then save it as a new custom filter, users can make any necessary adjustments to the **Agencies**, **Zones**, and **Types** sections, then tap the **Save As** button. The user can type a name for the new filter and tap **Confirm** to save it. This new filter automatically applies to the **Calls** screen and displays in the dropdown menu when the user taps the name of the filter on the top right corner of the **Calls** screen.

No matter what filters a user applies to calls, they always see their assigned calls. At this time, custom call filters are saved for the signed-in user.

4.11
StateLink

4.11.1
State Specific Updates

The following updates have been completed for the following states:

Table 23: StateLink Updates

State	ID	Description	StateLink Version
AZ	SLT-9747	Custom TOC ID implementation	1.0
CA	SLT-9743	CA DOJ Purpose Code field added	2.0
VT	SLT-9740	Nlets NIEM update (In-State Vehicle Registration)	2.0

Chapter 5

Release 2023.4

This chapter presents changes made to Flex for the 2023.4 release.

5.1 CAD

5.1.1 The MOV Command

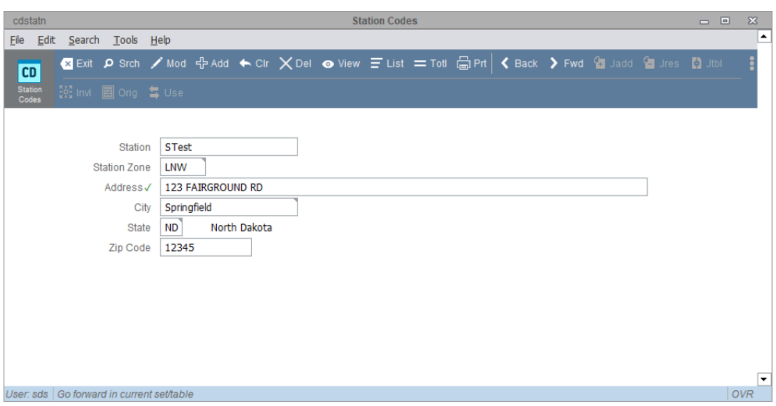
The MOV command (move unit(s) to another station) allows dispatchers to change a unit's station and zone through a single command on the command line. As of the 2023.4 release, this feature can be enabled for CAD users. The command changes the unit's station in the **syunit** table only, so the station listed in the **cdunit** table remains unchanged.

The command format is: `mov {unit,unit,... {h}{station}}`

Multiple units can be moved to the same station at once by separating them with a comma. The `h` character is used to move the unit(s) back to their "home" station listed in **cdunit**.

As of the 2023.4 release, the **cdstatn** table has been extended to include more information than just the station code.

Figure 97: Extended cdstatn table



For the MOV command to work, at least **Station Zone** must be configured for each station. If no zone exists for the station, an error message appears below the command line.

5.1.1.1 Admin: Enabling the Use of the MOV Command

As of the Flex 2023.4 release, you can enable CAD users to move units between stations and zones by using the MOV command.

Beginning with the Flex 2023.4 release, the **cdstatn** (**Station Codes**) table is extended to include more information than just the **Station** code:

- **Station**

- **Station Zone** (coded from **tbzones**)
- **Address**
- **City** (coded from **apcity**)
- **State** (coded from **apstate**)
- **Zip Code**

For the MOV command to work, in addition to **Station** you must configure at least **Station Zone** for each station that can be involved in the movement of units.

Prerequisites: Ensure that each unit has its zone and its “home” station set in the **cdunit** (**Units**) table.

Procedure:

In the **cdstatn** table, perform the following actions:

a. In the **Station** field, enter the station name.

Station names can have spaces but no special characters are currently supported.

b. In the **Station Zone** field, enter the zone of the station.

The **Station Zone** value is coded from the **tbzones** table.

c. Optional: Complete the remaining fields.

d. Optional: In the `Module.CAD.MoveCommandUnitStatus` adminutil setting, specify which status of the unit changes after using the MOV command.

By default, the value of the setting is empty, which means that the unit(s) status will not change from its current status. By changing the value to a tb10code, you can select the required change of the unit(s) status.

5.1.1.2

Using the MOV Command Moving Units Between Stations

As of the Flex 2023.4 release, CAD users are able to move units between stations and zones by using the MOV command.

Prerequisites:

- Contact your admin if the feature is enabled at your agency. In the extended **cdstatn** (**Station Codes**) table, each station involved in the movement of units must have an assigned **Station Zone** code. When an error message saying that no zone is set for a station appears under the command line, contact your admin.
- For the following scenarios, let us assume that:
  - The **cdstatn** table for each of the stations Stat1, Stat2, and Stat3 contains the **Station Zone** code: `Zone1`, `Zone2`, and `Zone3`, respectively.
  - In the **cdunit** table, the **Primary Zone** of the unit 101 is `Zone1` (displayed in the Zone column of the **CAD Unit Status** window).
  - In the **syunit** table, the current **Station** of the unit 101 is `Stat1` (the “home” station of this unit from the **cdunit** table).
  - In the **cdunit** table, the **Primary Zone** of the unit 102 is `Zone2` (displayed in the Zone column of the **CAD Unit Status** window).
  - In the **syunit** table, the current **Station** of the unit 102 is `Stat2` (the “home” station of this unit from the **cdunit** table).

- In the **cdunit** table, the **Primary Zone** of the unit 103 is `Zone3` (displayed in the Zone column of the **CAD Unit Status** window).
- In the **syunit** table, the current **Station** of the unit 103 is `Stat3` (the “home” station of this unit from the **cdunit** table).

Procedure:

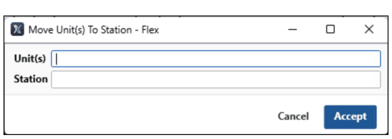
Choose from:

- If you want to move the unit 101 to the station Stat2, at the command line enter:
  `mov 101 Stat2`
  - A confirmation appears that the unit is moved to the new station.
  - In the Zone column of the **CAD Unit Status** window, the current zone of the unit 101 is changed from `Zone1` to `Zone2`.
  - In the **rlmain** table, **Unit Radio Log** for the unit 101 is automatically created with the relevant information in the **Description** field and in the **Incidents** area (in the **Zone** field).
  - In **Officer Radio Log Table** for the unit 101, the zone information is automatically updated, with **Narrative** stating the change of the station to Stat2.
- If you want to move units 101 and 103 to the station Stat2, at the command line enter:
  `mov 101,103 Stat2`
  - A confirmation appears that the units are moved to the new station.
  - In the Zone column of the **CAD Unit Status** window, the current zone of the unit 101 is changed from `Zone1` to `Zone2`, and the current zone of the unit 103 is changed from `Zone3` to `Zone2`.
  - In the **rlmain** table, **Unit Radio Log** for the unit 101 and for the unit 103 is automatically created with the relevant information in the **Description** field and in the **Incidents** area (in the **Zone** field).
  - In the **Officer Radio Log Table** for the unit 101 and for the unit 103, the zone information is automatically updated, with the relevant narratives.
- If you want to move units 101 and 103 from the station Stat2 back to their “home” stations, at the command line enter:
  `mov 101,103 h`
  - A confirmation appears that the units are moved to their stations.
  - In the Zone column of the **CAD Unit Status** window, the current zone of the unit 101 is changed from `Zone2` to `Zone1`, and the current zone of the unit 103 is changed from `Zone2` to `Zone3`.
  - In the **rlmain** table, **Unit Radio Log** for the unit 101 and for the unit 103 is automatically created with the relevant information in the **Description** field and in the **Incidents** area (in the **Zone** field).
  - In the **Officer Radio Log Table** for the unit 101 and for the unit 103, the zone information is automatically updated, with the relevant narratives.

NOTE:

- When you enter only `mov` on the command line, the `Usage` line appears underneath:
  `mov {unit,unit,... {h}{station}}`
- If you enter an incomplete command, a window prompts you to complete it.

  Figure 98: Prompt for Completing Unit(s) and Station

- If a unit or station does not exist, the relevant error message appears.

5.1.2 Covering Zones Enhancements

Covering Zones enhancements can increase the predictability of the recommendations for dispatchers provided by the software. The enhancements simplify the understanding and implementation of the Covering Zones feature. Administrators do not have to choose between Covering Zones and Mutual Aid (or other sort criteria).

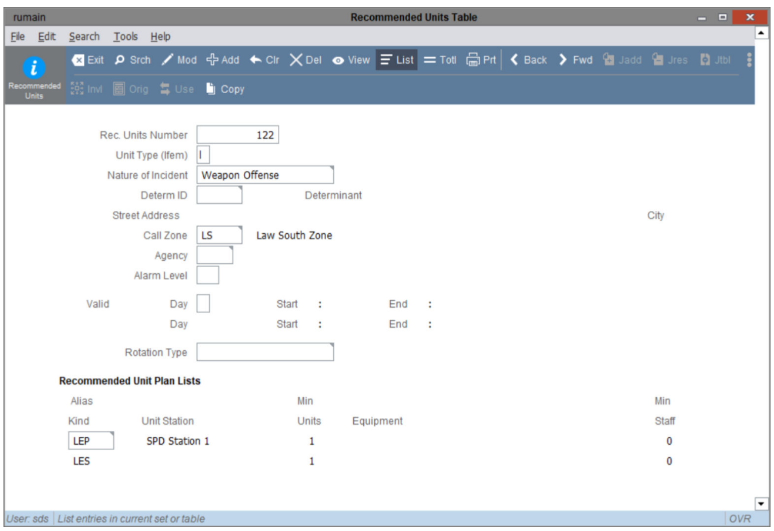
The Covering Zones feature requires the following settings in the Administrator Manager (`adminutil`):

- `Module.CAD.FlexUnitRecommendations.CoveringZonesByAliasKind` – set to `True`
- `Module.CAD.FlexUnitRecommendations.EnableCoveringZones` – set to `True`

Covering Zones Can Now Work with Other Recommended Unit Sort Parameters

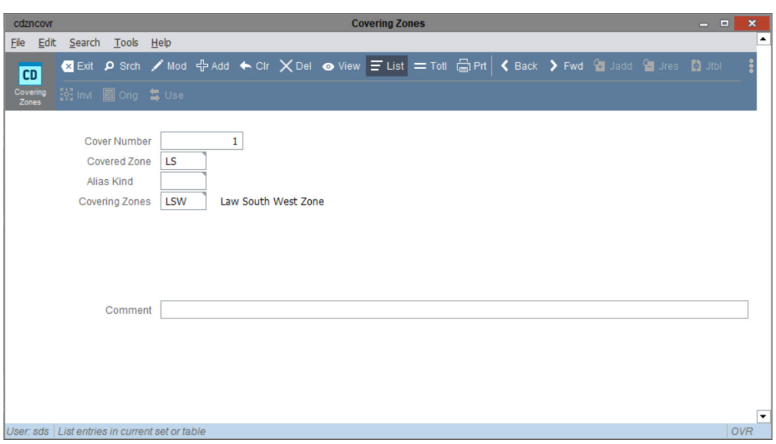
In the following example, prior to the Covering Zones setup, an administrator defined the **Unit Station** in the **Recommended Units Table**.

Figure 99: Unit Station Definition in the Recommended Units Table



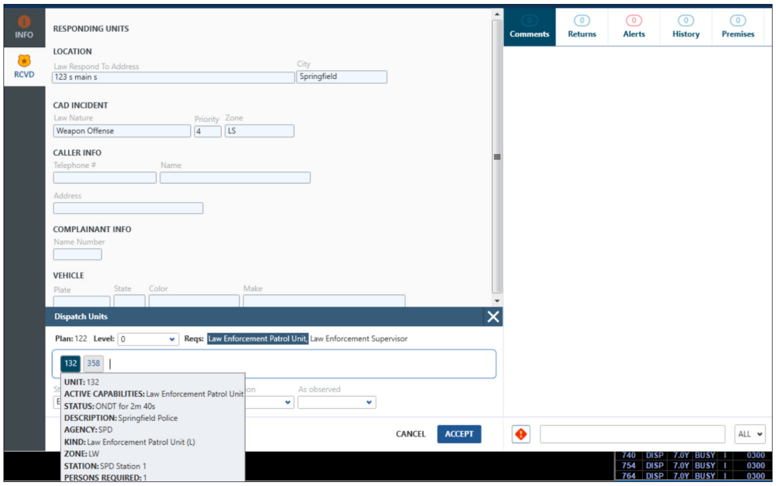
Then, in the **Covering Zones** table, the administrator configured the `LSW` zone.

Figure 100: Covering Zones Configuration (LSW)



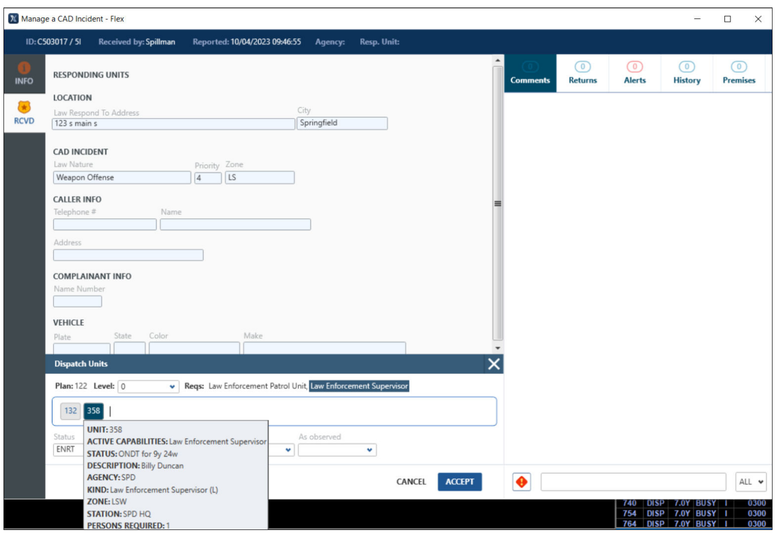
When a dispatcher creates the incident, the following software recommendations appear:

Figure 101: The First Recommended Unit (132)



The first recommended unit is `132` from the `SPD Station 1` that was previously defined in the **Recommended Units Table**.

Figure 102: The Second Recommended Unit (358)



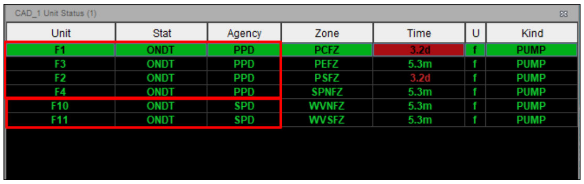
Covering Zones Can Now Work with Mutual Aid Limits

The following scenario is an example of how the software recommends units by using the Covering Zones feature with Mutual Aid limits.

Assumptions:

- The `mutaid` apparam (`Agencies' Mutual Aid Limits`) for the PPD agency is set to `PPD,3,2`
- Two (2) units are available at the SPD agency, four (4) units at the PPD agency.
  In the following figure, the available units are marked with red frames.

Figure 103: Initial Statuses of PPD and SPD Pump Units


CAD_1 Unit Status (1)

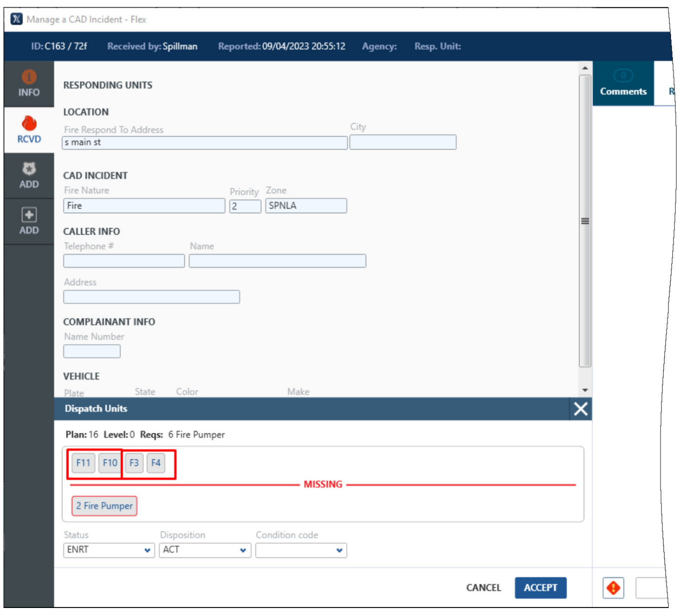
Unit	Stat	Agency	Zone	Time	U	Kind
F1	ONDT	PPD	PCFZ	3.2d	f	PUMP
F3	ONDT	PPD	PEFZ	5.3m	f	PUMP
F2	ONDT	PPD	PSFZ	3.2d	f	PUMP
F4	ONDT	PPD	SPNFZ	5.3m	f	PUMP
F10	ONDT	SPD	WVNFZ	5.3m	f	PUMP
F11	ONDT	SPD	WVSFZ	5.3m	f	PUMP

- A fire incident requires to use six (6) pump units.

Sequence of events:

1. Dispatcher dispatches units to the fire incident.
2. The software recommends the both (2) available units from the SPD agency, but only two (2) from the PPD agency (due to the limit of units per dispatch outside the agency's area set to `2`, even if the agency has more units available).

Figure 104: Units Recommended by the Software



3. As `2 Fire Pumper` units are missing, the software must look for units from other agencies.
4. Let us suppose that due to another fire incident, the dispatcher wants to dispatch next six (6) units.

   The current statuses of the PPD and SPD units are as follows (in the following figure, the available units are marked with red frames):

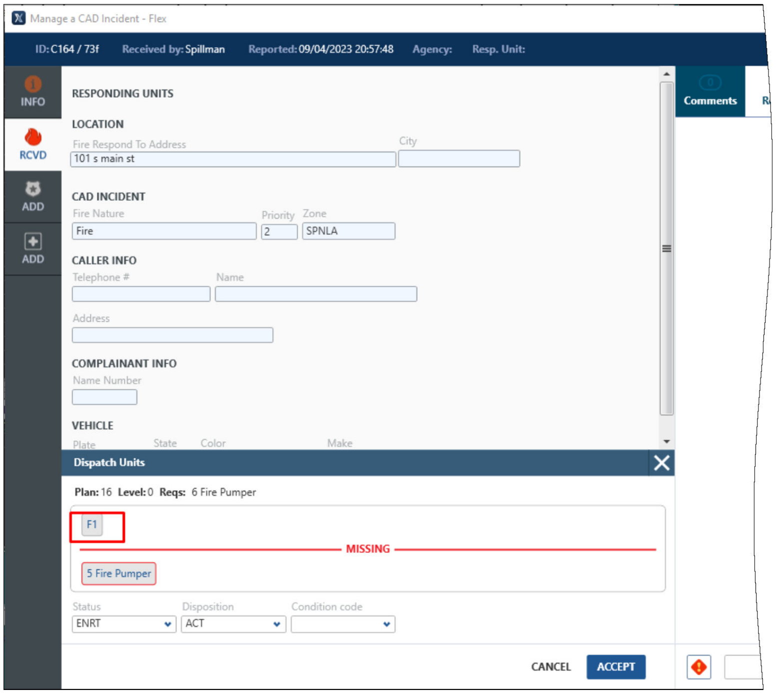
   Figure 105: Current Statuses of PPD and SPD Pump Units


CAD_1 Unit Status (1)

Unit	Stat	Agency	Zone	Time	U	Kind
F1	ONDT	PPD	PCFZ	3.2d	f	PUMP
F3	ENRT	PPD	PEFZ	1.0m	f	PUMP
F2	ONDT	PPD	PSFZ	3.2d	f	PUMP
F4	ENRT	PPD	SPNFZ	1.0m	f	PUMP
F10	ENRT	SPD	WVNFZ	1.0m	f	PUMP
F11	ENRT	SPD	WVSFZ	1.0m	f	PUMP

5. The software recommends only one (1) unit from the PPD agency, even if the agency has more units available. This is due to the maximum number of units allowed outside the area set to `3`, and that two (2) of that limit were already dispatched.

Figure 106: Unit Recommended by the Software



6. As `5 Fire Pumper` units are missing, the software must look for units from other agencies.

5.2
Interfaces

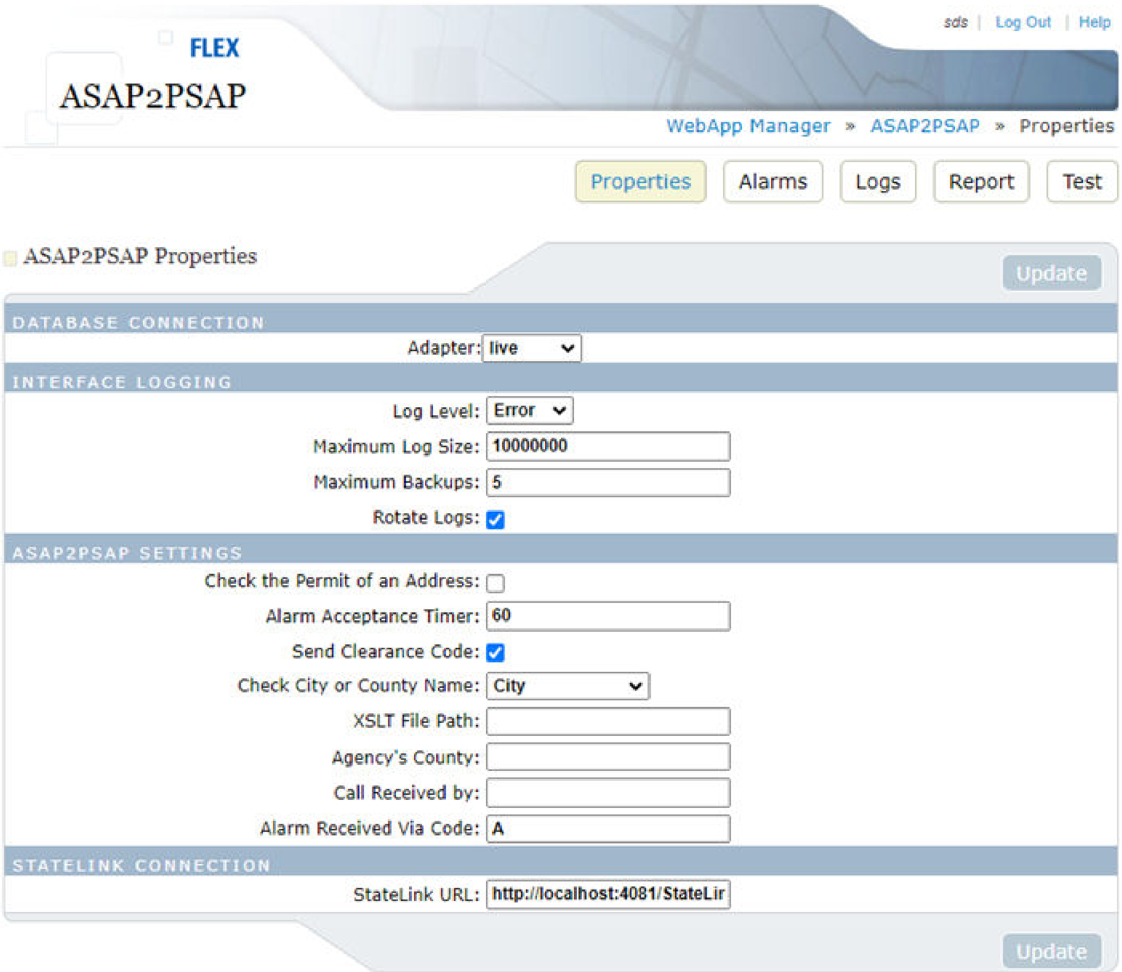
5.2.1
ASAP2PSAP Properties Changes

The WebApp Manager for this release features two changes on the ASAP2PSAP Properties page:

- New **Alarm Received Via Code** field
- **Send Clearance Code** default enablement

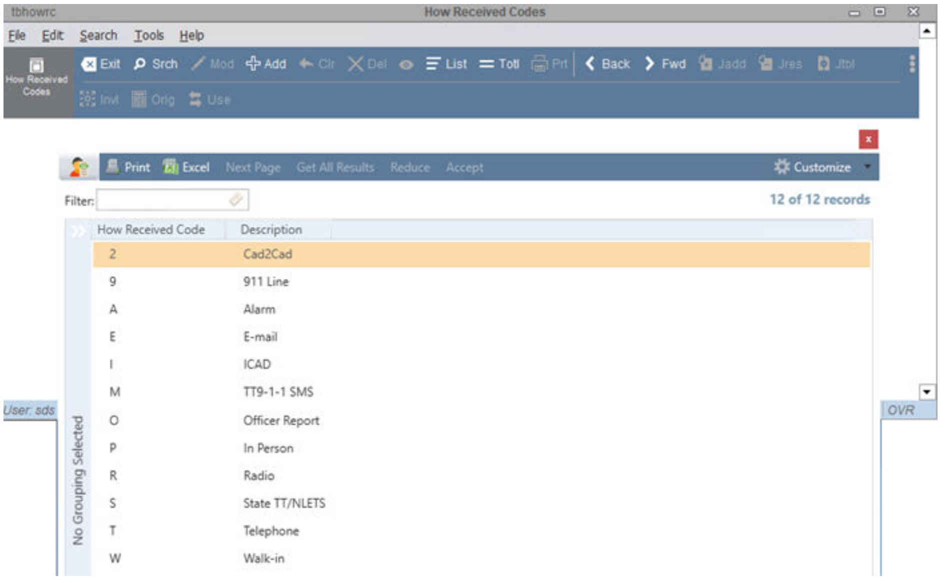
Administrators can configure how alarms are received with a the **Alarm Received Via Code** field under **ASAP2PSAP Settings**.

Figure 107: Alarm Received Via Code Field



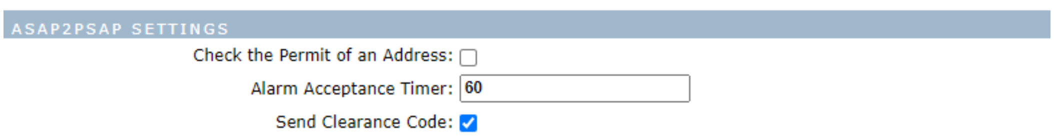
The field allows you to set how alarms are processed by using either an existing or a new code from the **How Received Codes** table (tbhowrc) in the Flex administrator tool.

Figure 108: How Received Codes Table



The **Send Clearance Code** check box is selected by default to send a clearance description along with a confirmation when the call is closed.

Figure 109: Send Clearance Code Check Box



5.2.2 FirstDueFireRMS Interface for First Due

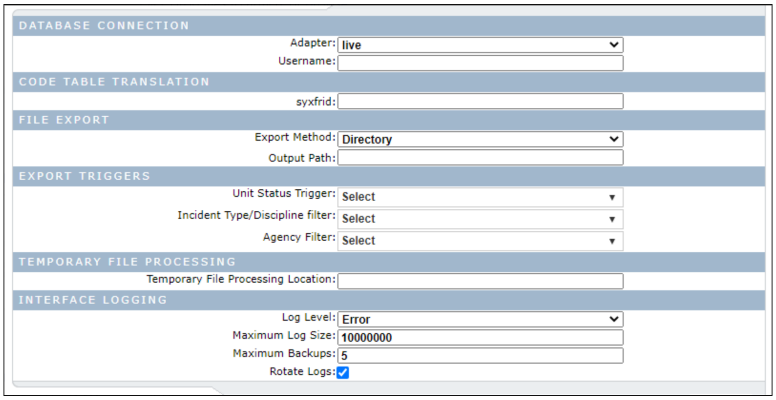
Agencies that use First Due for Fire and EMS reporting, can transfer call and incident data into their platform. This is achieved by using the **FirstDueFireRMS Interface** web app.

FirstDueFireRMS Interface is a new module provided at no additional cost for Flex and First Due customers.

NOTE: The FirstDueFireRMS Interface was formerly known as CADIncidentExport. If your agency currently has CADIncidentExport, note that future enhancements will only be made to the FirstDueFireRMS Interface. Please reach out to Support to switch to the FirstDueFireRMS Interface.

5.2.2.1
Admin: Setting Up FirstDueFireRMS for First Due

Figure 110: FirstDueFireRMS Properties Screen

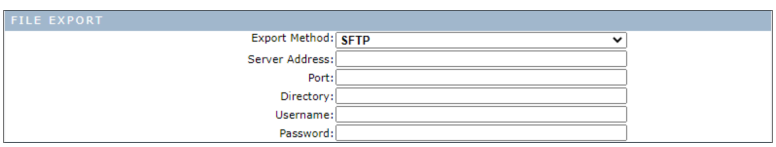


Prerequisites: Confirm that the **FirstDueFireRMS** web app is installed on the Flex server. If it is not, reach out to Technical Support or your Customer Success representative.

Procedure:

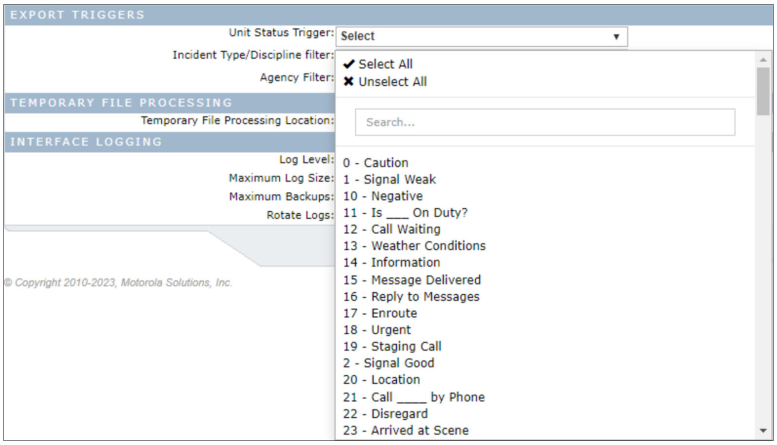
1. Set up **DATABASE CONNECTION** properties:
   a. Ensure that the Adapter is set to the correct database on your system. A typical setting is **live**.
   b. Enter a username with which the web app will communicate with the database. A specific user with specific permissions should be created for use in this field.
2. Set up **FILE EXPORT** properties:

   Figure 111: FILE EXPORT Fields

   a. Select the **Export Method** to be used to send the files to First Due. The recommended export method is **SFTP**.
   b. From First Due, obtain the Server Address, Port, Directory, Username, and Password data and fill in the relevant fields.
3. Set up **EXPORT TRIGGERS** properties:
   a. Select the **Unit Status Trigger** (tb10codes) that will send an update to First Due. You should enter all of the tb10codes that are defined in the **cdstatse** table for the agency(s) that are using this interface.

Figure 112: Unit Status Trigger Selection



b. Select the **Incident Type/Discipline** filter that is defined for the agency(s) sending data to First Due.

c. In the **Agency Filter** field select the agency(s) whose call and incident data you want to send to First Due.

4. Set up the setting by providing the Temporary File Processing Location:

   a. Enter a location on your server in which the XML files can reside until they are transferred to First Due.

      Typically files appear in this folder for less than a second and then are automatically deleted.

5. Click **Save**.

5.2.3

LIDS-CORIS Export Interface Update

The LIDS-CORIS interface exports data from the jail system to be sent to the Virginia LIDS-CORIS, the Local Inmate Data System (LIDS) system.

The interface gathers information on inmates, arrests, offenses, and others on a regular interval determined by your agency. The interface exports a text file that has fixed length values to be transferred to the LIDS-CORIS system.

LIDS-CORIS interface exports the following data from Flex Jail Records:

- Inmate Name Information
- Booking/Inmate Information
- Offense Data
- Name Alias Data
- Gang Data

5.2.4 Rapid Notification 2.0 Send Incident Updates Improvement

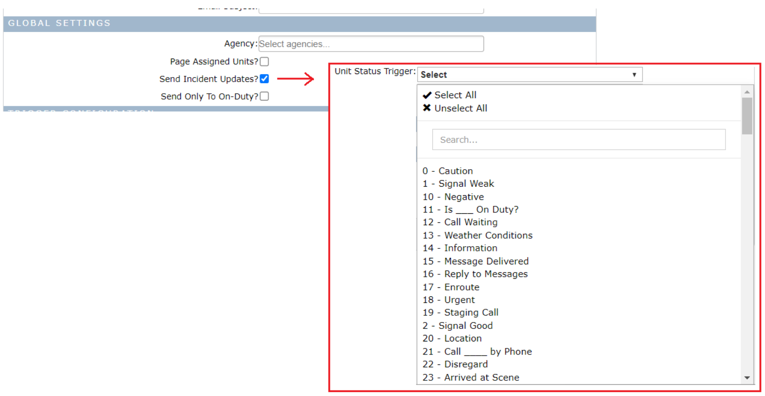
A **Unit Status Trigger** drop-down list now appears when you check the **Send Incident Updates?** check box.

You can customize when incident updates are sent to recipients by selecting unit statuses from this drop down list. You can select as many as needed. This drop-down list displays values from `tb10code.abbr` and `tb10code.desc`.

Message exports only send when the statuses selected in this drop-down are set for a unit in CAD. Previously, incident updates were sent for any incident status change.

The default setting for this new drop-down is **all**. This prevents the breakage of current implementations where exports are sent for all statuses.

Figure 113: Send Incident Updates? Drop-down Menu



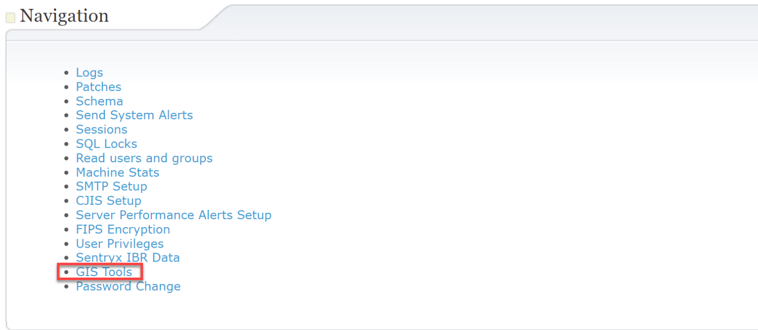
5.3 GeoValidation/Mapping/Quickest Route

5.3.1 Admin: GeoValidation Test Tools in the Spillman and Geobase Webapps

As part of a continuous effort to improve the performance of geovalidation, administrators can now explore new testing tools, especially for ArcGIS Pro that is available as of the 2023.3 release.

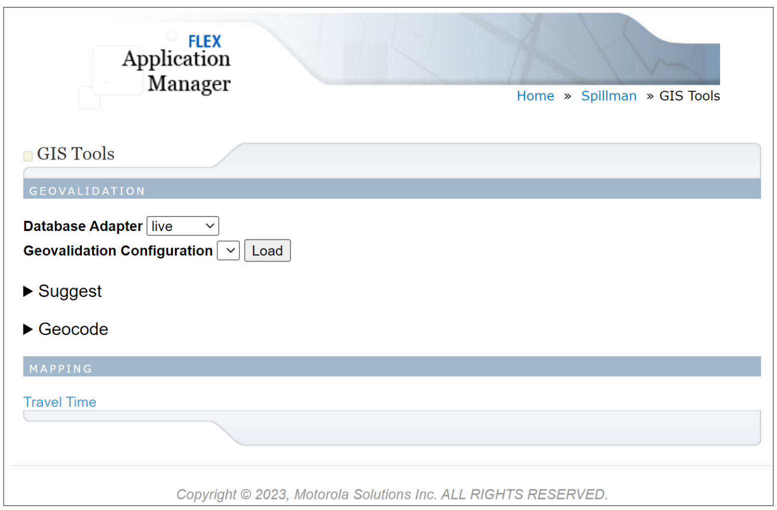
As an administrator, you can access these tools through the Application Server, in the Spillman webapp. The **GIS Tools** link is located in the **Navigation** area.

Figure 114: GIS Tools



When you select the **GIS Tools** link, the following page appears:

Figure 115: GIS Tools Page



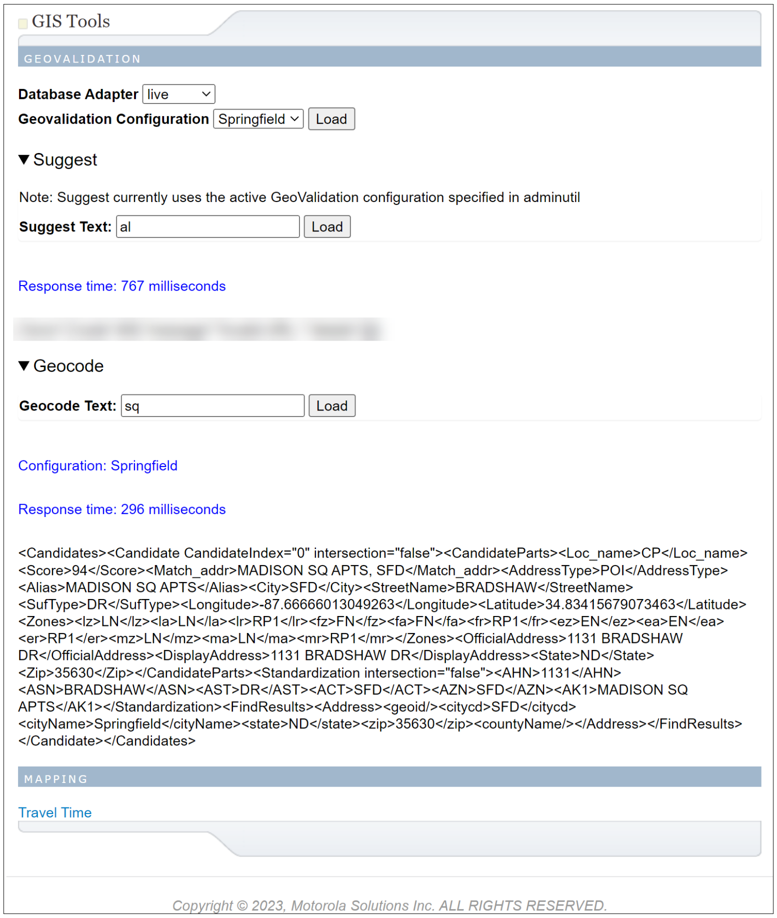
NOTE: The page also provides access to the **Travel Time** functionality, which is moved from the **Superuser Items** area.

In the **GEOVALIDATION** area you can:

- choose a **Database Adapter**,
- choose a **Geovalidation Configuration**,
- expand the **Suggest** and **Geocode** links to test responses to your entries.

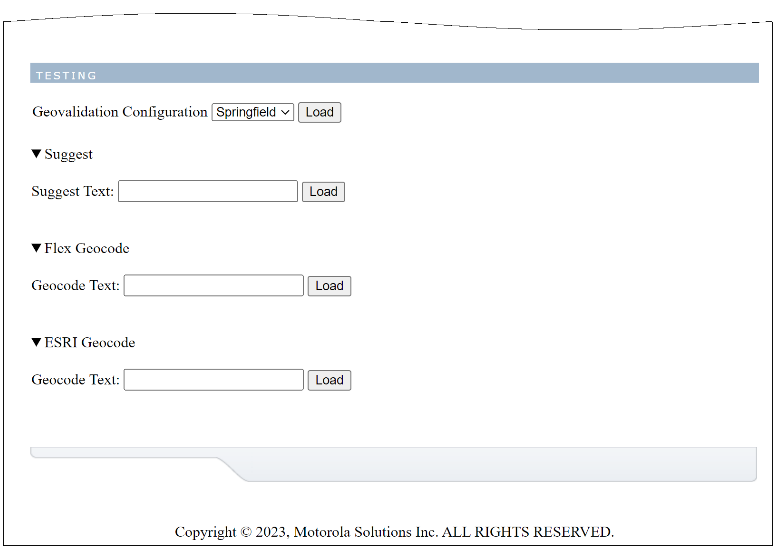
At the current stage, the responses include raw search data and response times, which can help locate problems.

Figure 116: Example Test Results for Suggest and Geocode Entries



The new tools are also available at the bottom of the Geobase page, in the new **TESTING** section.

Figure 117: TESTING Section in the Geobase Webapp



In addition to **Suggest** and **Geocode**, this section contains the **ESRI Geocode** item that allows you to load texts directly to the GIS server, without involving the Geobase webapp.

5.4
Hub/Platform

5.4.1
Recording of Logins to the Flex System

As a reminder, due to CJIS compliance requirements, all successful or unsuccessful login attempts to the Flex system are recorded and stored in the **aplilogin** table. This applies to the Flex Desktop Application, Flex Mobile, Flex Touch, Flex Web Application Server, and DEX API Interface.

5.5
Records

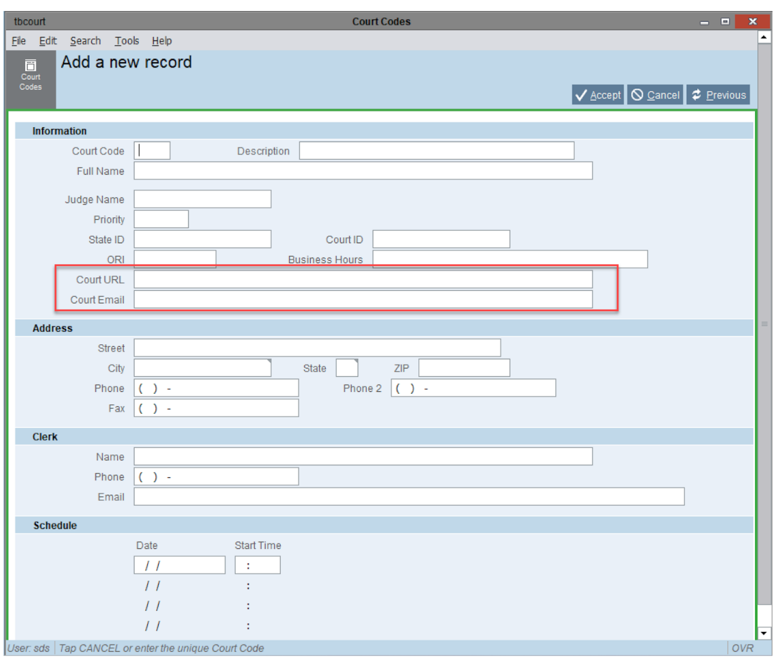
5.5.1
Court Website and Court Email Address Field Additions

The **Court Website** and **Court Email Address** fields were added to the Court Codes (tbcourt) screen.

Table 24: Added Fields

Field	Description
Court URL	Use this field to enter the official website URL of the court
Court Email	Use this field to enter the general email address of the court

Figure 118: Updated tbcourt Screen



5.5.2
Updated Workflow Status Dialog Box

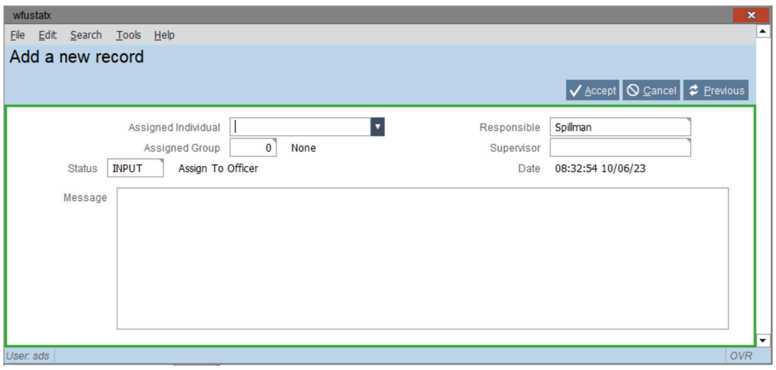
Now you can view only **Assigned Individual**, **Responsible** and **Supervisor** assigned to your agency so as to reduce the number of options when viewing the list.

If desired, you can toggle between agency view and viewing all users on the system by clicking **Show All**. This will benefit multi-agency Flex systems.

This affects the following fields in the **Records Workflow** (**wfustatx**) screen:

- **Assigned Individual**
- **Responsible**
- **Supervisor**

Figure 119: Records Workflow Screen

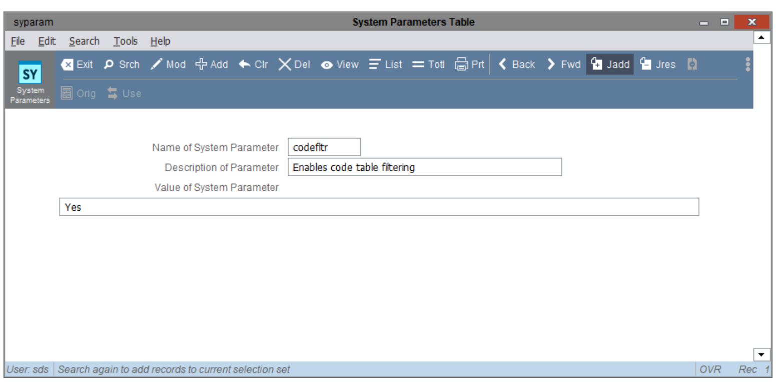


5.5.2.1
Admin: Agency Filtering for Code Tables Activation

Agency Filtering for Users uses the syparam **codefltr** which is also utilized by other dropdowns in Flex.

You can determine whether the **Workflow Status** fields display all system users or only the users from the same agency as the currently logged on user by modifying the syparam codefltr to **Yes**.

Figure 120: System Parameters Table



If this setting is enabled, users first see individuals from their own agencies. Users can see individuals from other agencies by clicking **Show All** (see Agency Filtering on page 144).

5.5.2.2
Agency Filtering

Depending on agency settings, if code table filtering has been enabled, you initially see individuals from your agency when you access the drop-down menus in the following fields in the **Records Workflow** (**wfustatx**) screen:

- **Assigned Individual**
- **Responsible**
- **Supervisor**

You can view all individuals from all agencies by clicking **Show All** when the drop-down menus are open.

NOTE: Agency Filtering for **Assigned Group** in Flex Desktop will be released in a future update.

Figure 121: Records Workflow Screen

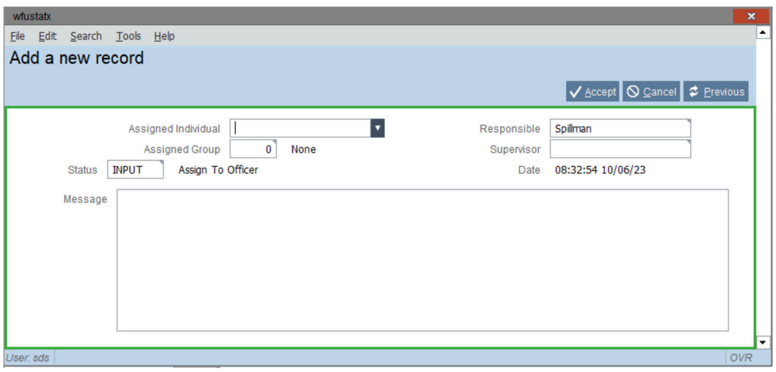


Figure 122: Records Assigned Individual Drop-down

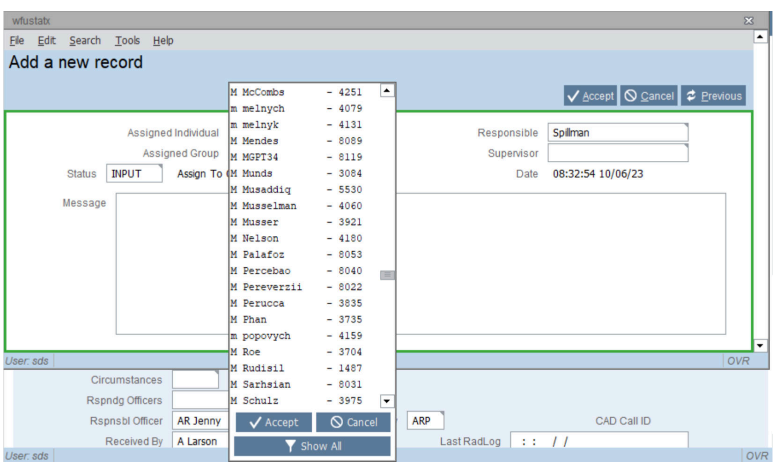
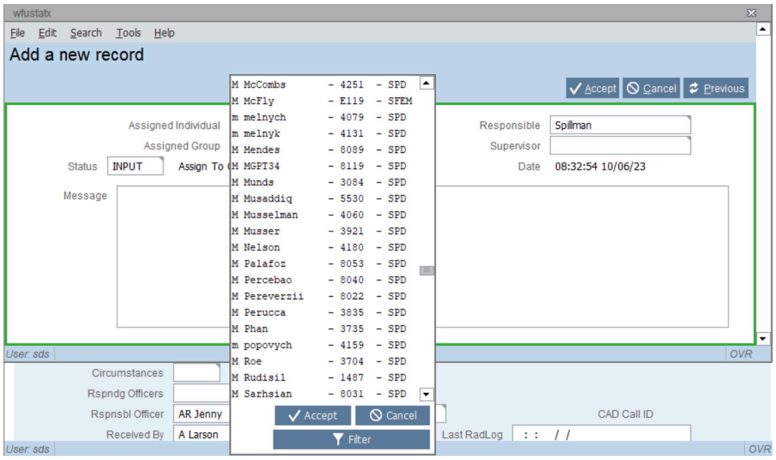


Figure 123: Records Assigned Individual Drop-down with All Agencies



5.6
Touch

5.6.1
Ability to List Calls by Zone and Agency in Touch

You now have more options for how to filter calls on the **Calls** screen.

You can now create and edit multiple filters as needed, filtering calls by **Agency**, **Zone**, and **Type**, such as whether or not they are a Law, EMS, Fire, or Misc (Miscellaneous) call. The filter persists between sessions for each user.

5.6.2
Creating Custom Call Filters

You can filter your calls by various criteria, depending on your needs.

NOTE: No matter what filters you apply to your calls, you always see calls assigned to you. At this time, custom call filters are saved for the signed-in user.

Procedure:

1. From the **Calls** screen, tap **All** in the top-right.

   The following options appear:

   Table 25: Call Filter Options

Option	Description
All	Select this option to display all active calls.
New Filter	Select this option to create a new call filter.

2. Optional: To create a new filter, tap **New Filter**.

   NOTE:
   You can clear your filter information at any time by tapping **Clear All**.

You can edit an unsaved custom filter by tapping the **Edit** button next to the **Filtering by** label at the top of the calls list.

For more information, see Editing or Deleting Custom Call Filters.

3. To save your filter, perform the following actions:
   a. Click on the **Save** icon in the top right of your screen.

      The **Save Filter** window appears, prompting you to name your filter.

   b. In the **Filter Name** field, enter your new filter name.
   c. Tap **Confirm**.

   The saved filter is automatically applied to the **Calls** screen.

   Saved filters also display in the list display when you tap **All**.

Result:
When you apply your filter and return to the **Calls** screen, the **All** button transforms into the **Custom Filter** button, which indicates you are using a custom filter.

5.6.3
UI Updates

Text and background colors for both night and day themes have been made easier to read.

5.7
Jail

5.7.1
E-Signature for Medical Assessments

Flex Jail now includes the ability to accept eSignatures on Medical Assessments.

To enable accepting eSignatures on Medical Assessments, your admin must set up the following settings in the Administrator Manager (adminutil):

- `System.Client.TouchScreenSignatur` – set to `True`
- `System.Client.OfficerSignature` – set to `True`

Principles of operation:

- The logged in user is prompted for a signature. This can be the saved officer signature of the logged in user.
- The system prompts for the inmate signature.
- The signed record is attached to the record as a file attachment.

5.8
IBR

5.8.1
Improved Synopsis Report

Now, you can select multiple months within a given year to obtain a report within a window of time by using the Synopsis Report. The report always reads the database when you click **Run Report**, not cached data. The Synopsis Report was previously tied to the IBR submission process.

Now the report displays previously submitted and updated records and displays all the records for a month (minimum scope) including previously submitted records. The report previously showed updated records with only the contents of the submission file, which could be a partial month.

5.8.2
State-Specific Updates

The following are state-specific IBR updates:

Table 26: State-Specific IBR Updates

State	ID	Description	IBR Version
Iowa	IBR-4835	Updated statute spreadsheet	N/A
California Louisiana	IBR-4522	Fixed 262 errors not being able to submit same offense codes with different statutes	2022.4
Indiana	IBR-4885	Updated statutes	N/A

5.9
InSight

5.9.1
InSight Authentication Encryption

The encryption method for Insight authentication has been enhanced to AES256 encryption.

If your Mobile product does not have encryption enabled, then the InSight password will not be stored and you will have to enter your InSight credentials once per login unless they are the same as your Flex credentials.

5.10
StateLink

5.10.1
State Specific Updates

The following updates have been completed for the following states:

Table 27: StateLink Updates

State	ID	Description	StateLink Version
ID	SLT-9453	Idaho QNP Screen	2.0
AZ	SLT-9474	Decommissioned SOPQ and SORI Screens	1.0
IA	SLT-9465	Released StateLinkIA 2.0 Package	2.0

5.11
Mobile

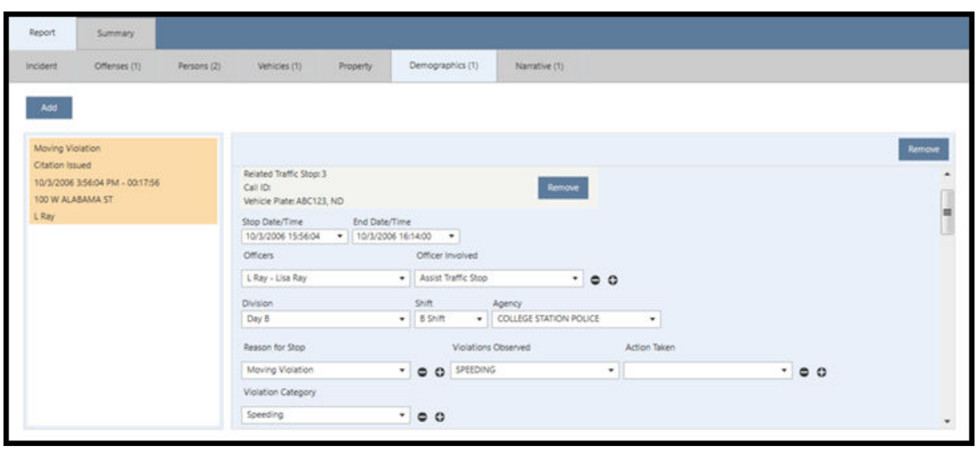
5.11.1
Demographics Summary Data Entry in Mobile Law

As of the 2023.4 release, you can access the Demographics tab from the Mobile Law Incident Screen. This allows officers to fill out demographic information while deployed in the field without access to the Flex Desktop.

Admin: Setup

The **Demographics** tab is automatically enabled. The demographics tab can be added or removed by going into adminutil and modifying the **Module.FR.ActivateDemographicsInIncidentForm** to `true` or `false`. If the administrator changes the setting to `false`, the **Demographics** tab does not display.

Figure 124: Demographics Tab in Mobile Law Incident

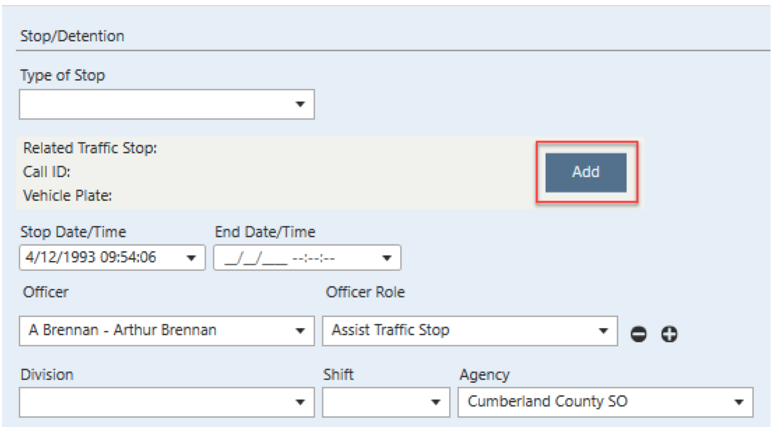


User

The Flex Mobile **Demographics** tab contains the same information fields as the Flex Desktop **Demographics Summary** screen. Additionally, users can perform the following actions on the **Demographics** tab:

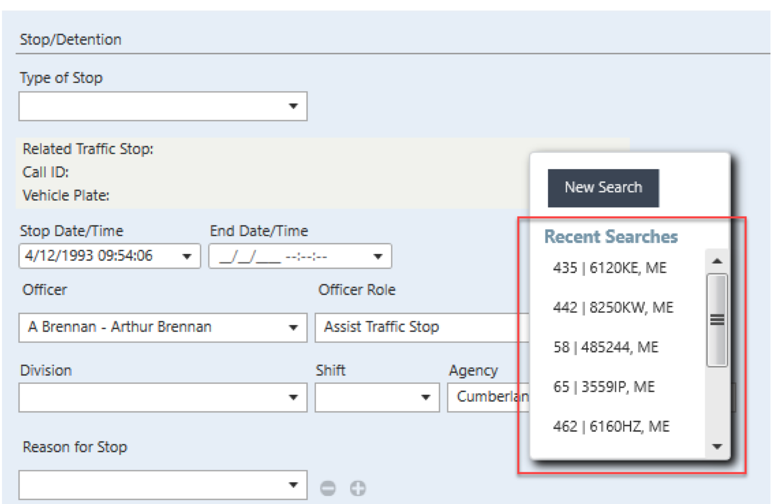
- In the **Traffic Stop** section of the tab, users can search for related traffic stops by tapping **Add** → **New Search**. This opens the **Traffic Stop Search** screen which allows users to search for and add a related traffic stop to the **Demographics** tab.

  Figure 125: Add Button

  This button also lists recent searches so users can easily access information they have recently searched for.

  Figure 126: Recent Searches Menu

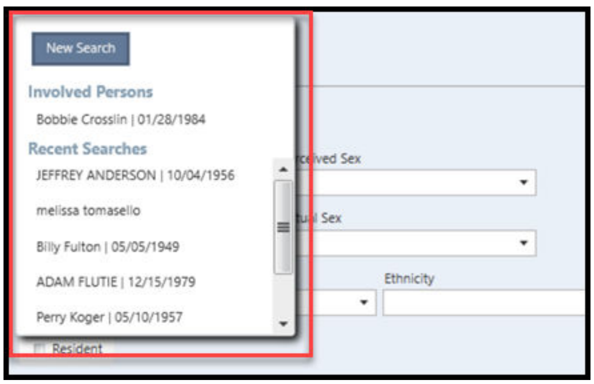
  

- In the **Search** section of the tab, users can expand or collapse the **Search Conducted** and **Contraband Found** sections by selecting or deselecting their respective check boxes.
- An **Import** button has been added to the **Stopped Person Demographics** section which allows users to quickly import **Involved Persons** related to the incident.

Figure 127: Import Button - Stopped Person Demographics Section

A list of **Involved Persons** and **Recent Searches** displays when the user taps the **Import** button.

Figure 128: Import Button - Involved Person and Related Searches Lists



- An **Import** button has also been added to the **Passengers/Group Members** section which allows users to quickly import passengers related to the incident. When a user selects a name from the **Import** button list, the name is removed from the list and the data related to that name populates in the **Relationship**, **Race**, **Sex**, **Age**, and **Ethnicity** fields. This allows the user to see persons they have added to the incident and who they have not added.

Figure 129: Import Button List - Passengers/Group Members Section

5.11.2 Updated Workflow Status Dialog Box

We modernized the **Workflow Status** dialog box in Flex Mobile to prepare for future workflow enhancements.

Now you can view only the **Assigned Individual**, **Assigned Group**, **Responsible Person** and **Supervisor** assigned to your agency so as to reduce the number of options when viewing the list. If desired, you can toggle between agency view and viewing all users and groups on the system by clicking **Show All**. This will benefit multi-agency Flex systems.

This affects the following fields in the **Workflow Status** dialog box:

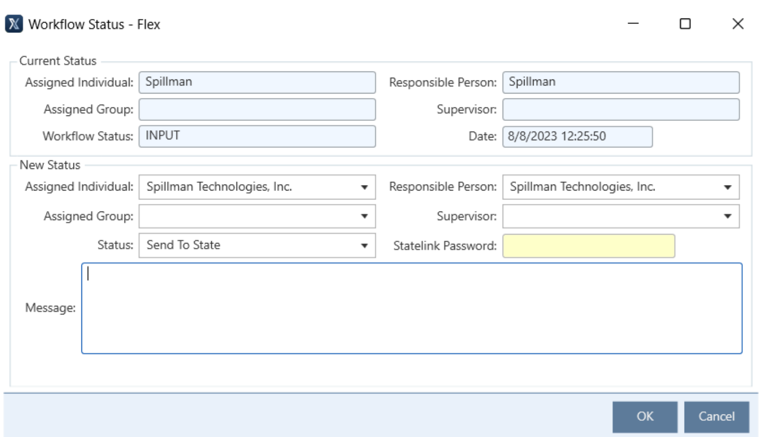
- **Assigned Individual**
- **Assigned Group**
- **Responsible Person**
- **Supervisor**

The **Update Status** dialog box has been renamed to the **Workflow Status** dialog box.

Additionally, when you select a status from the **Status** field that requires you to enter their credentials as per state requirements, such as **Send To State**, the new **Workflow Status** dialog box displays a **Statelink Password** field.

You can continue to use this dialog box to update workflow records.

Figure 130: New Workflow Status Dialog Box



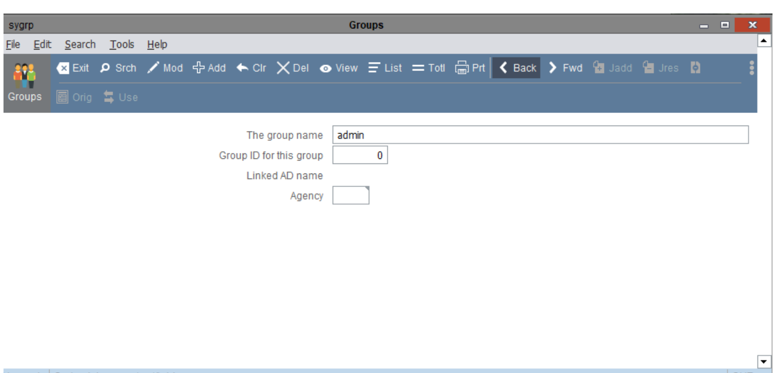
5.11.2.1 Admin: Agency Filtering for Groups in sygrp

To enable group filtering by agency, you must assign groups to agencies in the **sygrp** table.

The **Agency** field is a new optional field on the **sygrp** table. This field allows you to assign a group to one or more agencies.

When you assign a group to an agency, this only affects code filtering. If a group does not have an **Agency** filter on it, it appears at all times.

Figure 131: System Group Table Setup

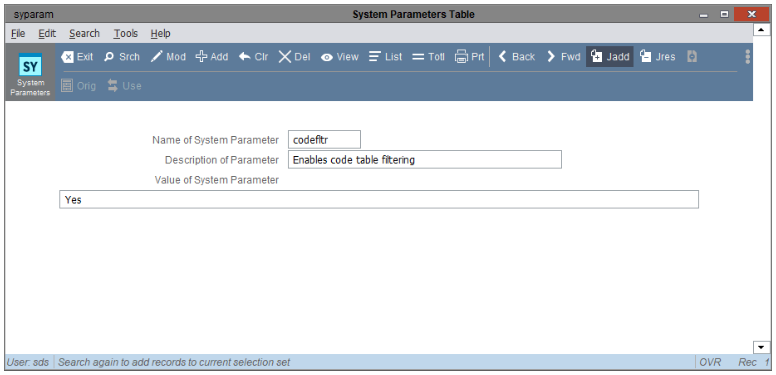


5.11.2.2
Admin: Agency Filtering for Code Tables Activation

Agency Filtering for Users and Groups uses the syparam **codefltr** which is also utilized by other dropdowns in Flex.

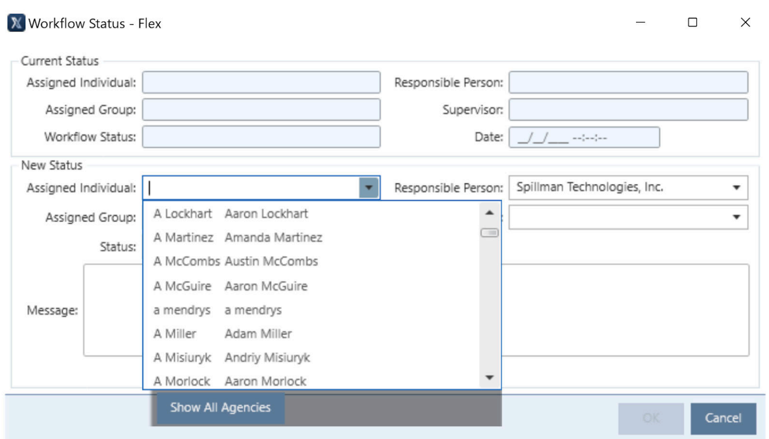
You can determine whether the **Workflow Status** fields display all system users or groups or only the users and groups from the same agency as the currently logged on user by modifying the syparam codefltr to **Yes**.

Figure 132: System Parameters Table



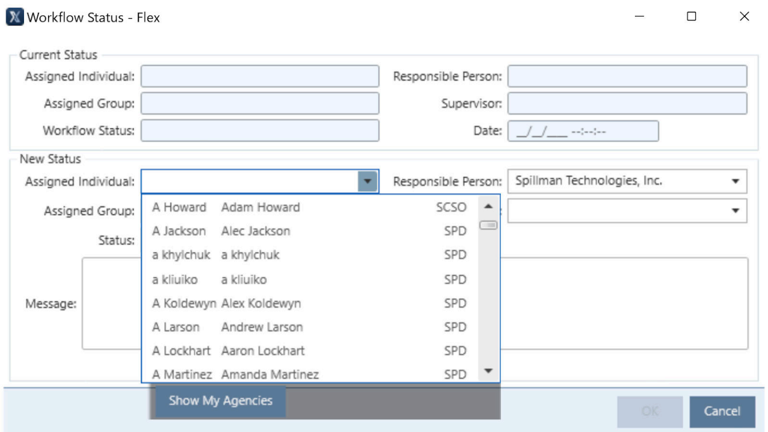
If this setting is enabled, users first see individuals and groups from their own agencies.

Figure 133: Filtered Results (Agency)



Users can see individuals and groups from other agencies by clicking **Show All Agencies**.

Figure 134: Unfiltered Results (All Agencies)



If this setting is not enabled, users always see individuals and groups from all agencies.

NOTE:
Agency Filtering for Assigned Groups in Flex Desktop will be released in a future update.

5.11.2.3
Agency Filtering

Depending on agency settings, if code table filtering has been enabled, you initially see individuals and groups from your agency when you access the drop-down menus in the following fields in the new **Workflow Status** dialog box:

- **Assigned Individual**
- **Assigned Group**
- **Responsible Person**
- **Supervisor**

You can view all individuals and groups from all agencies by clicking **Show All Agencies** when the drop-down menus are open.

Figure 135: Mobile Assigned Individual Drop-down Menu

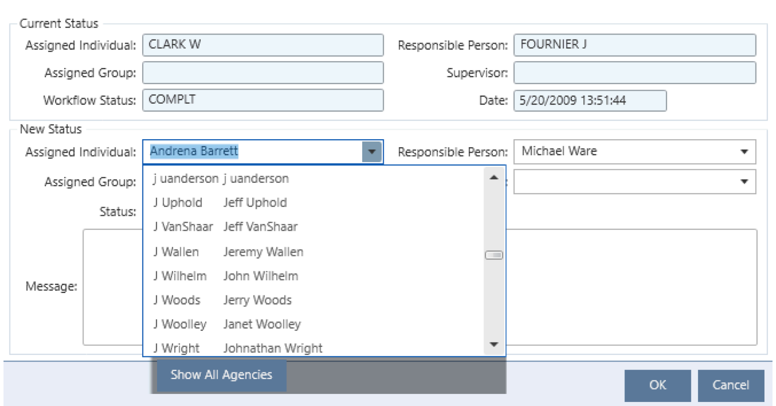
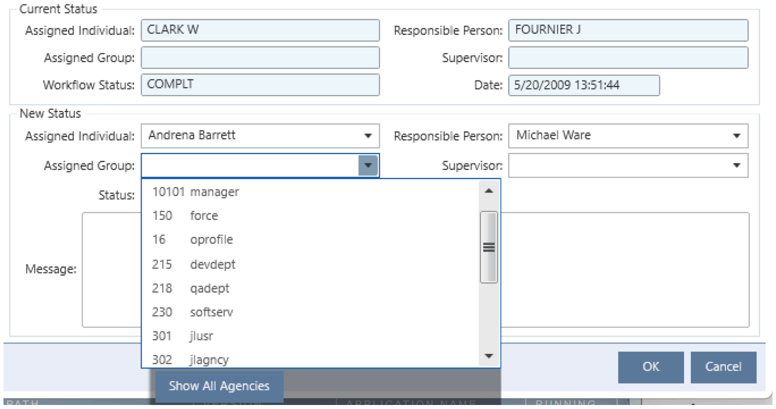


Figure 136: Mobile Assigned Group Drop-down Menu



Chapter 6

Release 2023.3

This chapter presents changes made to Flex for the 2023.3 release.

6.1 CAD

6.1.1 Assignment of Covering Zones by Unit Alias Kind

As of the 2023.3 release, your admin can enable this new feature if your agency uses the Flex CAD Incident screen and response plans with covering zones.

The default behavior with this feature turned off always considers the units belonging to the covered (primary) zone first. When this feature is enabled, the **Alias Kind** field located in the **Covering Zones** (`cdzncovr`) table allows your admin to modify recommendations to select covering zones sequences based on unit kind and zone rather than just zone. In the **Dispatch Units** area, you might see unit recommendations in a sequence based on that principle.

For more information about using this feature, contact your admin.

6.1.1.1 Admin: Configuring Covering Zones by Unit Alias Kind

As of the 2023.3 release, you can enable this new feature if your agency uses the Flex CAD Incident screen and response plans with covering zones.

The default behavior with this feature turned off always considers the units belonging to the covered (primary) zone first. When this feature is enabled, the **Alias Kind** field located in the **Covering Zones** (`cdzncovr`) table allows you to modify recommendations to select covering zones sequences based on unit kind and zone rather than just zone.

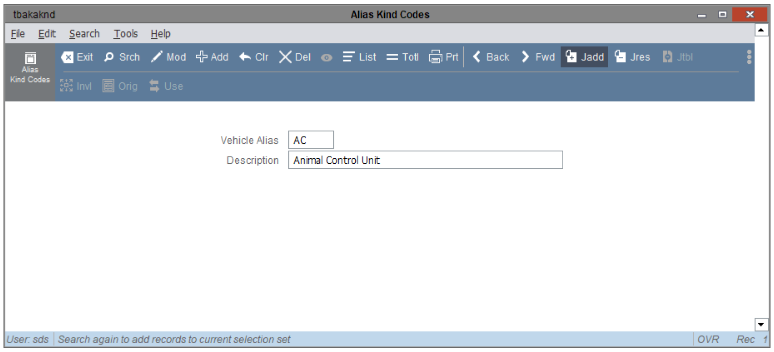
Prerequisites:

1. Ensure that your agency is using:
   - Flex 2023.3 software release,
   - Flex CAD Incident screen,
   - Response plans with covering zones.
2. Ensure that the following settings are configured in **Adminutil**:
   - `Module.CAD.FlexUnitRecommendations.EnableCoveringZones` – set to `True`
   - `Module.CAD.FlexUnitRecommendations.CoveringZonesByAliasKind` – set to `True`

   You can set the settings at the `World` or `Agency` level.

   NOTE: If the covering zones by alias kind functionality is not needed, the `Module.CAD.FlexUnitRecommendations.CoveringZonesByAliasKind` setting should be set to `False` (which is the default value), or the **Alias Kind** field should be left empty.
3. Add your Alias Kind codes to the **Alias Kind Codes** (`tbakaknd`) table.

Figure 137: tbakaknd Table with an Example Vehicle Alias Code

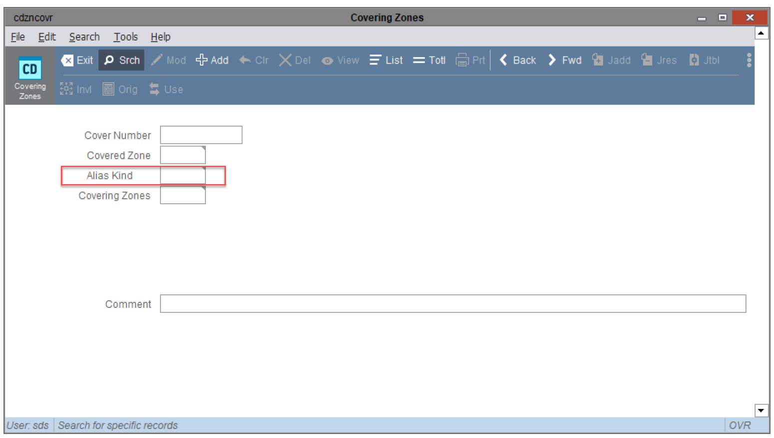


Procedure:

1. On the command line, enter `cdzncovr`

   As of the 2023.3 release, the **Covering Zones** table includes the **Alias Kind** field.

   Figure 138: Covering Zones Table with the Alias Kind Field

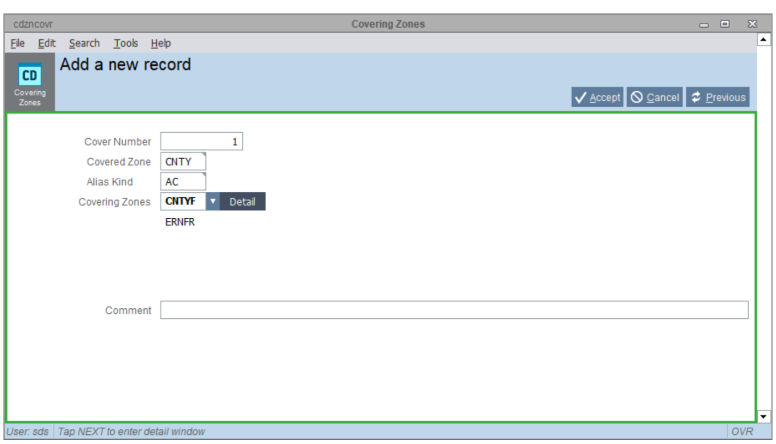
2. From the toolbar, click **Add** and add/select entries in the **Covered Zone** and **Covering Zones** fields.

   If you need more information, see Setting Up Covering Zones where the only difference in the **Covering Zones** table is that it has not the **Alias Kind** field.

3. In the **Alias Kind** Field, enter/select unit recommendations for a covered (primary) zone.

   Step example:

   Figure 139: Covering Zones Table with an Alias Kind Entry

Unit recommendations will consider this entry in the `cdzncovr` table. Any unit recommendations for the specific unit alias kind (in the preceding figure, `AC`) are ordered based on this list, which will first match vehicle alias kinds, then look for records with a blank alias. Recommendations from the `CNTYF` zone will be shown first, then the recommendations from the `ERNFR` zone.

NOTE:
You can add the primary zone's own units to its list of covering (secondary) zones, so that these units might be recommended in order depending on their positions in the list.

If you do not add the covered (primary) zone to its own list, then **no** recommendations for the zone's own units will be shown.

6.1.2
Customizable Lists for CAD Users

As of the 2023.3 release, CAD users who want to change the predefined sort order and arrangement of columns in lists are able to sort and customize the lists directly in CAD.

The feature requires the following settings in **Adminutil**:

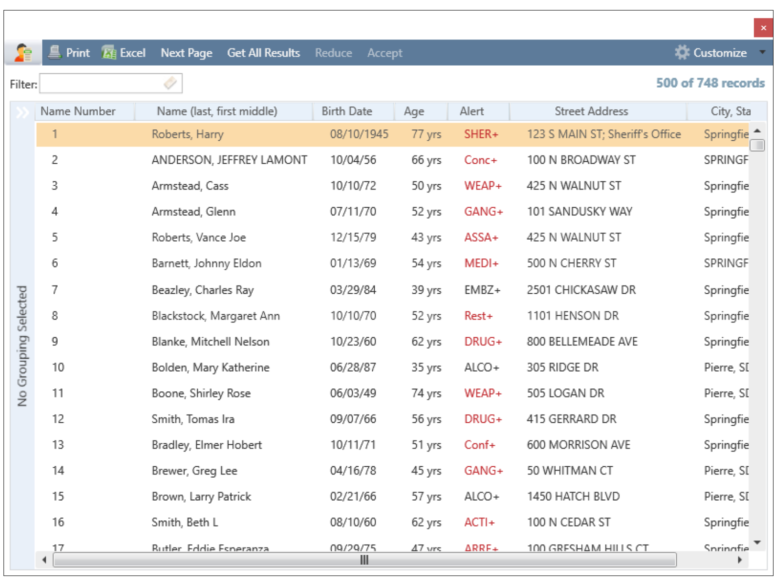
- `System.Client.CustomizableListforCAD` – set to `True` (the default value is `False`)
- `System.Client.CustomizableListforCADMaxRecordsToLoad` – set to `1000000` (the default value; an integer)
- `System.Client.CustomizableListforCADResultMax` – set between `100` (the default value) and `500` (an integer)

By default, the settings are locked at the `User` level.

The following figures are examples of customization options for a list in the Names Table (`nmmain`), which is opened by clicking **List** on the table toolbar.

The `System.Client.CustomizableListforCADResultMax` value is set to `500`.

Figure 140: Customizable Names List



Name Number	Name (last, first middle)	Birth Date	Age	Alert	Street Address	City, Sta
1	Roberts, Harry	08/10/1945	77 yrs	SHER+	123 S MAIN ST; Sheriff's Office	Springfie
2	ANDERSON, JEFFREY LAMONT	10/04/56	66 yrs	Conc+	100 N BROADWAY ST	SPRINGF
3	Armstead, Cass	10/10/72	50 yrs	WEAP+	425 N WALNUT ST	Springfie
4	Armstead, Glenn	07/11/70	52 yrs	GANG+	101 SANDUSKY WAY	Springfie
5	Roberts, Vance Joe	12/15/79	43 yrs	ASSA+	425 N WALNUT ST	Springfie
6	Barnett, Johnny Eldon	01/13/69	54 yrs	MEDI+	500 N CHERRY ST	SPRINGF
7	Beazley, Charles Ray	03/29/84	39 yrs	EMBZ+	2501 CHICKASAW DR	Springfie
8	Blackstock, Margaret Ann	10/10/70	52 yrs	Rest+	1101 HENSON DR	Springfie
9	Blanke, Mitchell Nelson	10/23/60	62 yrs	DRUG+	800 BELLEMEADE AVE	Springfie
10	Bolden, Mary Katherine	06/28/87	35 yrs	ALCO+	305 RIDGE DR	Pierre, SI
11	Boone, Shirley Rose	06/03/49	74 yrs	WEAP+	505 LOGAN DR	Pierre, SI
12	Smith, Tomas Ira	09/07/66	56 yrs	DRUG+	415 GERRARD DR	Springfie
13	Bradley, Elmer Hobert	10/11/71	51 yrs	Conf+	600 MORRISON AVE	Springfie
14	Brewer, Greg Lee	04/16/78	45 yrs	GANG+	50 WHITMAN CT	Pierre, SI
15	Brown, Larry Patrick	02/21/66	57 yrs	ALCO+	1450 HATCH BLVD	Pierre, SI
16	Smith, Beth L	08/10/60	62 yrs	ACTI+	100 N CEDAR ST	Springfie
17	Butler, Eddie Esperanza	09/29/75	47 yrs	ABRE+	100 GRESHAM HILLS CT	Springfie

Figure 141: List with Filtered Items (MEDI)

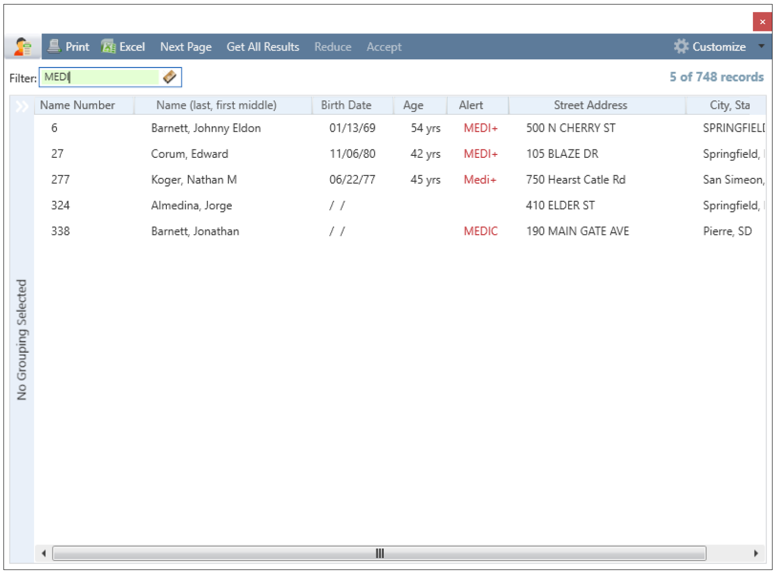


Figure 142: Customize Drop-down Options

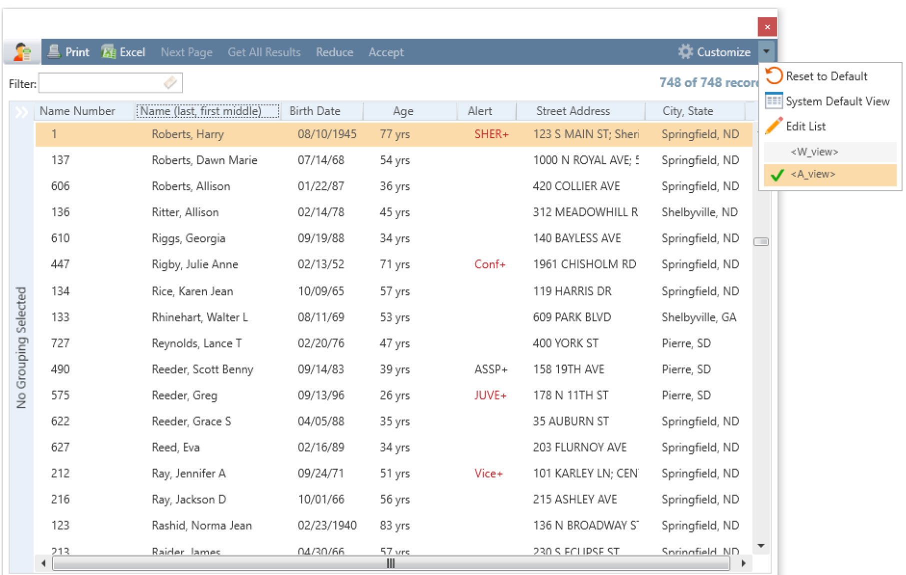


Figure 143: Edit Custom List Views Window

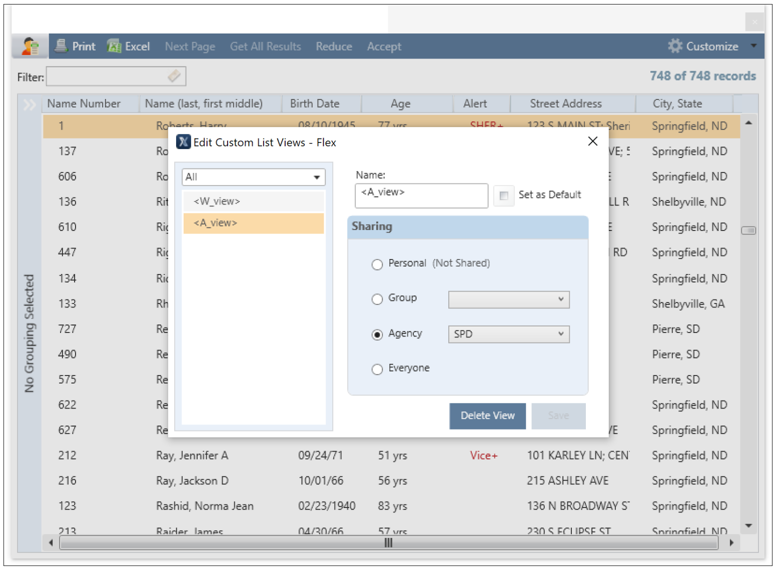
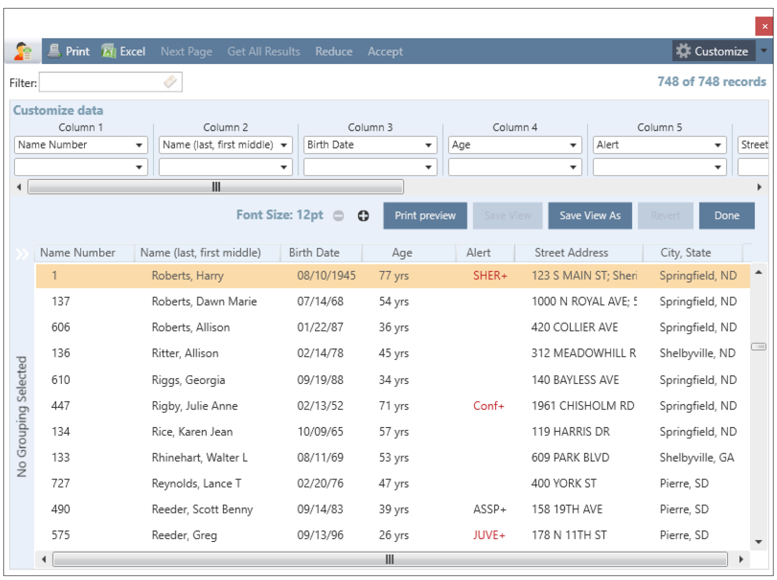


Figure 144: List Customize Data Options

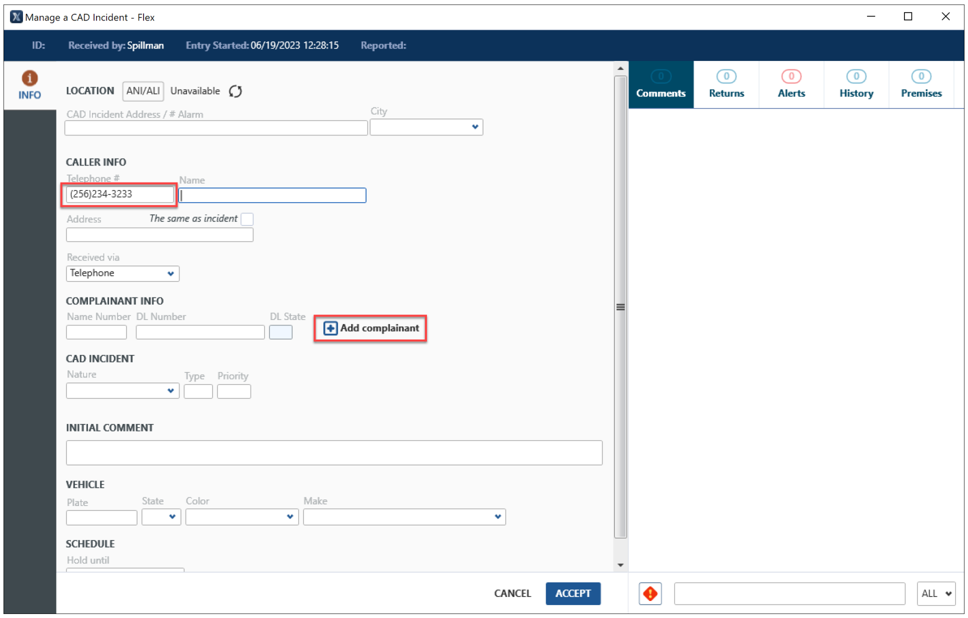


6.1.3

Searchable Telephone Number Field for the Complainant

The **Telephone** field on the CAD Incident screen is now searchable. You have the ability to search names by phone number at work number, home number, and other phone numbers.

Figure 145: CAD Incident Screen with an Entry in the Telephone Field



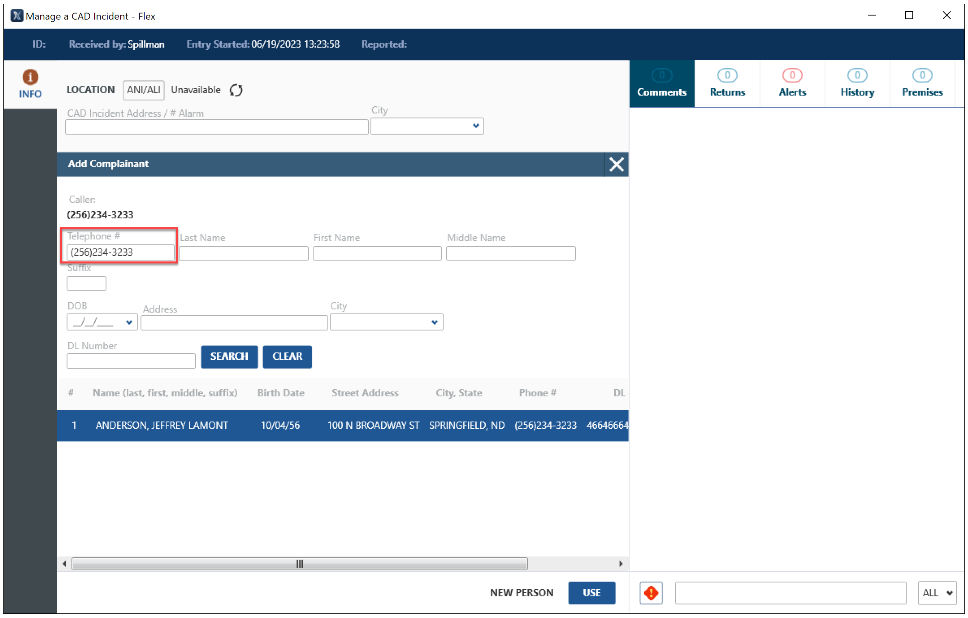
After you enter into the **Telephone** field a phone number and click **Add complainant**, the **Add Complainant** window opens with the new **Telephone** field populated with the same number.

NOTE:
To get a search result, you must enter the full telephone number, without any wildcards.

You do not need to enter additional data such as the name of the person. If the phone number exists in any of the following tables and fields, the software provides the search result. However, if you include the phone number and name, the search takes into account the both entries.

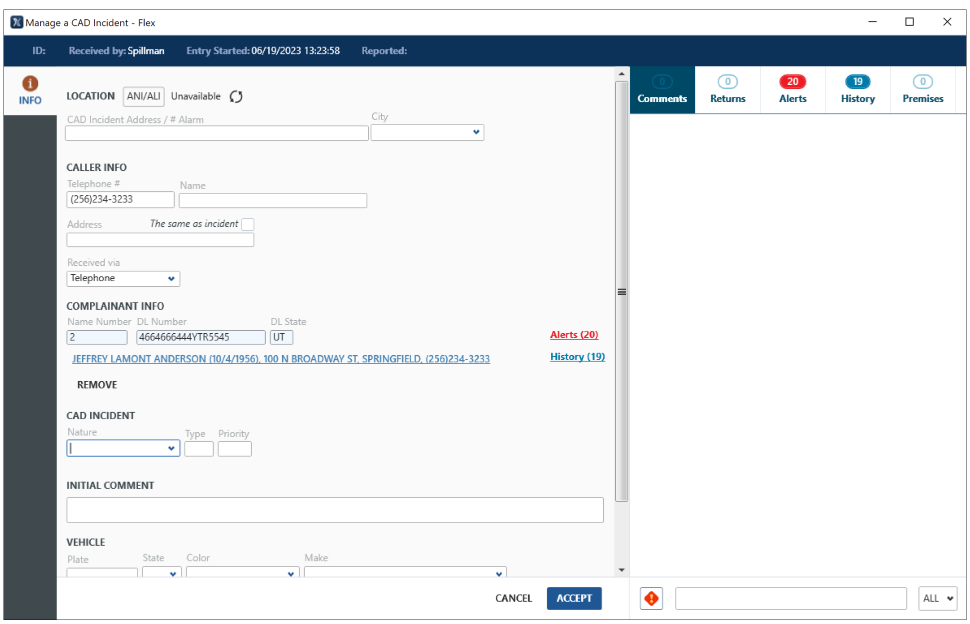
```
nmmain.phone
nmmain.wrkphn
nmmain.nmotel
```

Figure 146: Add Complainant Window with Telephone Field and the Search Result



By clicking **Use** (F3), you can add the selected person as a Complainant to the CAD incident.

Figure 147: CAD Incident with Complainant Information



6.1.4
CAD Performance Improvements

The latest CAD performance improvements include faster opening and closing of the new CAD incident screens. Beginning with the 2023.3 release, administrators who want to change the client cache size must perform a new procedure.

Faster Opening of the CAD Incident Screen

In order to open the new CAD Incident screen in less than one second, the adminutil setting `Module.CAD.ClientCommandLineParser` is set to `True` by default. This setting determines whether the `AC`, `AT`, `CI`, `DC`, `DU`, `MC`, `UC`, or `UU` command opens the new CAD screen without calling to Hub, which reduces the screen loading time. The default value of this setting was `False`.

Faster Closing of CAD Calls

Now, it takes less than one second to close the new CAD incident screens, instead of 2–3 seconds as before. This is achieved by eliminating the waiting time for verification if the content of all fields needs to be saved, which included fields that were not actually changed.

Configurable Client Cache Size with Higher Defaults

As of the 2023.2 release, each user can open up to eight (8) Flex CAD windows that load quickly thanks to a new default cache setting. The maximum number of cached windows is increased to ten (10). The higher values improve the performance of opening multiple windows. Administrators can configure these settings, but beginning with the 2023.3 release, the procedure is different: see Admin: Configuring the Amount of Cached CAD Windows (2023.3+) on page 162.

This feature requires the following setting in **adminutil**:

- `Module.CAD.ClientCommandLineParser` – set to `True`

6.1.4.1
Admin: Configuring the Amount of Cached CAD Windows (2023.3+)

The client cache settings are now configurable. As of the 2023.2 release, you can decide how many cached CAD windows are supported by the Flex application. However, beginning with the 2023.3 release, the procedure is different.

The initial cache size (the initial number of cached windows) depends on the `initialWindowCacheSize` value, and the maximum size (the maximum number of cached windows) is limited by the `maxWindowCacheSize` value. By default, the values of the settings are 8 and 10, respectively. If, as an administrator, you need to change the default values, perform the following actions.

Procedure:

1. Go to the Flex installation directory.

   Example: `C:\ProgramData\Spillman\Spillman\application\FlexClient`
2. Open `FlexClient.json` by using any text editor.
3. In the following code section, uncomment the two lines relating to `initialWindowCacheSize` and `maxWindowCacheSize`

Figure 148: Code Section Defining Cache Size

```
/** Defines various client settings for the CAD module **/
"cad": {
    /** Defines how many CAD incident windows are created when Flex starts up (be sure to uncomment the line for the value to take effect) **/
    "initialWindowCacheSize": 2,

    /** Defines how many CAD incident windows the cache can hold at a maximum (be sure to uncomment the line for the value to take effect) **/
    "maxWindowCacheSize": 4,
},
```

```
/* "initialWindowCacheSize": 2, */

        /* "maxWindowCacheSize": 4, */
```

4. Change the existing values to values of your choice.

   The `initialWindowCacheSize` and `maxWindowCacheSize` values must be integer numbers, and the initial value cannot be greater than the max value. In the example, you should replace `2` and `4` with your values. Usually, as the initial and max values you might expect 8 and 10, which are the default values.
5. If needed, restart the Flex client application.

When the user once opens another window above the initial value count, and the count is not exceeding the max value, the application will extend the cache size and keep it ready for use after closing any of the open windows. Due to the extended cache size, another window “replacing” the closed one will open more quickly.

When the user has opened the number of windows indicated by the max value, and opens another one, the new window cache is not available anymore after closing the window, so that any “excessive” window needs more time to appear.

6.1.5
OSC Command and Screen Changes

As of the 2023.3 release, the OSC command line format is updated with the ability to add optional parameters: License Year and License Type. The Onsite Call Command (`oscscr`) screen includes three new fields: **Lic Year**, **Lic Type**, and **Comments**.

These updates ensure compatibility with StateLink in terms of search. Previously, the same optional parameters were introduced to the TS command line format and reflected on the Traffic stop (`cdts`) screen.

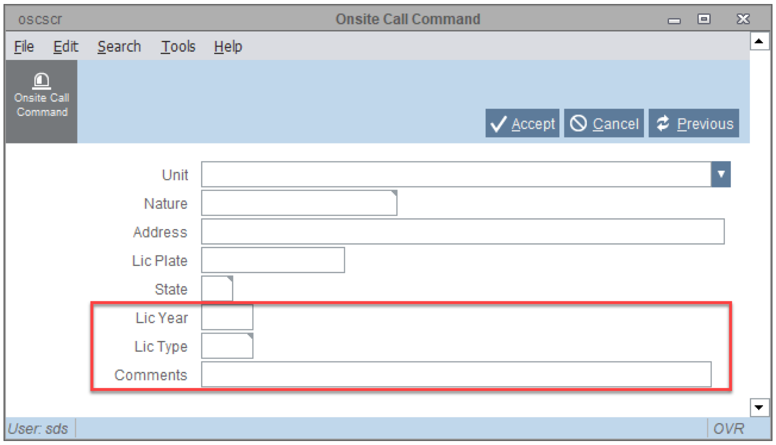
The **Usage** of the OSC command changes to:

```
OSC {unit{,unit} {nature {address}. {plate {st {year {lptype}}}} .comment}}
```

The OSC command quick format changes to:

```
OSC [unit] {,unit...} [nature] [address]. {plate {st {year
{lptype}}}} .comment}}.
```

Figure 149: New Fields on the oscscr Screen



6.1.6

Address Typeahead

On the **Manage a CAD Incident** screen (**CAD Incident** screen), the **CAD Incident Address** field is enhanced so that after you type at least three characters, the software provides address typeahead suggestions in a drop-down list.

If you select an address suggestion, the address is automatically validated, so the **Address Selection** window does not open. The address typeahead also works with intersections, common place names or place aliases.

If you press **Tab** and move out of the address field without selecting a suggestion, the **Address Selection** window still opens for you to validate the address.

6.1.6.1

Admin: Setting Up the Address Typeahead Feature

The Address Typeahead feature provides a list of suggested addresses regardless of whether the Exact Match logic is turned on as part of your GeoValidation setup.

For the Address Typeahead feature to work, perform the following actions.

Procedure:

- Ensure that you are using an ArcGIS Pro multirole locator.
- In **Adminutil**, ensure that the `Module.GeoValidation.EnableSuggestions` setting is set to `True`.
- Ensure that your GeoValidation setup is configured with the appropriate geocoding and map service to work with ESRI suggestions.

  For this iteration of the feature, Zone and Location information is not provided to the user.

6.1.7 ArcGIS Pro

Flex now supports ESRI ArcGIS Pro. ArcGIS Server 10.9.1 is compatible with ArcGIS Desktop 10.8.2 and ArcGIS Pro 2.9 and is the last version to support ArcGIS Desktop.

Updating to ArcGIS Pro is a major update, which will require models and locators to be rebuilt. Please review the *Flex Hardware and System Requirements* for more information and contact your administrator or Motorola Representative about updating to ArcGIS Pro.

6.2 Interfaces

6.2.1 ERS Interface Mutual Aid Enhancements

The existing Send All Units feature was improved to function as expected.

When the **Properties** → **Agency Settings** → **Units** is set to **Send All Units**, the application sends all units attached to a call from multiple agencies.

6.2.2 Livescan 2.0 Change Mapping

You can now configure LiveScan 2.0 for LA County to use the Arrest Number instead of Booking Number when exporting to the LiveScan machine. Previous functionality is still available.

6.2.3 WestnetLocution Silence Data Enhancement

You can now use the WestnetLocution interface to select if the following information is spoken:

Table 28: WestnetLocution Silence Data Enhancement

Check Box	Description
Say Incident Number	When checked, the interface speaks the incident number (**IB** field). When unchecked, the interface instructs WestnetLocution to not read this data.
Say Incident Comments	When checked, the interface speaks the incident comments (**IC** field). When unchecked, the interface instructs WestnetLocution to not read this data.

6.3
Hub/Platform

6.3.1
.NET 6 Migration

Flex 2023.3 requires the .NET 6.0 SDK to be installed on all Windows clients that will utilize Flex. If you launch Flex 2023.3 without the .NET 6.0 SDK, Flex will prompt you to install it.

.NET 6.0 SDK helps our developers work more quickly and securely while supporting under-the-hood stability improvements throughout all aspects of the Flex suite. If your agency does not have .NET 6.0 SDK installed when launching Flex 2023.3 and beyond, they will be unable to launch Flex until it is installed.

We are working on efforts to improve this process in the future to reduce disruption during the patch process. For more information, contact Motorola Technical Support or Customer Success.

6.3.2
Flex Server Diagnostic Tool Removed for Versions 2023.3+

Due to software enhancements, beginning with the 2023.3 release the Flex Server Diagnostic Tool is no longer needed and is removed.

This tool is still available for users of previous releases.

6.4
Records

6.4.1
Admin: Transition from VaultIntegration to CCAssetSync

The CCAssetSync integration service takes over the role of the VaultIntegration service. If your agency uses CommandCentral Evidence (CCE), Flex RMS and CCAssetSync allow your agency to synchronize the images and files on your Flex server with CCE.

If you change the record in Flex, the appropriate tags are updated in CCE. Also, if you delete the file or image in Flex, this content is removed from CCE.

Also, in Flex, files attached to an incident number include files uploaded through CCE if those files are tagged with the same incident ID.

At this time, the integration between Flex and CommandCentral Evidence using CCAssetSync must be configured by the CommandCentral Cloud Activation Team.

Once your agency has placed an order for CommandCentral Evidence and Flex Integration, you will be contacted by the team to start the integration process.

NOTE: If your agency is currently configured with CCVault, you must transition to CC Evidence to use CCAssetSync. Please reach out to Customer Success to initiate the transition to CC Evidence.

For information about further configuration of this feature, see the *Flex Administrator Manual*.

6.4.2
Evidence Audit and Movement Webpage

Depending on agency settings, you can now generate and print Audit and Movement reports by accessing the **Audit** and **Movement** web pages and selecting which reports you want to print.

The report titles now reflect the type of report printed. For example, if you print an evidence report, your report title will be Evidence Scanner Audit.

Figure 150: Audit Reports Page

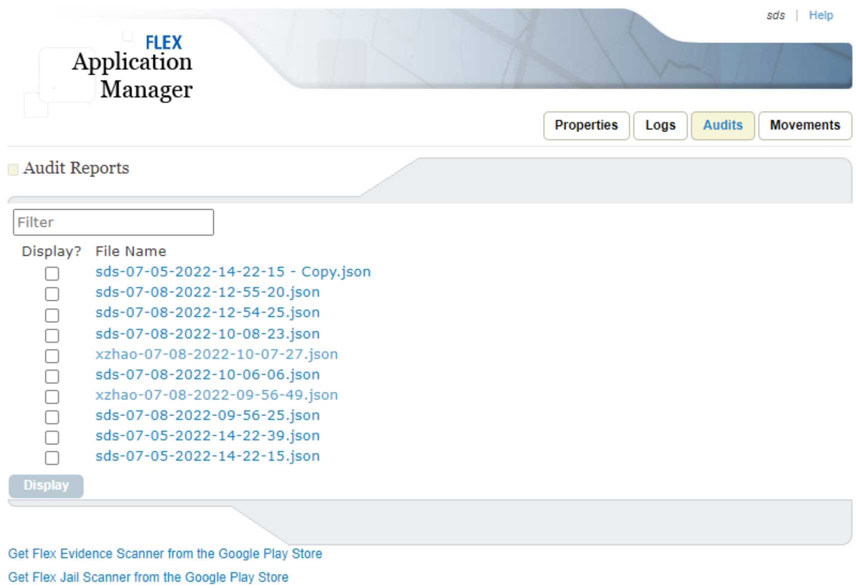
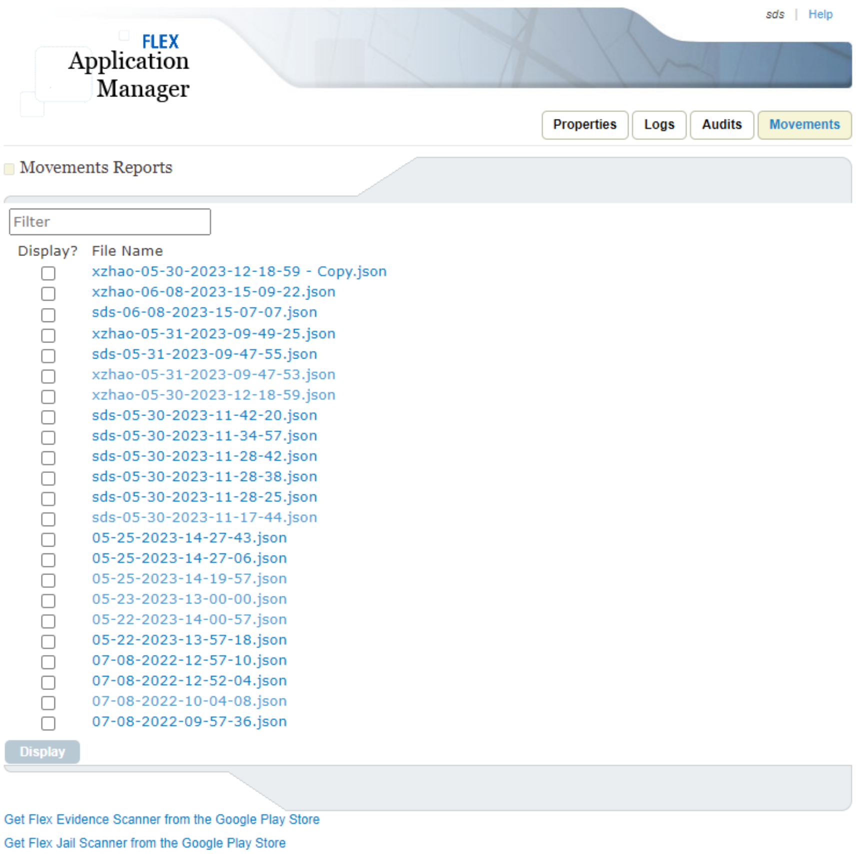


Figure 151: Movements Report Page



6.4.3

Pronoun Field

Due to some requirements, there is now a **Pronoun** field on the following screens:

- **Names** screen on Flex Desktop
- **View Names** screen in Mobile
- **Add/Edit** Names screen in Mobile

This feature is enabled automatically.

The following pronouns have been loaded by default and can be updated by an administrator by using the **nmtbpron** table.

Table 29: Default Pronouns

Code	Description
H	He/Him/His
HIR	Ze/Hir/Hir/Hirs
OT	Other
S	She/Her/Hers
T	They/Them/Their

Code	Description
ZIR	Ze/Zir/Zir/Zirs

Figure 152: Pronoun Field on the Names Screen

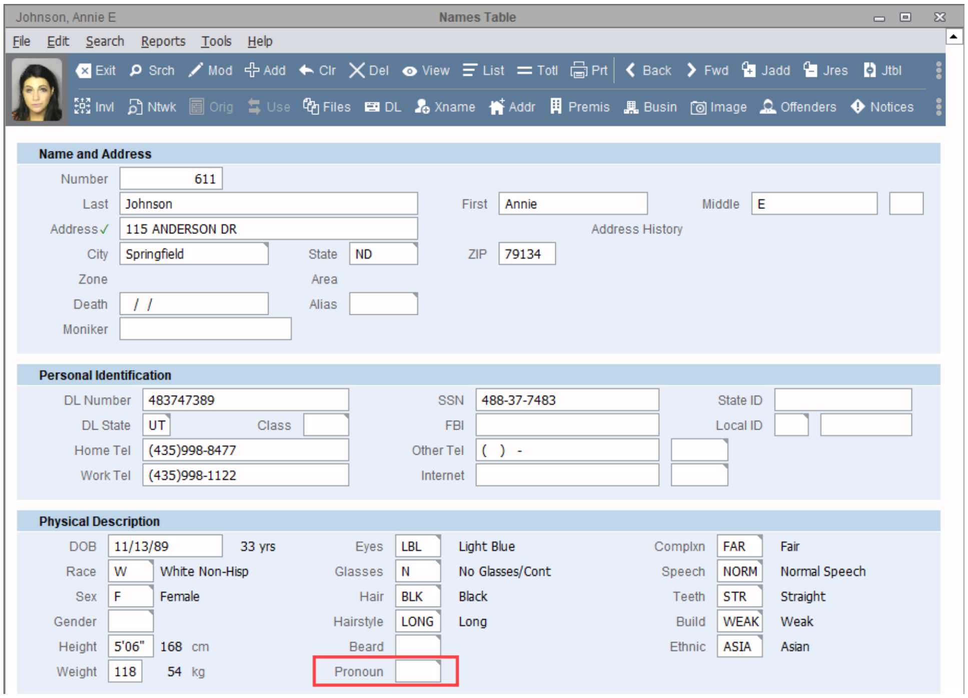


Figure 153: Pronoun Field on the Mobile Names Screen

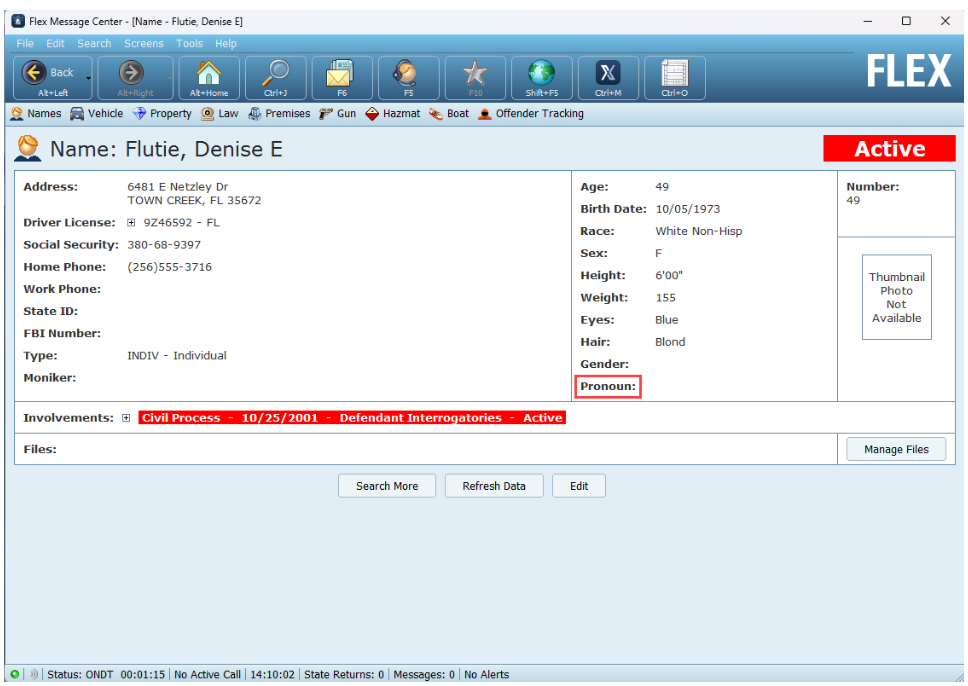
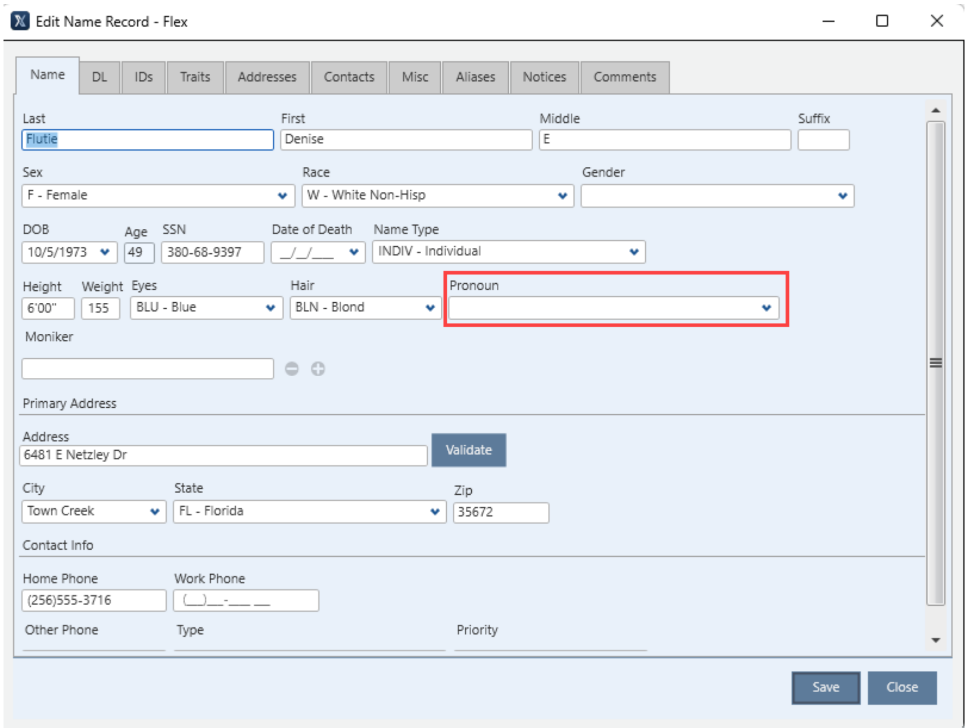


Figure 154: Pronoun Field on the Mobile Add/Edit Names Screen



6.5
Reports

6.5.1
New and Updated Reports

In the 2023.3 release, we added new reports, made enhancements to certain reports according to customer feedback, and eliminated errors that were reported to us by users.

Reports beginning with `rp` are accessible by users with appropriate sypriv privileges from the Flex command line by entering the file name without any extension. Example: `rpevchr`

Reports with file names the same as the screen names are accessible by clicking the **Print** button on the respective screens.

Any report with an `.x` extension is printed in a PDF format, and any report with an `.r` extension is printed in a fixed-width text format.

New Reports

- `cdcall.x1` – **Call Detail Report**
  - New PDF version of the report.
- `lwmain.x5` – **Chain of Custody for Law Incident**
  - For printing the Chain of Custody for items related to a Law Incident.
- `lwsupl.x1` – **Law Supplemental Report**
  - For printing one or many Law Supplements with the agency header at the top.
- `nmmain.x1` – **Name Summary Report**

  - For printing summary information about a Name Record and a list of that record's involvements.
- `rpjliapop.x1` – **Iowa Jail Population Report**
  - New monthly report for Iowa Jail Population for submission to the state. See Iowa Monthly Jail Report on page 172.
- `rpjlowp.x1` – **Jail Event Activity by Officer**
  - For printing the list of an officer's jail event activity.
- `rpevrand.x1/.r1` – **Random Evidence Audit List**
  - For printing a random list of evidence for audit purposes.
- `rpvrss.rcsr/.r1` – **Verify Status of Inmate Veterans**
  - This report tabulates all current inmate's information in a format accepted by the US Veterans Administration to determine if an inmate is a veteran.
  - For printing submission and audit report.

New/Updated Reports

- `rpevchr.x1/.r1` – **Chain of Custody**
  - New PDF format.
  - Provides full reason without truncating text (both the x1 and r1 versions).

Updated Reports

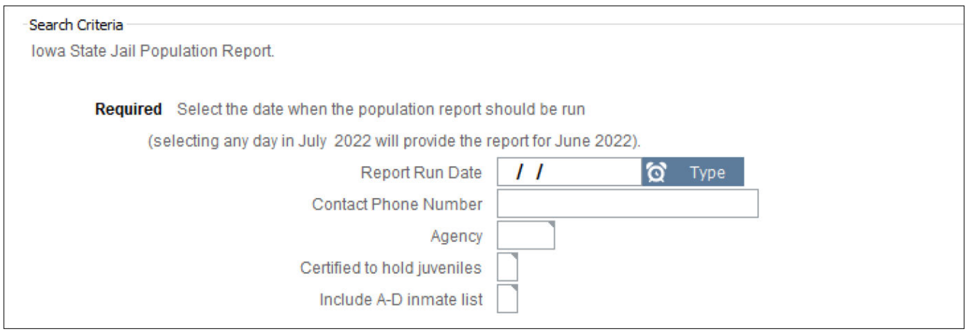
- `rpjlbook.x1` – **Individual Arrest/Booking Report**
  - OS version is now dynamically recognized.
- `rpjlbsr.x5/.x6` – **Booking Summary Report**
  - Offense section is improved.
- `rpjlinci.x1` – **Jail Incident Report**
  - Involved officers section is improved.

6.6
Jail

6.6.1
Iowa Monthly Jail Report

You can now print the Iowa Monthly Jail Report from the Flex Jail **Iowa Jail Population Report** screen (rpjliapop).

Figure 155: Iowa Jail Population Report Screen



6.6.1.1
Printing the Iowa Monthly Jail Report

The Iowa Monthly Jail Report is only available if your agency has enabled it.

Procedure:

1. To open the **Iowa Monthly Jail Report** screen, at the Flex Command Line, enter `rpjliapop`
2. Complete the following fields:

Table 30: Iowa Monthly Jail Report Fields

Field	Description
ReportRun Date	Enter the date or select the time by clicking the **Time** button.
Contact Phone Number	Enter the phone number of the contact.
Agency	Enter the agency code.
Certified to hold juveniles	If your agency is certified to hold juveniles, enter `Y` If your agency is not certified to hold juveniles, enter `N`
Include A-D inmate list	If you want to print out a list of all the inmates counted for sections A-D, enter `Y` If you do not want to print out a list of all the inmates counted for sections A-D, enter `N`

3. To print the report, press **Print**.

   When you submit the report, the information in the report is pulled from the month before the date that you chose. For example, for the July report, you must select a date from August.

6.6.1.2 Admin: Enabling the Iowa Monthly Jail Report

To enable the Iowa Monthly Jail Report, you must configure several settings.

Procedure:

1. In the Flex Command Line, enter `adminutil`
2. Configure the following settings:

Table 31: Iowa Monthly Jail Report Settings

Setting	Description	Affected Report Section
Module.Jail.IA.Population.housedInOtherCounty	Location Level 1 value that indicates a location in another county	Section G
Module.Jail.IA.Population.electronicMonitoring	Location Level 1 value that indicates a location used for electronic monitoring	Section G
Module.Jail.IA.Population.housedInOtherInstitutions	Location Level 1 value that indicates a location in other institutions	Section G
Module.Jail.IA.Population.housedOutOfState	Location Level 1 value that indicates a location in another state	Section G
Module.Jail.IA.Population.otherTypeOfRelease	Location Level 1 value that indicates a location for misc release types	Section G
Module.Jail.IA.Population.suicideEvent	Jail Incident nature that indicates a suicide	Section E
Module.Jail.IA.Population.attemptedSuicideEvent	Jail Incident nature that indicates an attempted suicide	Section E

3. Give users **Access** privilege sypriv for rpjliapop.

6.7 Mobile

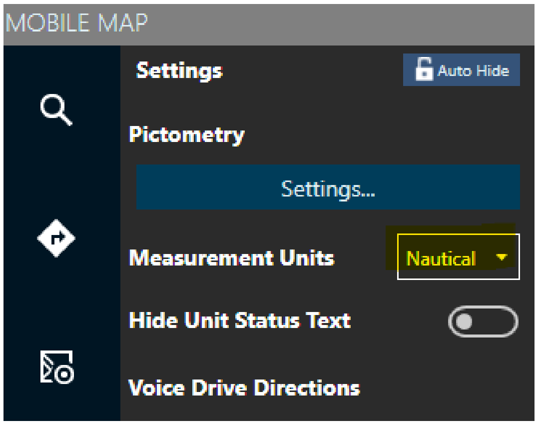
6.7.1 Aircraft and Marine Vessel Routing

Available in Flex Mobile Map, you can now calculate the direct distance and direction to your destination without relying on the street network.

NOTE: This method does not follow any restrictions or barriers. For example, if there are flight restrictions in an area, this does not recognize them.

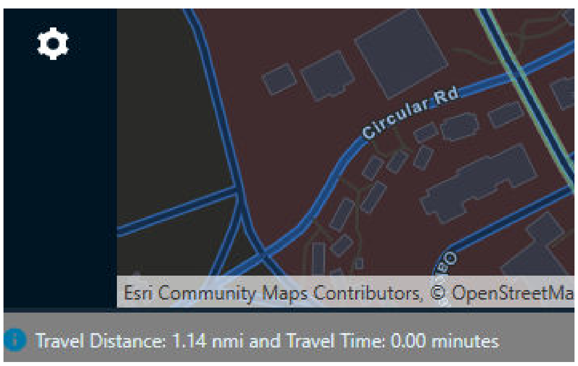
When **Measurement Units** is set to **Nautical**, the next route created uses Nautical routing. When a route is created, a message displays at the bottom right of the map, showing the total distance in nautical miles.

Figure 156: Nautical Measurement Units



If the starting location is selected from a device with AVL information, the travel time includes the number of minutes it takes based on the velocity of the device when it is calculated. If no velocity is found, the travel time is 0 minutes as seen in the following figure.

Figure 157: Travel Distance 0 Minutes



When following a nautical route, the directions state which bearing to use to travel to the destination from the given origin. The bearing is given as a true bearing between 0 and 360 degrees. The following is an example of how the current direction displays.

Figure 158: Bearing

NOTE: When the distance is less than a quarter nautical mile, the units of measurement switch to feet.

With the nautical navigation, the travel time can easily go up to more than one hour. The system displays hours if the total travel time is greater than one hour. Otherwise, it displays only a minute and second.

6.7.2 License and Permits Update

You can now add, view and edit licenses and permits from Mobile.

6.7.2.1 Adding, Editing, and Viewing New Licenses and Permits

Procedure:

1. To add a new License or Permit, on the **Form** screen, click the **License/Permits** link.

   The **Licenses & Permits** screen opens.

2. Complete the fields as needed.

   If the permit type is Animal, Bike, or Weapon, the relevant tab appears to the left of the **Fees** tab. You must complete this tab.

3. To save, click the **Save** button.

6.7.2.2 Admin: Setting Up License & Permits

Procedure:

Set sypriv **mdcmdlfrlicper**.

6.8 IBR

6.8.1 Use of Force Reports

With this release, Pennsylvania has been added to the list of states that can create and submit Use of Force Reports through Flex IBR. This can be accessed through the IBR Incident screen or the Mobile Law Incident. Currently, Flex IBR can be used to submit Use of Force Reports for Florida, Pennsylvania and New Mexico.

Your agency can customize their Use of Force data collection and report as they do with IBR. You can generate these reports in the same process that you generate IBR reports.

In IBR, an Use of Force (UOF) incident consists of the following:

- Incident level UOF data element
- One or more Officers

  You can add officer roles as needed.
- One or more Subjects

  You can add subject roles as needed.

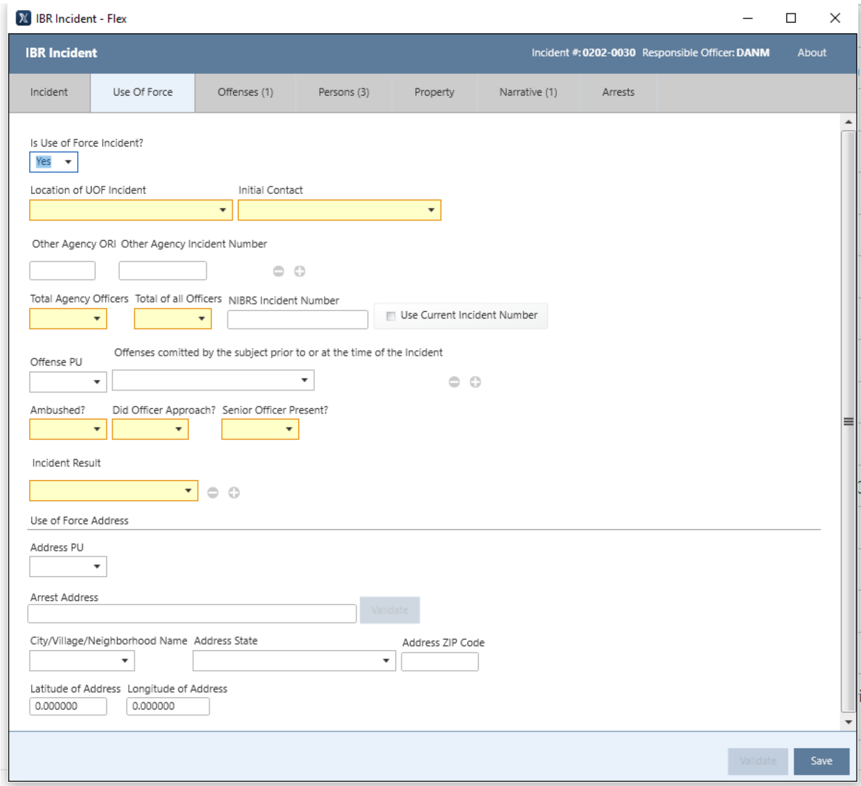
NOTE: You must use Sentryx IBR to access this functionality.

UOF is separate from the NIBRS submission, but IBR generates both each time you run the **Generate Report** option on the **IBR Agency** screen. When you submit an UOF incident submission, you create one file per incident or zero report. The data in those files can either be JSON flat file format or XML format.

All the files generated for submission for both IBR and UOF are placed in a single zip archive and copied to the client from the server. Your agency decides how to submit Use of Force files to the State. You can update the submission status by confirming it through the standard report confirmation process in the IBR Agency interface.

You can set up a standalone UOF incident with an offense and UOF offense translation value. You can also associate an IBR incident different from the current incident or may reference the current incident using the NIBRS Incident Number in the **UOF Incident** tab or **Officer** on the **Persons** tab.

Figure 159: Office Use of Force Tab



6.8.1.1 Admin: Pennsylvania Use of Force Setup

Pennsylvania Use of Force (UOF) is a subset of the national standard that encourages reporting Use of Force after an initial investigation has been completed so that complete and useful data can be submitted about the Use of Force incident.

The only location information collected is a location code and latitude and longitude coordinates. All other address fields, the national standard codes for **Pending Further Investigation** and **Unknown** have been dropped.

Pennsylvania UOF Generates one incident or zero report per JSON file. UOF and IBR reports are generated at the same time for the same reporting period from the IBR Agency UI.

The client receives a single zip file containing both IBR and UOF submission files for the reporting period.

6.8.1.2

Admin: Configuring Use of Force Reports

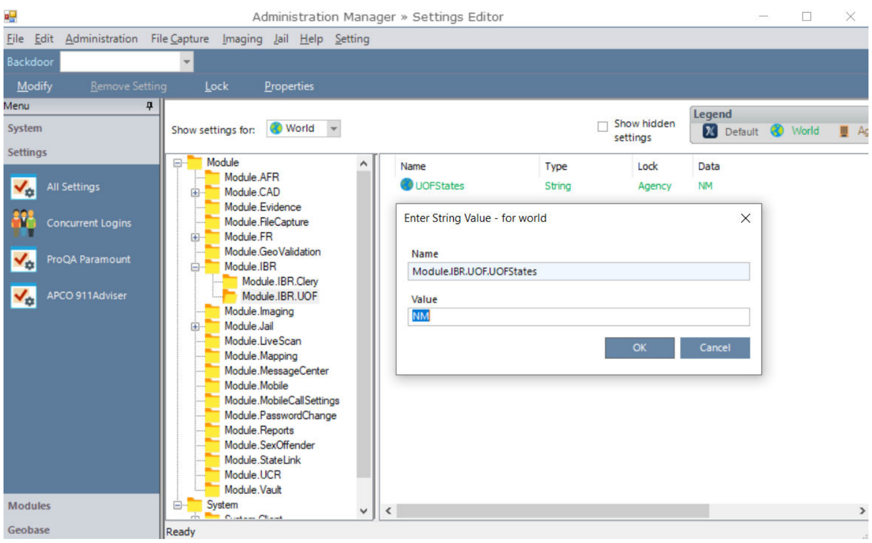
The Use of Force feature is installed as part of the Flex IBR product installation for Pennsylvania, Florida and New Mexico, but is enabled through separate setup.

Procedure:

1. Open adminutil.
2. In the `Module.IBR.UOF.UOFStates` setting, add State Code.

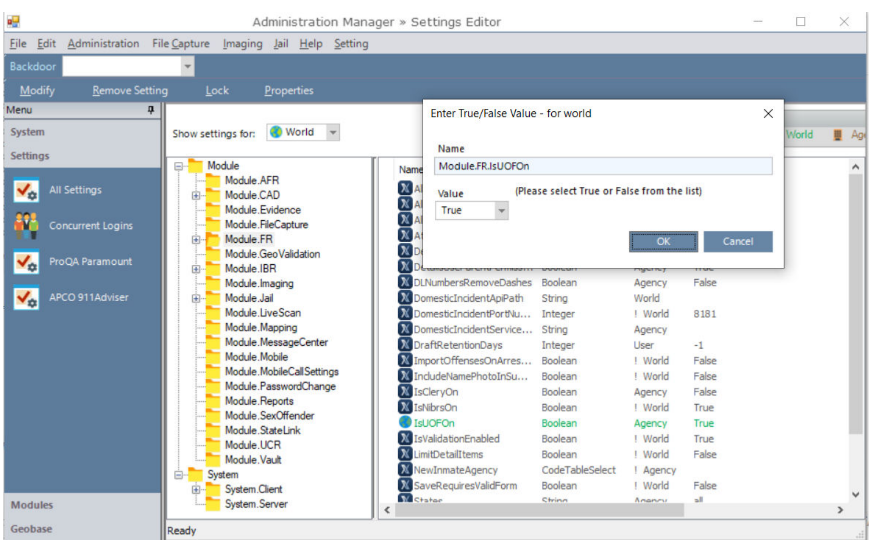
   NOTE: Currently, only the following state codes can be added: FL, PA, NM.

   Figure 160: Module.IBR.UOF.UOFStates Modification

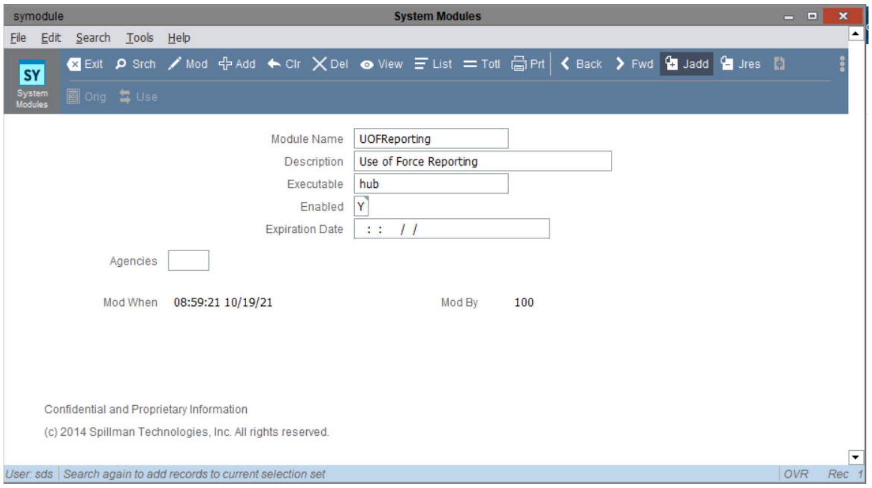
3. In adminutil, set `Module.FR.IsUOFOn` to `True`.

   Figure 161: Module.FR.IsUOFOn Modification

4. Enable `UOFReporting` symodule record.

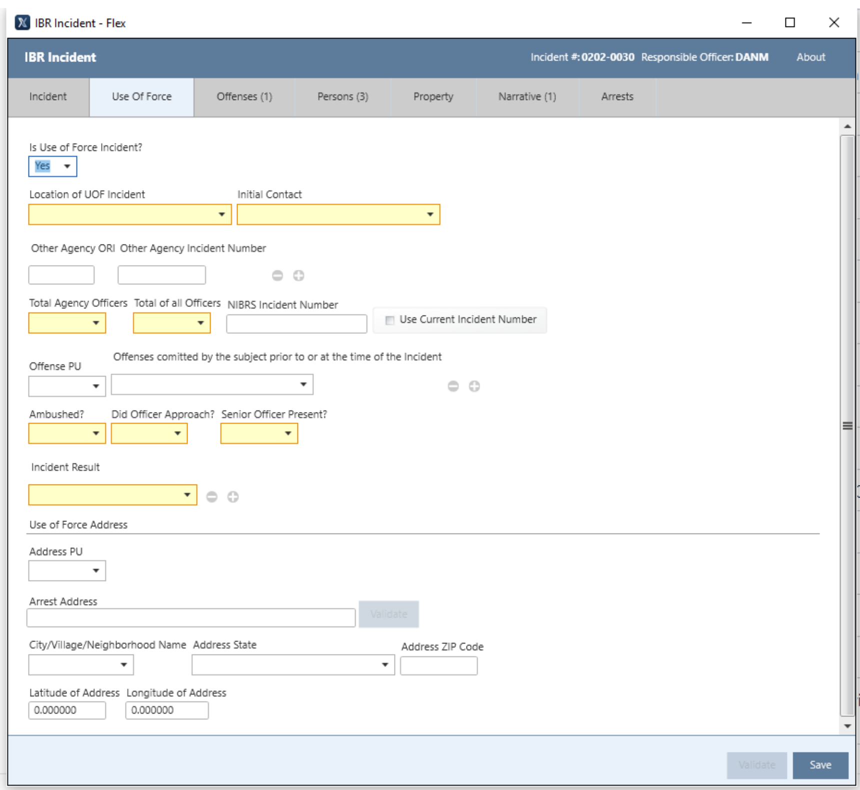
Figure 162: UOFReporting Symodule Record



Result:

The **Use Of Force** client screen, when Use Of Force has been enabled:

Figure 163: Use Of Force Client Screen



6.9
Rapid Notification

6.9.1
Failover WebService URL

You can now add a secondary URL for VESTA to use in the case that the VESTA WebService URL fails in the following field: **VESTA Failover WebService URL**

This failover allows the configuration and logic to automatically use a secondary URL if the primary is unreachable. This enhancement is accessible through a new field on the properties page for each vendor: **VESTA Failover WebService URL**.

In this optional field, you can enter the url that the server will use if the main VESTA WebService URL does not function. The system will use the failover URL until there is a new trigger.

6.10
InSight

6.10.1
InSight Broker Update

The InSight Broker has been updated to remove dependencies on Microsoft Internet Explorer and Microsoft Silverlight, which are both no longer supported by Microsoft.

Users will now be able to access the InSight Broker Web UI through modern web browsers such as Microsoft Edge or Google Chrome.

NOTE:
Agencies must request this update to the InSight Broker through Technical Support. The InSight update is not done automatically as part of a Flex Patch and does not require Flex 2023.3.

This update applies only to InSight Brokers. **No** updates or changes are required on Flex Servers that connect to the InSight Broker.

6.11
StateLink

6.11.1
State-Specific Updates

The following updates have been completed for the following states:

Table 32: StateLink Updates

State	ID	Description	StateLink Version
AZ	SLT-9239	Decommission Message Key NFQI	1.0
	SLT-9275	Run DQ by SSN in CAD	1.0
	SLT-9277	Run Canadian Driver & Vehicle Queries	1.0
HI	N/A	Race Code Translation	2.0

State	ID	Description	StateLink Version
CA	SLT-7767	CARPOS Protected/Restrained Persons Order Type (TYP)	2.0 (CALA)
	SLT-9185	Gun Caliber Updates	2.0 (CLETS)
NY	SLT-8218	Updated Parsing to display and highlight appropriate DL Status, DL Expiration, and Restriction Code values	2.0
NM	DQ: SLT-8566	Import TX Driver and Vehicle Responses	2.0
	RQ: SLT-9240		
ID	SLT-8585	Added CAD/Hit alert functionality	2.0
OK	SLT-9037	Response Parsing Updates	2.0
WA	SLT-9096	Code Table updates to EDP/MDP	2.0

Chapter 7

Release 2023.2

This chapter presents changes made to Flex for the 2023.2 release.

7.1 CAD

7.1.1 Configurable Client Cache Size with Higher Defaults

In the 2023.2 release, each user can open up to eight (8) Flex CAD windows that load quickly thanks to a new default cache setting. The maximum number of cached windows is also increased to ten (10). The previous default values were 2 and 4, respectively. The new values improve the performance of opening multiple windows. Administrators can now configure these settings.

This feature requires the following setting in **adminutil**:

- `Module.CAD.ClientCommandLineParser` – set to `True`

7.1.1.1 Configuring the Amount of Cached CAD Windows

The client cache settings are now configurable. As of the 2023.2 release, you can decide how many cached CAD windows are supported by the Flex application.

NOTE: Beginning with the 2023.3 release, the procedure is different. See Admin: Configuring the Amount of Cached CAD Windows (2023.3+) on page 162.

The initial cache size (the initial number of cached windows) depends on the `initialWindowCacheSize` value, and the maximum size (the maximum number of cached windows) is limited by the `maxWindowCacheSize` value. By default, the values of the settings are 8 and 10, respectively. If, as an administrator, you need to change the default values, perform the following actions.

Procedure:

1. Go to the Flex installation directory.

   Example: `C:\ProgramData\Spillman\Spillman\application\FlexClient`
2. Open `FlexClient.exe.config` by using any text editor.
3. Add the following section:

```
<appSettings>
<add key="initialWindowCacheSize" value="<INITIAL_VALUE>"/>
<add key="maxWindowCacheSize" value="<MAXIMUM_VALUE>"/>
</appSettings>
```

where the ***<INITIAL_VALUE>*** and ***<MAXIMUM_VALUE>*** are integer numbers, and the ***<INITIAL_VALUE>*** is **not** greater than the ***<MAXIMUM_VALUE>***

NOTE:
When the user once opens another window above the ***<INITIAL_VALUE>*** count, and the count is not exceeding the ***<MAXIMUM_VALUE>***, the application will extend the cache size and keep it ready for use after closing any of the open windows. Due to the extended cache size, another window “replacing” the closed one will open more quickly.

When the user has opened the number of windows indicated by the ***<MAXIMUM_VALUE>***, and opens another one, the new window cache is not available anymore after closing the window, so that any “excessive” window needs more time to appear.

4. If needed, restart the Flex client application.

7.2
Interfaces

7.2.1
Flex Export Interface

The Flex Export Interface exports pre-built queries. You can select which pre-built query to run and the destination of the queried data. The following pre-built queries are available:

- Accidents
- Active Inmate Offense List
- Active Inmate Offense List Enhanced
- Active/Released Inmate List
- CAD Calls with Radio Logs
- CAD Calls with Radio Logs Enhanced
- Citations
- emergencyIncident
- Inmate Court Housing

You can choose XML and JSON export file formats as well as the method for exporting the file, such as FTP, FTPS, SFTP, local directory, and email. Either a specified time or user action can initiate an export.

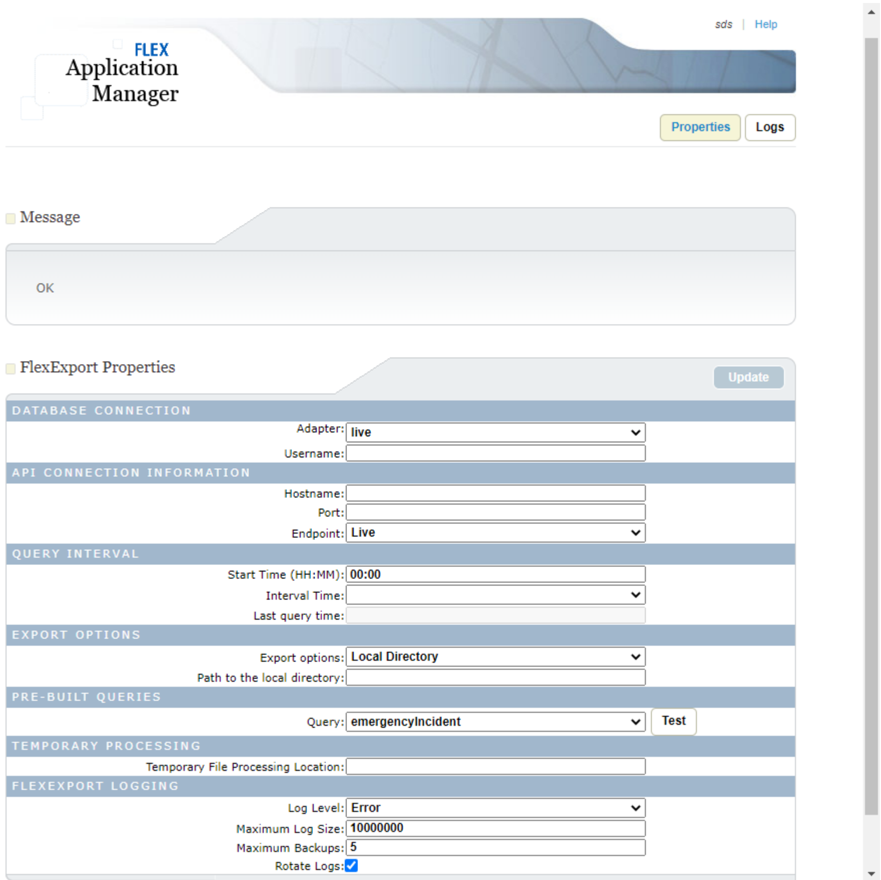
The Flex Export Interface is installed on the Flex server as a Web service that runs on Apache Tomcat. Its operation requires the following system components:

- Flex 2022.1+

The Flex WebApp Manager is the site of the **FlexExport Properties** configuration where you can set:

- Database and Server Connections
- Query Time Parameters
- Data Export Destination Options
- Pre-built Query Selections and Query Testing
- Logging Information and File Options

Figure 164: FlexExport Properties Page



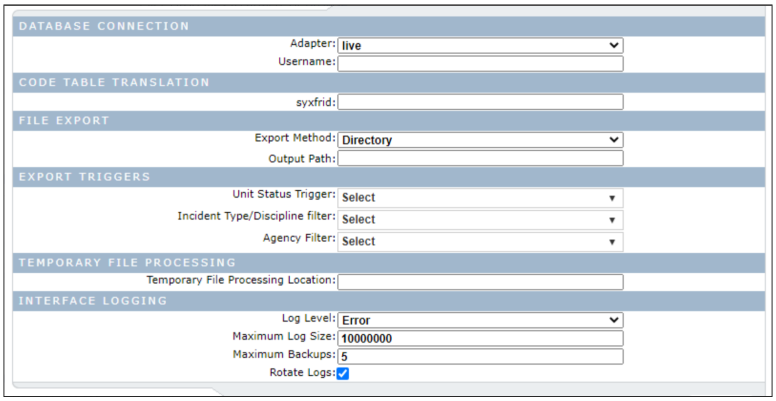
7.2.2
CADIncidentExport

As of the 2022.3 version, agencies that use First Due for Fire and EMS reporting, can now transfer call and incident data into their platform. This is achieved by using the CADIncidentExport webapp.

CADIncidentExport is a new module provided at no additional cost for Flex.

7.2.2.1
Setting Up CADIncidentExport

Figure 165: CADIncidentExport Properties Screen



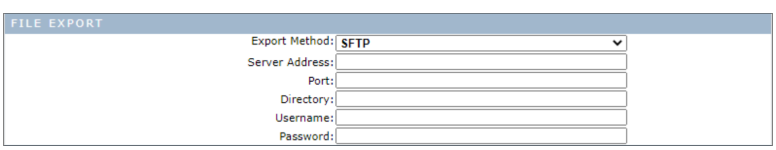
Prerequisites: Confirm that the CADIncidentExport webapp is installed on the Flex server. If it is not, reach out to Technical Support or your Customer Success representative.

Procedure:

1. Set up **DATABASE CONNECTION** properties:
   a. Ensure that the **Adapter** is set to the correct database on your system.

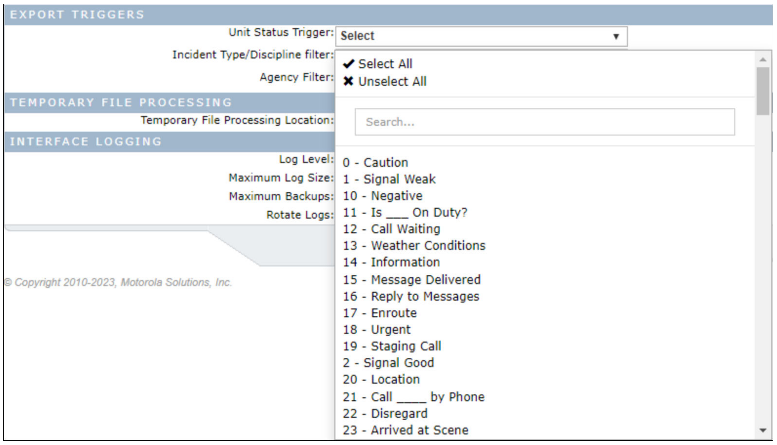
      A typical setting is `live`
   b. Enter a username with which the webapp will communicate with the database.
2. Set up **FILE EXPORT** properties:

   Figure 166: FILE EXPORT Fields

   a. Select the **Export Method** to be used to send the files to a third party host server.
   b. From a third party, obtain the **Server Address**, **Port**, **Directory**, **Username**, and **Password** data and fill in the relevant fields.
3. Set up **EXPORT TRIGGERS** properties:
   a. Select the **Unit Status Trigger** (tb10codes) that will send an update to the third party host server.

Figure 167: Unit StatusTrigger Selection



You should enter all of the tb10codes that are defined in the **cdstatse** table for the agency(s) that are using this interface.

b. Select the **Incident Type/Discipline filter** that is defined for the agency(s) sending data to a third party host server.

c. In the **Agency Filter** field select the agency(s) whose call and incident data you want to send to a third party host server.

NOTE: The Agency filter looks at the **sycad.agency** field, which is populated from the **tbzones.agency** field when a call is created. If the zones for locations where a third party customer is operating are not configured correctly, their call information is not sent by the Flex interface. It is imperative that the **tbzones.agency** values for the locations where they operate are configured correctly. Alternatively, if other agencies own those zones and they cannot change, simply configure those agencies in the Agency Filter on the properties page to ensure the data will be sent.

4. Set up the **TEMPORARY FILE PROCESSING** setting by providing the **Temporary File Processing Location**:

a. Enter a location on your server in which the XML files can reside until they are transferred to a third party host server.

Typically files appear in this folder for less than a second and then are automatically deleted.

5. Click **Save**.

7.3
Hub/Platform

7.3.1
Updated Naming of Flex Application Shortcuts

For naming consistency, starting with the 2023.2 version, the desktop icon to launch the Flex application is renamed to **Flex** instead of "Spillman". In addition to the desktop icon, the Start Menu folder is also renamed to **Flex** along with the application shortcut within.

This happens automatically when the Flex client is updated after a patch to the 2023.2 or a higher version occurs. Any existing custom shortcuts or links will continue to function. The change only affects the name of the Flex shortcuts, so that there are no changes to the Mobile application shortcuts.

Figure 168: Flex Desktop Icons

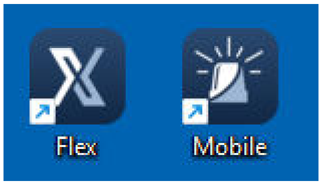
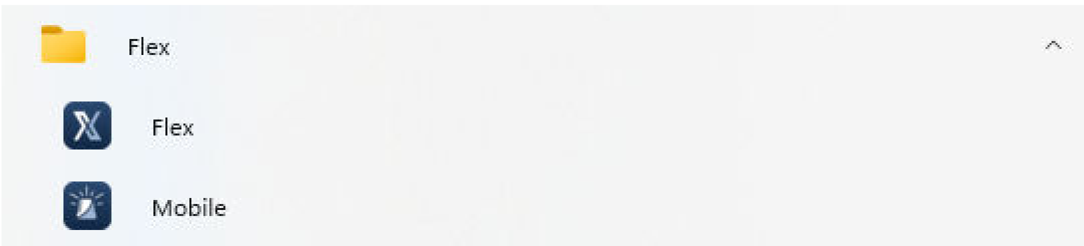


Figure 169: Flex Start Menu Folders



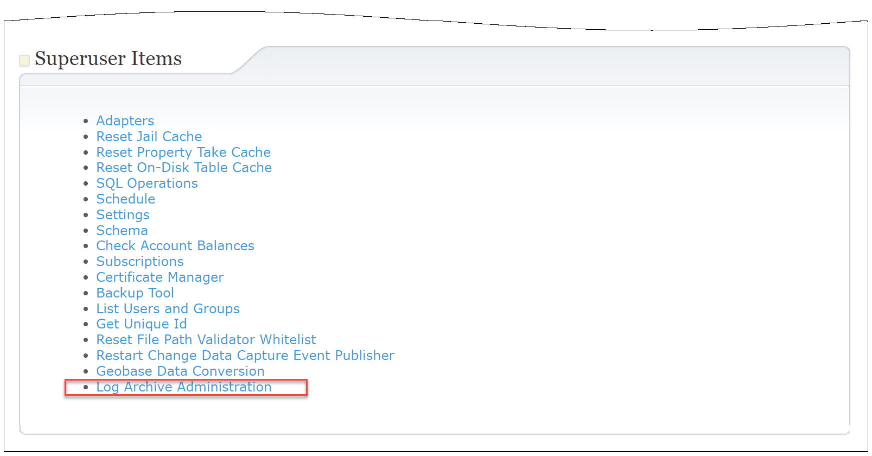
7.3.2 Log Archive Administration Tool

The tool has been created to facilitate archiving and removing records from large tables. It allows agencies to configure settings once and not have to worry about archiving and removing records from those tables. Along with scheduling a reoccurring archive, users can also run any archive tasks manually.

Admin: As a Superuser, you can access the tool from the Flex WebApp Manager:

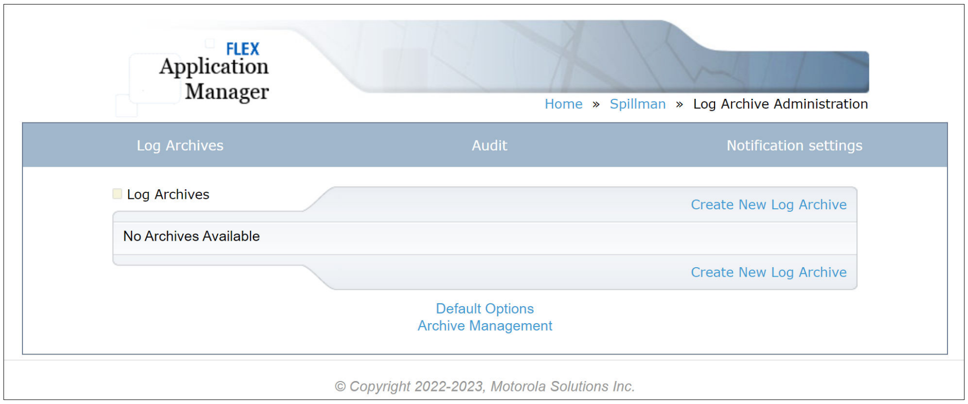
Home → Spillman → Log Archive Administration

Figure 170: Log Archive Administration Link



The available options are shown in the following figure:

Figure 171: Log Archive Administration Options



You can create a new archive configuration by clicking **Create New Log Archive** on the Add/Edit archive page.

Figure 172: Add/Edit Archive Page with the List of Selectable Tables

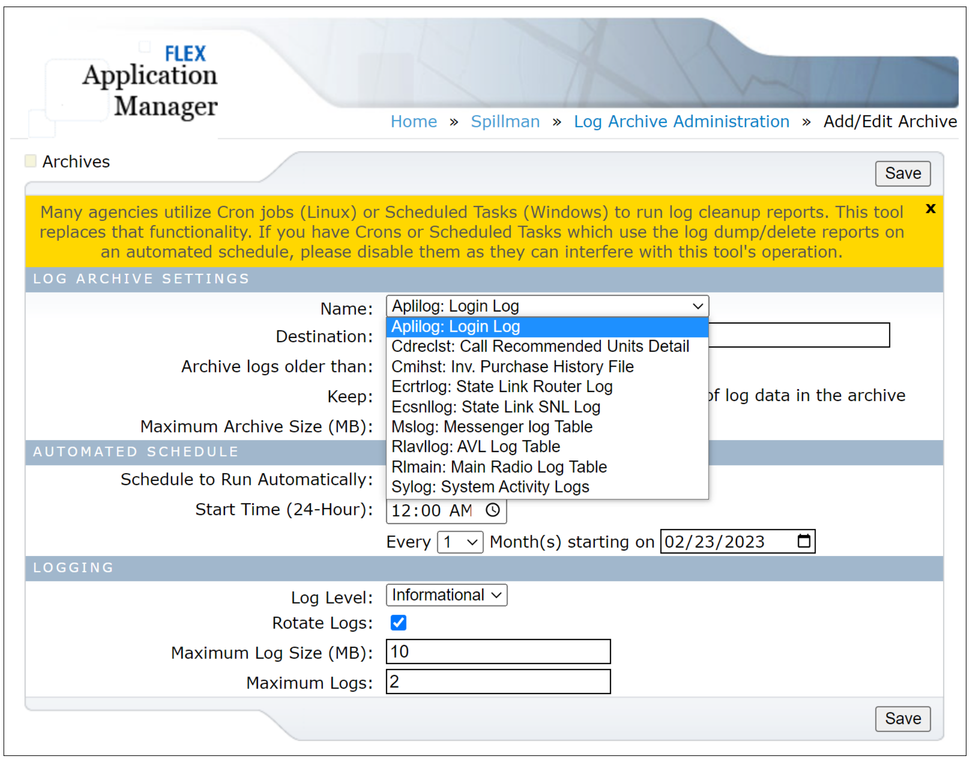


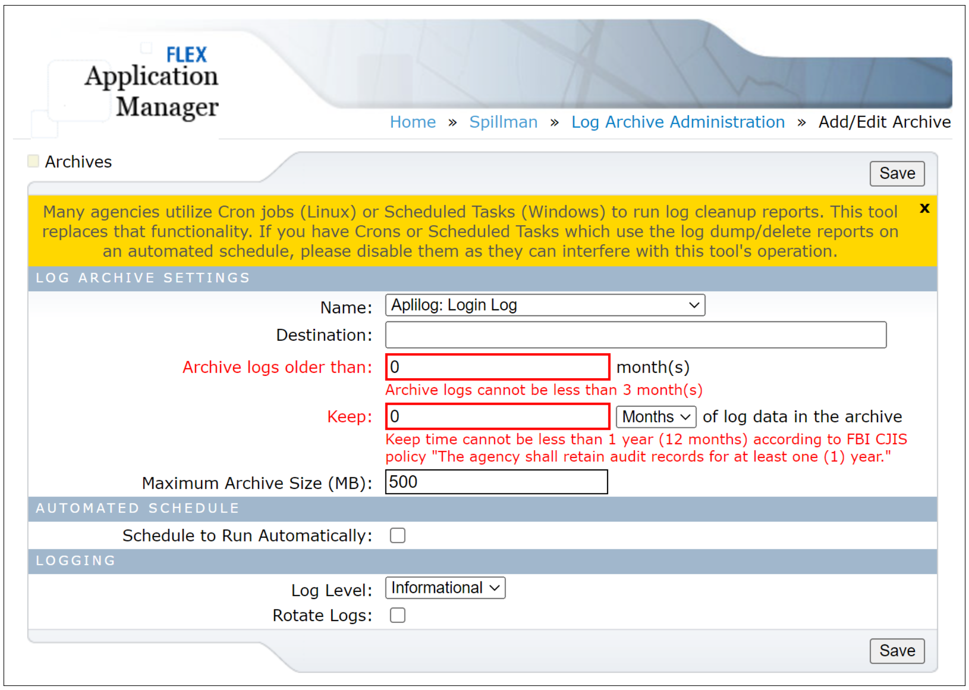
Table 33: Descriptions of LOG ARCHIVE SETTINGS

Setting	Description
Name	The drop-down contains the list of currently available tables that can be selected for archiving.
Destination	Path on a server to store archives.
Archive logs older than	***<x>*** `month(s)` – Any records from the chosen table which are older will be archived and deleted from the database.

Setting	Description
Keep	***<z>*** `Months/Years of log data in the archive` – Stored archive files will be permanently deleted from the file system ***<z>*** months/years after the date the logs were initially archived.
Maximum Archive Size (MB)	The largest size in MB of the archive files allowed on the server hard drive before the operation stops. The log information will remain in the Flex database if the archive operation stops in this way.

When you hover over a field in the **LOG ARCHIVE SETTINGS** section, a tooltip with its description appears. If you attempt to set improper values, individual parameters turn red along with explanations.

Figure 173: Archive Configuration Warnings



AUTOMATED SCHEDULE Settings

Figure 174: Automated Schedule Example

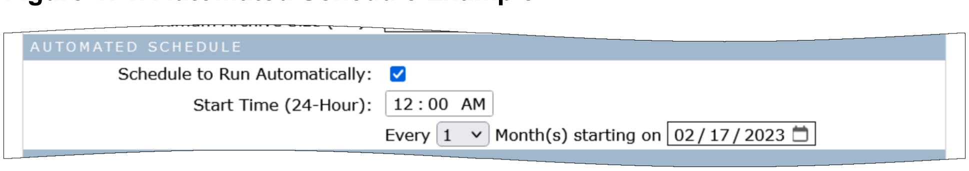


Table 34: Descriptions of AUTOMATED SCHEDULE Settings

Setting	Description
Schedule to Run Automatically	Enable/Disable the automatic archive process with the specified schedule.
Start Time (24-Hour)	Time of the automatic archive execution.
Every *<#>* Month(s) starting on	The interval between archive executions and the date of the first run by schedule (***<#>*** must be an integer).

LOGGING Settings

Figure 175: Logging Settings Example

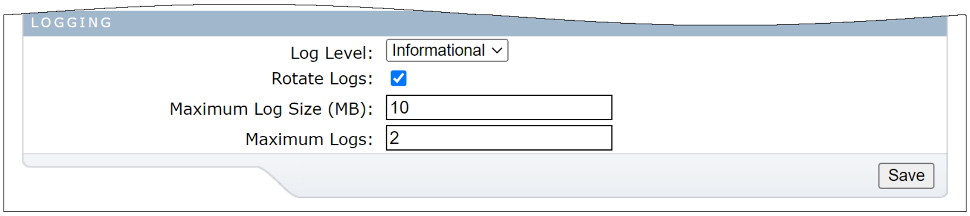
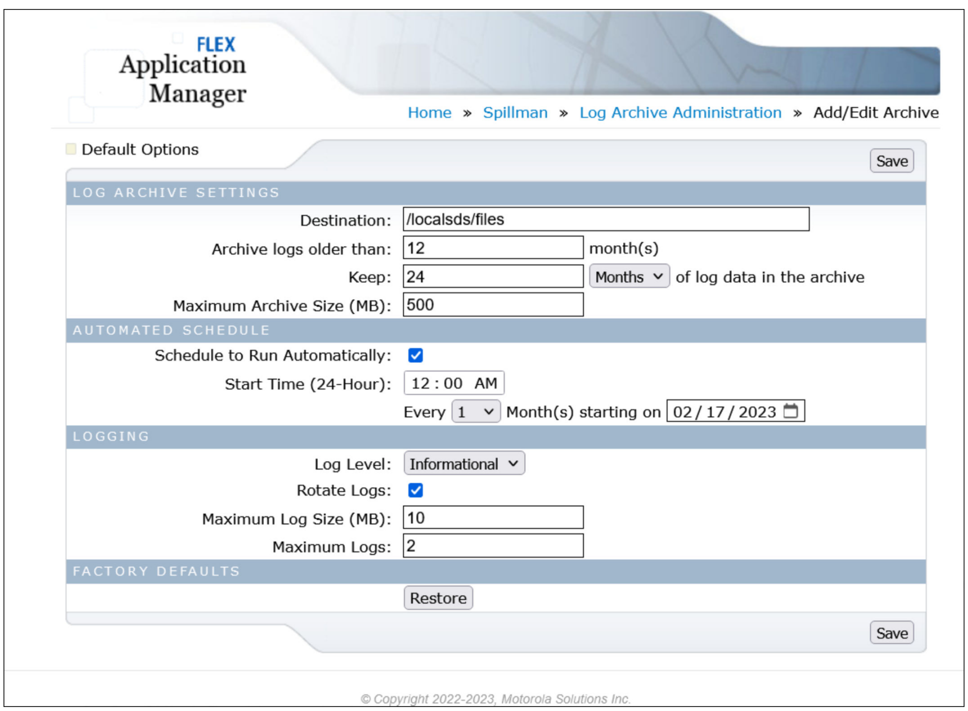


Table 35: Descriptions of LOGGING Settings

Setting	Description
Log Level	Informational/Error/Debug
Rotate Logs	Enable/Disable archive log rotation task.
Maximum Log Size (MB)	Maximum size in MB of one log instance.
Maximum Logs	Maximum number of log instances for the given task.

FACTORY DEFAULTS

Figure 176: Default Options Page with Example Settings

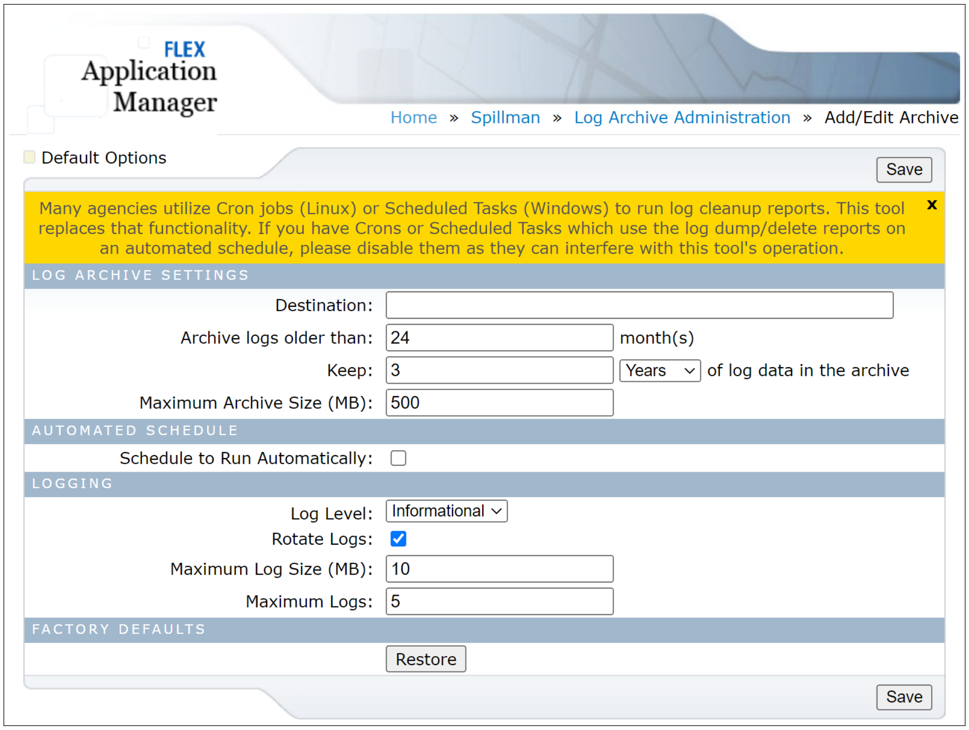


The **FACTORY DEFAULTS** section is available only on the Default Options page.

The Default Options page allows you to set your agency's archive defaults and store them by selecting **Save**. In the upper right corner of the page, the `Default Options Saved` confirmation appears.

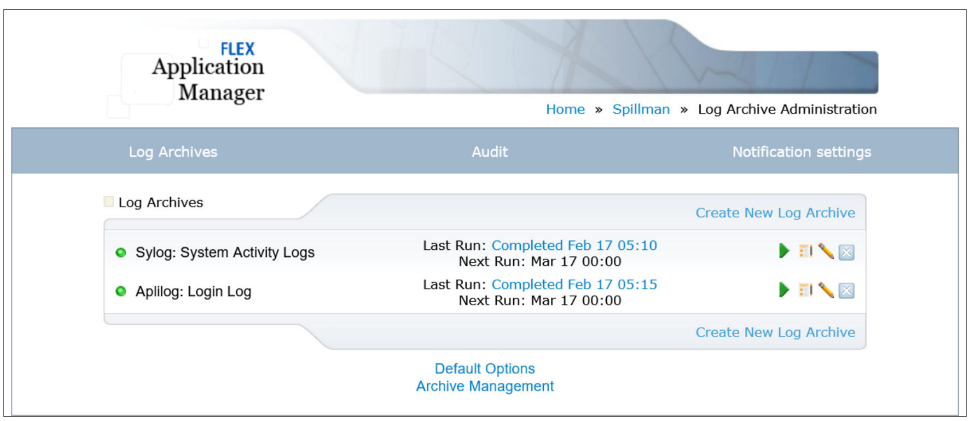
Otherwise, you can select **Restore** which will revert the values of the application settings to the hard-coded defaults. This does not modify the existing backups. Only new backups created afterward are subject to the change.

Figure 177: Default Options – Factory Defaults



Log Archives Tab

Figure 178: Log Archives Tab



This tab shows the tables that were configured to archive, status of the last archive execution, next run time, and the actions panel with the following options (icons on the right, from left to right):

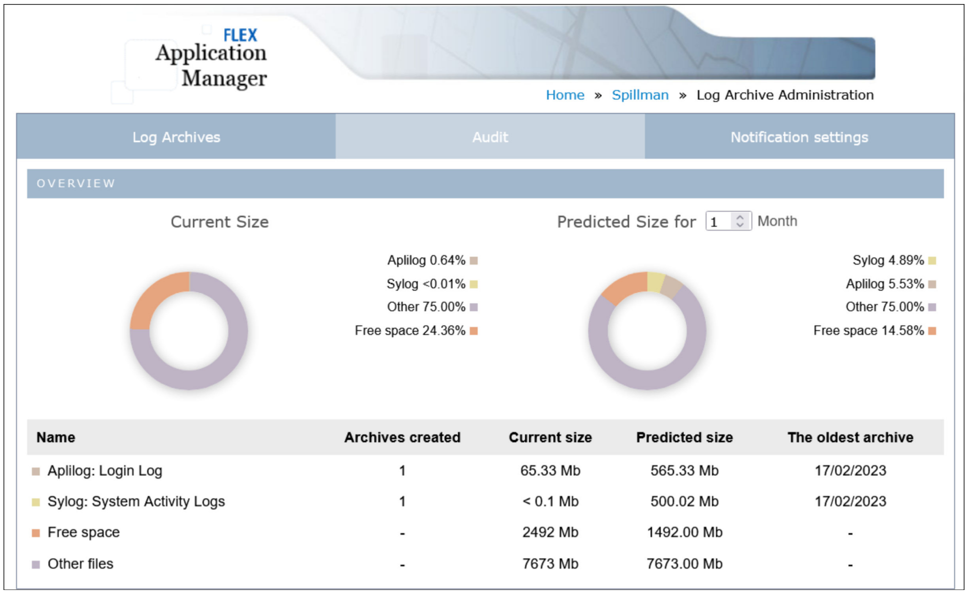
- **Manual run**: Immediate archive task execution.
- **Test run**: Similar to manual run with the only difference that data is preserved in the database (to test the configuration without making any modifications to the actual data).
- **Edit configuration**: To change archive task settings.
- **Delete configuration**: To delete the previously created configuration.

Audit Tab

This tab allows you:

- to check available disk space and how much data is used by the created archives;
- to predict the free/used space in the future after the selected number of months.

Figure 179: Audit Tab

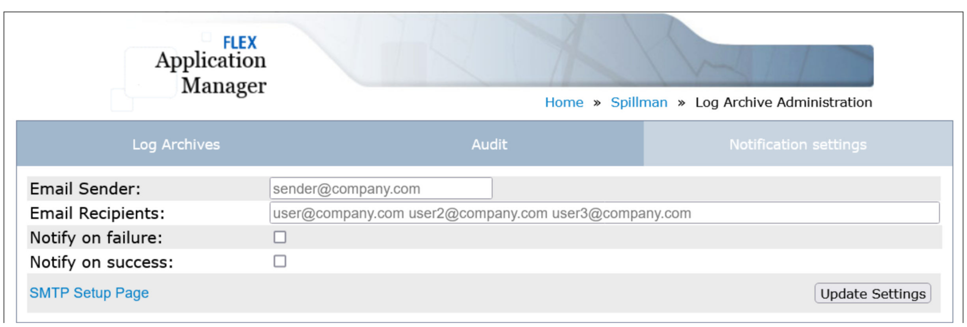


Notification Settings Tab

NOTE: In order for notifications to be sent, an SMTP server connection must be set up on your Flex server.

This tab allows you to set up the email notification for each archive execution task in the case of its success or failure.

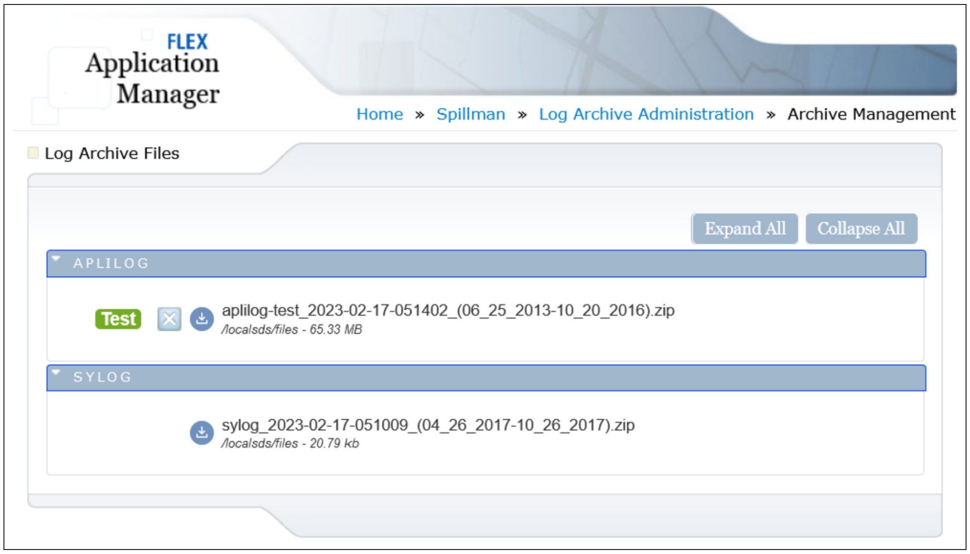
Figure 180: Notification Settings Tab



Archive Management Page

This page contains all archives grouped by database tables, which allows you to download them from the server for a further review. If you used the **Test run**, you have the option to delete test archives as the actual data is preserved in the database.

Figure 181: Log Archive Files on the Archive Management Page



The archive file name format (see examples in the preceding figure): `<database_table>[-test]_<execution_data_time>_(<oldest_record_in_archive>-<newest_record_in_archive>).zip`

7.4
Records

7.4.1
Limited Access Privileges for Evidence Audit Webapp

You can now provide access to the Flex Evidence Audit report to anyone who has the proper sypriv without requiring the user to be an administrator

You can now enable users who are not admins to directly browse the **Evidence Audit Page** located at `https://`***`<FlexServerHostName>`***`:4444/BarcodeScanner/#/audits` by using the new sypriv **scanneraudit**.

7.4.1.1

Admin: Granting Limited Access Privileges for Evidence Audit Webapp

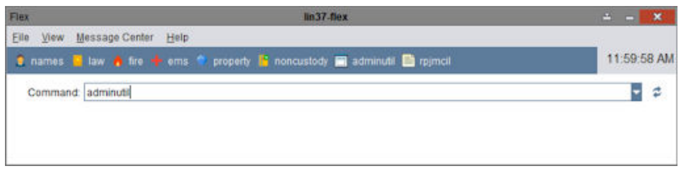
Procedure:

To grant limited access privileges for users, use either the sypriv or adminutil by performing the following actions:

<table>
<tr><th>Option</th><th>Actions</th></tr>
<tr><td>Using adminutil</td><td>

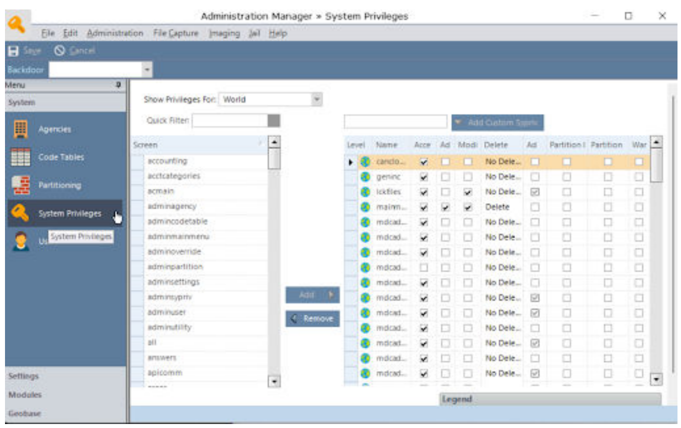
a. Enter `adminutil` at the Flex command line.

Figure 182: Flex Command Line



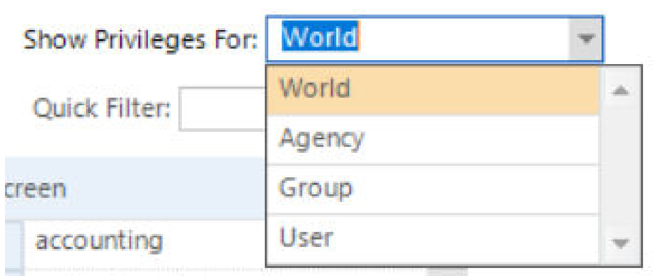
b. Click **System** → **System Privileges**.

Figure 183: Accessing System Privileges



c. Select whether the privilege will apply to **World**, **Agency**, **Group**, or **User**.

Figure 184: Privilege Choices



d. Select which Agency, Group, or User to apply the privilege to.

e. Enter `scanneraudit` into the **Add Custom Sypriv** field.

f. Click the **Add Custom Sypriv** button.

g. To allow access once the privilege is added to the list, check the **Access** column.

</td></tr>
</table>

<table>
<tr><th>Option</th><th>Actions</th></tr>
<tr><td>Using sypriv</td><td>

a. At the command line, enter `sypriv`

The **User Privileges** screen opens.

b. Click **Add**.

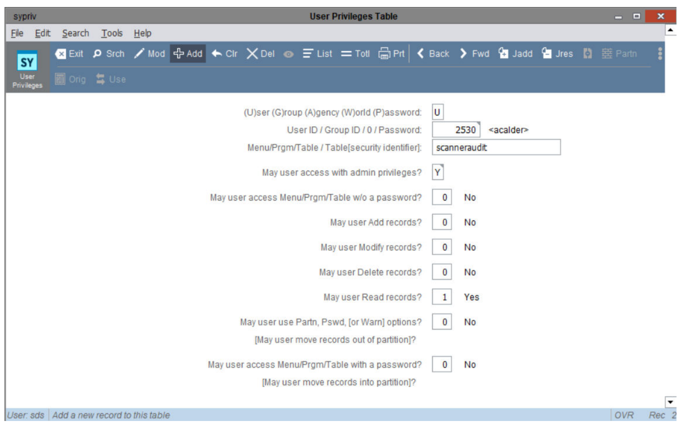
c. Enter the level at which this sypriv will apply.

For more information about sypriv fields, see the *Flex Administrator Manual*.

d. In the **Menu/Prgm/Table/Table[security identifier]** field, enter `scanner audit`

e. In the **May user access Menu/Prgm/Table/Table w/o a password?** field, enter `1`

Figure 185: Completed User Privilege Table



f. To save the record when finished, click **Accept**.

</td></tr>
</table>

7.4.2
Datalogic Memor X3 and Windows Mobile Device Center

The Datalogic Memor™ X3 is based on the Windows Mobile platform and requires the use of the Windows Mobile Device Center (WMDC) in order to synchronize data from the scanner to Flex. Microsoft no longer supports WMDC and it is **not** possible to install the WMDC on later versions of Windows 10 or any version of Windows 11.

Motorola Technical Support is very limited in the support that they can provide on the Datalogic Memor X3 due to the discontinuance of the WMDC software by Microsoft. If your agency is still using the Datalogic Memor X3, we suggest that you speak to your Account Sales representative to ensure continued use of the Flex Evidence Barcoding features.

7.4.3
Texas CR-3 Crash Form

In versions 2022.4 and later, the Texas CR-3 Crash Form has been updated to conform with the new Texas Department of Transportation's requirements for 2023. This updated form will be activated automatically once agencies patch to a version with this update.

Additionally, for agencies using eCrash Submission to directly submit the crash report to the Texas DOT, the submission broker has been successfully recertified by TX DOT to send the 2023 CR-3 Form.

7.4.4
New Jersey NJTR-1 Crash Form

In versions 2022.4 and later, the New Jersey NJTR-1 Crash form has been updated to conform with the new New Jersey Department of Transportation's requirements for 2023.

This updated form will be activated automatically once agencies patch to a version with this update.

7.4.5
New Jersey eCrash Submission

In versions 2023.1 and later, New Jersey Crash Form users are able to electronically submit their completed crash to the State's DOT repository using the NJ eCrash Submission module that has been certified for use by the NJ DOT.

This eCrash Submission module will also enable Crash Reports to be electronically submitted to other repositories via sFTP or Local Directory locations enabling easier dissemination to third-party crash providers. This module is included for all New Jersey agencies that have purchased the NJTR-1 Crash Form.

For more information, see the *New Jersey eCrash Manual*.

7.5
Touch

7.5.1
Increased Stability

In version 1.9.1 of Flex Touch for Android, application stability has been increased resulting in a 95%+ reduction in crashes.

7.6
Jail

7.6.1
Updated Inmate Information

The Inmate Card information has been updated to be consistent across Jail screens.

Booking Date

The **Booking Date** field now shows time since booking details when hovering over this field.

There is also now a new field, the **Complete Date** from the **Sentences** tab, which shows the most recent complete date.

Inmate Screen Inmate Card Arrangement

The information on the Inmate Card on only the **Inmate** screen is presented in the following manner:

Table 36: Inmate Card on the Inmate Screen

Line	Information
First	**Last**, **First**, **MI**, **Suffix**, **Sex**, **Race**, **DOB**
Second	**Gender**, **Ethnicity**, **Hair**, **Eyes**, **Height**, **Weight**, **Name Number**
Third	**Address**, **City**, **State**, **Zip**
Fourth	**Total Remaining Bond Amount**, **Current Inmate Balance**, **Hold Count**

Figure 186: Updated Inmate Card on the Inmate Screen

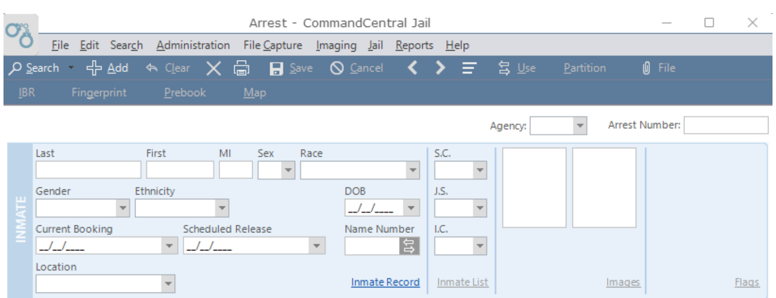
General Inmate Card Arrangement

The information on the Inmate Card is presented in throughout Flex the following manner:

Table 37: Inmate Card throughout Flex

Line	Information
First	**Last**, **First**, **MI**, **Suffix**, **Name Number**
Second	**DOB**, **Sex**, **Race**, **Ethnicity**, **Hair**
Third	**Address**, **Eyes**, **Height**, **Weight**
Fourth	**City**, **State**

Figure 187: Inmate Card throughout Flex



This new inmate arrangement appears on the following screens:

- **Arrest**
- **Non-Custody Booking**
- **Sentence**
- **Inmate**
- **Booking Checklist**
- **Bond**

- **Bond Payment**
- **Assign Housing**
- **Release Checklist**
- **Intake/Release**
- **Inmate Mail**
- **Disciplinary Actions**
- **Assignments**
- **Inmate Requests**
- **Inmate Account Register**
- **Visitation Appointment**
- **Jail Housing Log**
- **Inmate Medical**
- **Inmate Medical Condition**
- **Medical Chart**

7.6.2 Flex Livescan 3.0 Interface

The Flex Livescan 3.0 Interface populates a facility's Livescan application with offender demographic and arrest information during the fingerprinting process. Depending on its setup, the interface can also import additional data and mugshots from the Livescan application and send it to Flex, further simplifying the booking process. Examples of typical outputs are:

- Arrests records
- Inmate records
- Inmate name records
- Booking records
- Offenses

Flex Livescan 3.0 is compatible with the following vendors:

- DataWorks
- Idemia
- Identix
- IDS LiveScan
- InvizeID
- NEC LiveScan
- Printrak

Flex Livescan 3.0 Interface requires the following hardware and software:

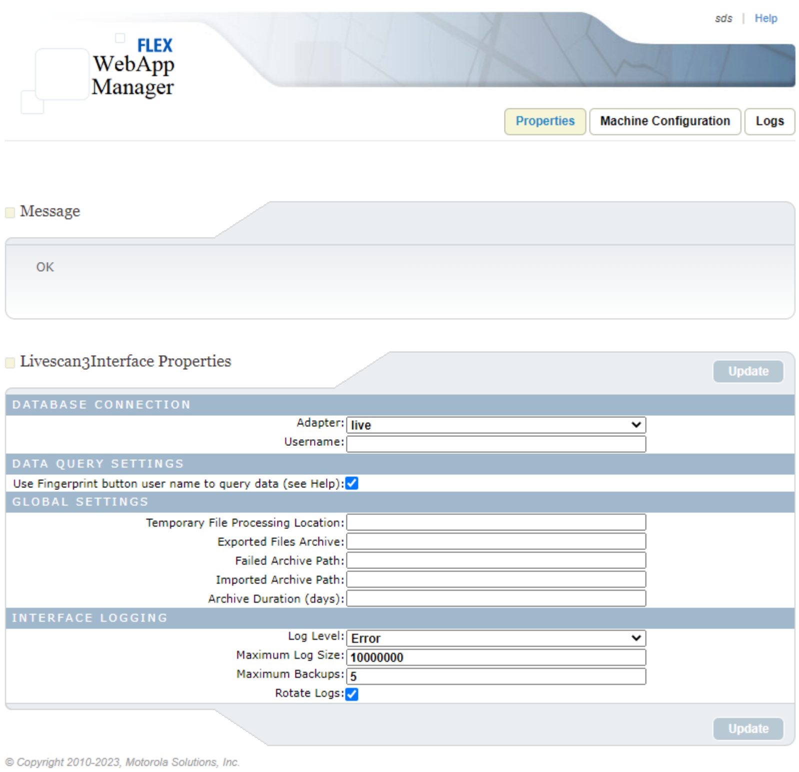
- Livescan machine that is operational and compatible with Flex specifications.
- Local network connection – A local static IP address or hostname for the Livescan server's network card.
- Livescan machine must have a TCP/IP or an intermediary file share system connection to the server on which the Flex software operates.
- Flex RMS and Flex Jail

By default, the Flex Livescan Interface runs DataExchange queries based on system privileges that are assigned to any user who clicks the **Fingerprint** button on the **Arrest** screen of the Flex Client. These system privileges are defined the sypriv privileges list.

The Flex WebApp Manager is the site of the **/Livescan3Interface** configuration where you can set:

- database and server connections
- query time parameters
- data export destination options
- logging information and file options
- Flex Livescan 3.0 machine

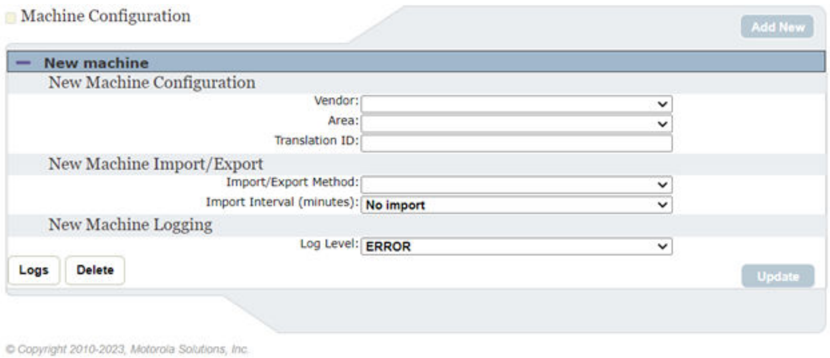
Figure 188: Livescan3Interface Properties Page



The Livescan 3.0 Interface configuration in the WebApp Manager includes configuring the connection to the fingerprinting machine.

The new machine import and export configuration options depend on your area selection for the machine. Either a choice of import/export methods or a socket configuration is made available. Each of them has its own set of configuration options.

Figure 189: Livescan3Interface New Machine Configuration Page

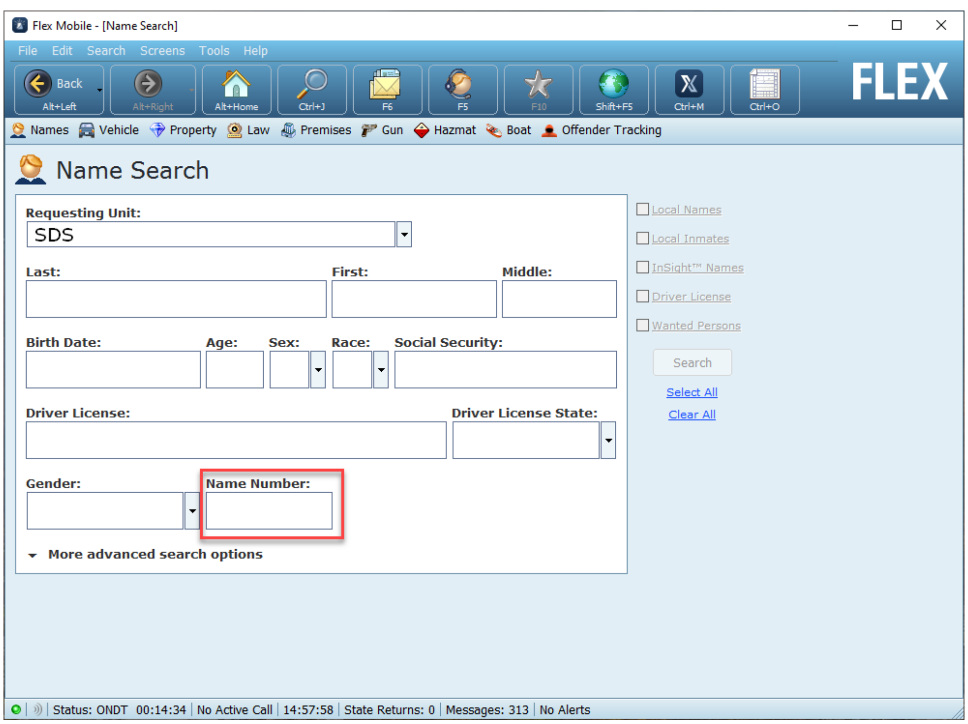


7.7
Mobile

7.7.1
Updated Mobile Name Search Screen

On the **Mobile Name Search** screen, the **Name Number** field has been moved above the **More advanced search options** drop-down area for ease of access.

Figure 190: Mobile Name Search Screen



7.8
IBR

7.8.1
Ability for Users to Not Send Records to IBR

If your agency is in Utah, you are now able to NOT send specific offense or name records to IBR.

This will reduce the number of `Mutually Exclusive` validation errors and assist agencies in completing reports that are IBR compliant and containing information that is relevant to the case, but is not deemed relevant by FBI IBR specifications.

This feature will be expanded to other states in the near future.

7.8.1.1
Admin: Allowing Users to Not Send Records to IBR

You must set up the application setting to enable the use of IBR in your agency.

Procedure:

In the **Module.IBR** setting folder, set up the setting based on information in the following table, as required by your agency:

Table 38: Module.IBR Settings

Setting	Description	Value
AllowSelectedOffenseVictimNotSendToIBR	Indicates whether your agency can allow users to NOT send selected name or offense record information to IBR. ● Set to **True** to enable users to NOT send record or name information to IBR. ● Set to **False** to **not** enable users to NOT send record or name information to IBR.	**True**/**False**

NOTE:
If the `Module.IBR.IBRStates` and state of the Incident is not UT (Utah), this setting will have no affect.

7.8.2
Statutes Expiration Tool

This new feature is available as of Flex release 2022.4. The statutes expiration tool is used to expire and unexpire (restore as valid) tblaw records in the Flex system.

The statutes (tblaw) table is used in various subsystems of Flex. It has one unique index having one field, **Abbreviation** (tblaw.abbr). It is shared by all agencies on a Flex server and no agency filtering or partitioning is supported. The use of this fast tool for expiring multiple statutes implies global changes for all statutes being expired or unexpired. Access to the IBRProcessor webapp is limited to administrators and possibly IBR Records Clerks.

After change are made in the Manage Statutes tool, Expired or Unexpired statutes are hidden/displayed to users upon their next login.

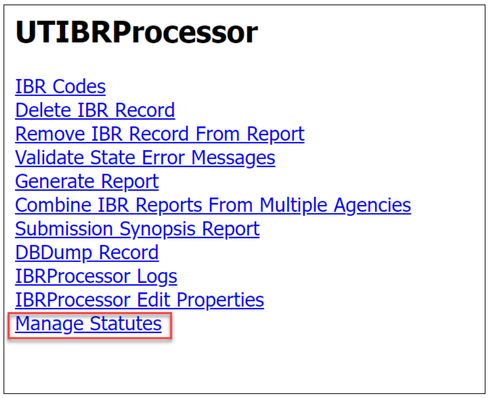
Admin: Manage Statutes Tool

You can access the tool from the Flex WebApp Manager:

Interface → /<yourstate>IBRProcessor → Manage Statutes

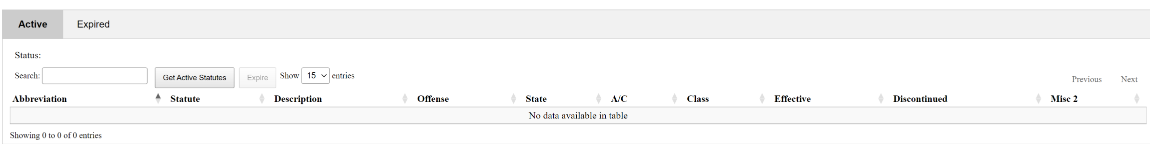
Example: **Interface → /UTIBRProcessor → Manage Statutes**

Figure 191: UTIBRProcessor



The page shown in the following figure appears.

Figure 192: Manage Statutes Page



The tool shows two tabs at the top, **Active** and **Expired**. Only one tab is active at a time showing its child tab contents. You must use your mouse to click the tabs.

For more information about the **Active Statutes** tab-specific buttons and the **Expired Statutes** tab-specific buttons, see the relevant sections in the *Flex Incident Based Reporting (IBR) Manual.*.

NOTE:
The tool does not ask for a confirmation of the action, so you must only press the **Expire** or **Unexpire** buttons if you intend to execute the operation.

The following elements are present on both tabs:

Table 39: Manage Statutes Page Elements

Element	Description
Status	The status text shows the status of attempted operations, or the failure of the same. It displays `OK` if it is successful. Errors are logged as well as shown.
Search bar	Supports searching using data or partial data found across all visible columns. Searching is not case sensitive. You can clear the search text by hovering over the control and pressing the **X** box.

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Pagination</td><td>

By default, 15 rows are shown in both tables if there are 15 records to display. This is to accommodate one tool for many states and types of statute records. You can select **10**, **15**, **20**, **25**, or **30** records to display in the tables.

On the right-hand side on the top of the tables are the following buttons: **Previous**, page number(s), and **Next**.

You can manually scroll through table records using these buttons. At the bottom of the tables is text describing how many records are shown and how many rows are currently selected.

</td></tr>
<tr><td>Columns</td><td>

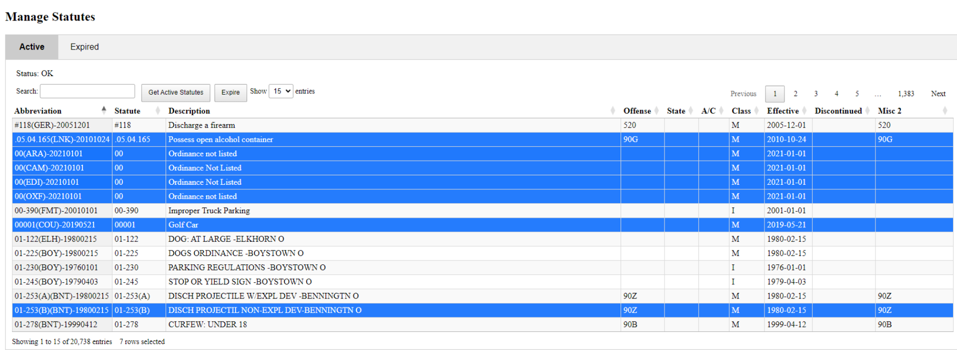
The column width for the rows is mostly auto-generated and sometimes column data wraps. Column widths cannot be manually resized.

For the best view of column data, you should maximize your browser when using this tool. You can sort the data in the tables by clicking on a column header.

</td></tr>
<tr><td>Rows and Row Selection</td><td>

The top row or column headers are frozen so if you need to scroll down vertically, it always shows this top row.

Figure 193: Rows and Row Selection



For more information about how to select rows, see the relevant sections in the *Flex Incident Based Reporting (IBR) Manual*.

</td></tr>
</table>

7.9 Rapid Notification

7.9.1 Limited Access Privileges for Rapid Notification 2.0 Users

You can now give access to dispatchers and supervisors without giving access to complete configuration of the application server by configuring the sypriv.

7.9.1.1

Admin: Granting Limited Access Privileges for Rapid Notification 2.0 Users

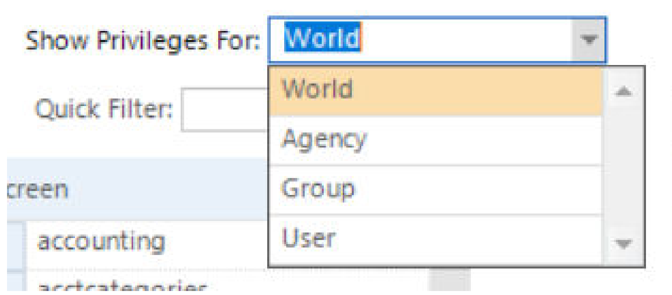
Procedure:

To grant limited access privileges for users, use either the sypriv or adminutil by performing the following actions:

<table>
<tr><th>Option</th><th>Actions</th></tr>
<tr><td>Using adminutil</td><td>

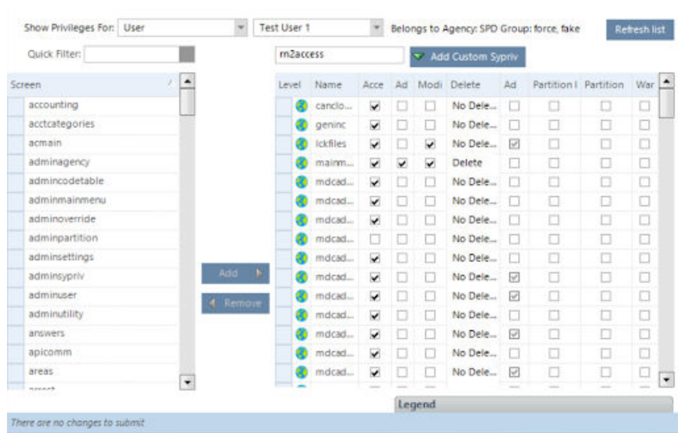
1. Enter `adminutil` at the Flex command line.
2. Click **System** → **System Privileges**.
3. Select whether the privilege will apply to **World**, **Agency**, **Group**, or **User**.

Figure 194: Privilege Choices



4. Select which Agency, Group, or User to apply the privilege to.
5. Enter `rn2access` into the **Add Custom Sypriv** field.
6. Click the **Add Custom Sypriv** button.

Figure 195: rn2access Configuration



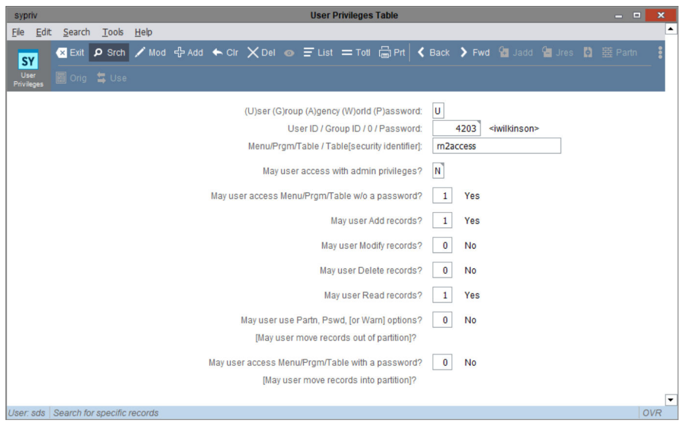
7. To allow access once the privilege is added to the list, check the **Access** column.

</td></tr>
</table>

<table>
<tr><th>Option</th><th>Actions</th></tr>
<tr><td>Using sypriv</td><td>

1. At the command line, enter `sypriv`
   The **User Privileges** screen opens.
2. Click **Add**.
3. Enter the level at which this sypriv will apply.
   For more information about sypriv fields, see the *Flex Administrator Manual*.
4. In the **Menu/Prgm/Table/Table[security identifier]** field, enter `rn2access`
5. In the **May user access Menu/Prgm/Table/Table w/o a password?** field, enter `1`

Figure 196: Completed User Privilege Table



6. To save the record when finished, click **Accept**.

</td></tr>
</table>

Chapter 8

Release 2023.1

This chapter presents changes made to Flex for the 2023.1 release.

8.1 CAD

8.1.1 Ability to Add and Use the No DOB Check Box for Demographics

There are legitimate reasons why an officer may not be able to capture a Date of Birth (DOB), despite that an entry for this field might be required.

Now, in the **STOPPED PERSON** and **Update Type Status** sections of the **CAD Incident** screen, and in interim **Update Demographics**, and **Complete Call** windows in Mobile, agencies can add **No DOB** check box to allow officers to record that they did not have a DOB to enter.

As an admin in the agency that needs to gather demographic information, you can enable the feature by performing the following task: Admin: Enabling the No DOB Check Box for Demographics on page 206.

For more details about this feature, see "No DOB" Check Box for Demographic Information on page 207.

8.1.1.1 Admin: Enabling the No DOB Check Box for Demographics

By default, the **No DOB** check box is not displayed. If you need to make the check box available for users in your agency, you must set it up.

Prerequisites: Ensure that the value of the `module.cad.trafficStopScreenLayout` setting is set to `Demographics` or `All`.

NOTE: In Mobile, the **Demographics** tab is active only if the `module.cad.trafficStopScreenLayout` setting is set to `Demographics`.

Procedure:

1. At the command line, enter `adminutil`
2. From the tree menu, expand the **Module** folder and click the **Module.CAD** folder.
3. In the settings window on the right, locate the `TrafficStopNoDOBForDemographics` setting and double-click it.

   The **Enter True/False Value - for world** dialog box opens, with the `False` default value of the `TrafficStopNoDOBForDemographics` setting.
4. Set the **Value** to `True` and click **OK**.
5. Close the **Administration Manager >> Settings Editor** window.
6. Restart the Flex Client.

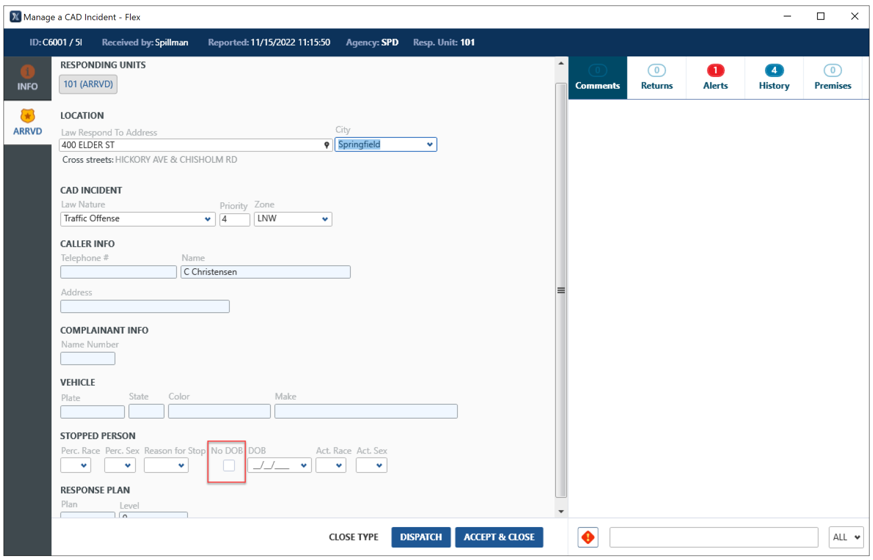
8.1.1.2
"No DOB" Check Box for Demographic Information

The date of birth might be required to close a type or complete a traffic stop call. If your admin enabled the **No DOB** check box, you should select it when you are unable to enter the date of birth of a stopped person.

Use of the "No DOB" Check Box in Flex

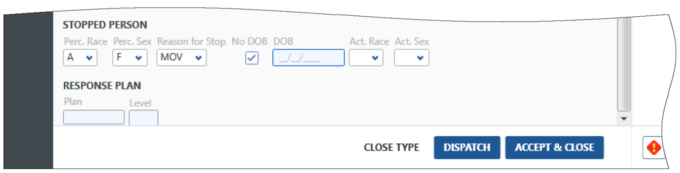
When your admin enabled the **No DOB** check box and you deal with a traffic stop, the box is located in the **STOPPED PERSON** area of the CAD Incident status screen.

Figure 197: No DOB Check Box



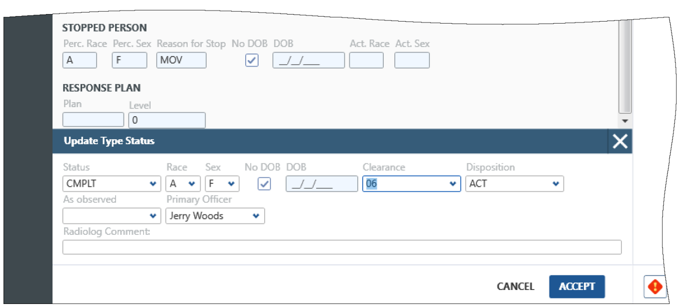
If the DOB cannot be determined, you are able to handle the call by selecting the **No DOB** check box. Then, the **DOB** field becomes inactive.

Figure 198: No DOB Check Box Selected



With this selection, you can update the call status without providing the date of birth, for example you can close the call by choosing **CLOSE TYPE**

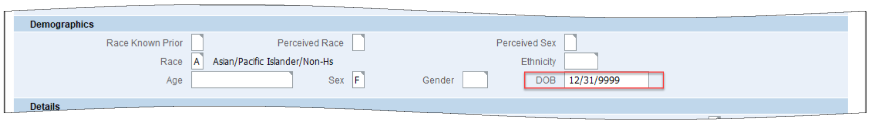
Figure 199: Update Type Status Data with No DOB Option



When you fill in all the required fields, you can close the type without a DOB entry by clicking **ACCEPT**.

In the **rcmain** table, the effect of selecting the **No DOB** field is shown in the following figure (a fictional date: `12/31/9999`).

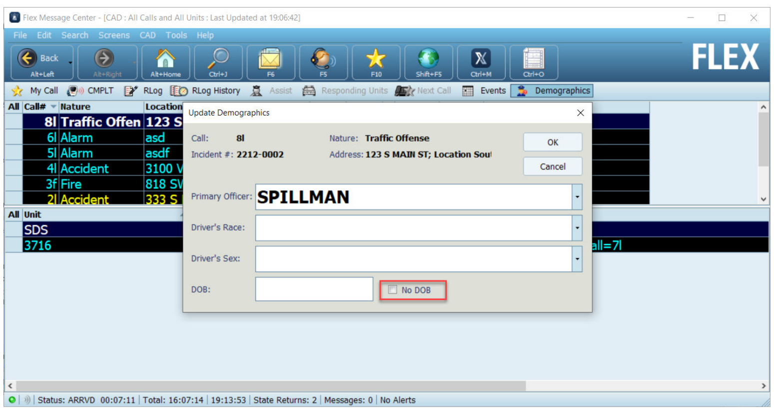
Figure 200: No DOB Appearance in the rcmain Table



Use of the "No DOB" Check Box in Mobile

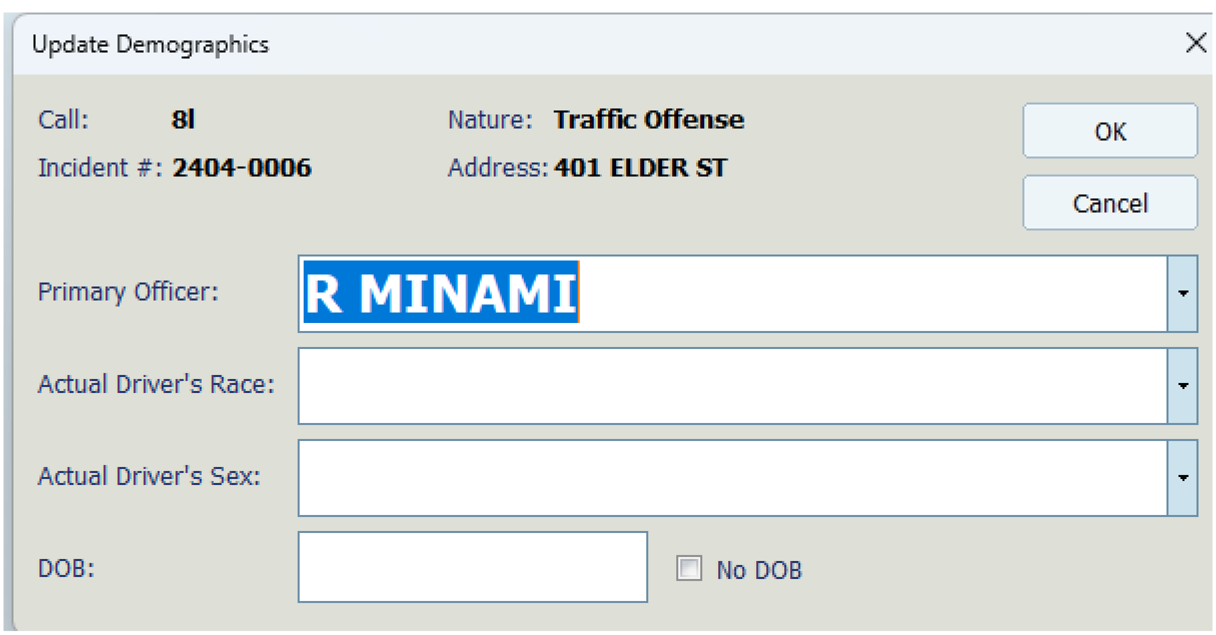
In Mobile, when your unit is assigned to the call, the **No DOB** field is available in the **Update Demographics**, and **Complete Call** windows. When you, as an officer, tap the **Demographics** tab and cannot provide the date of birth of the stopped person, you should select the **No DOB** field.

Figure 201: Update Demographics Window with No DOB Check Box



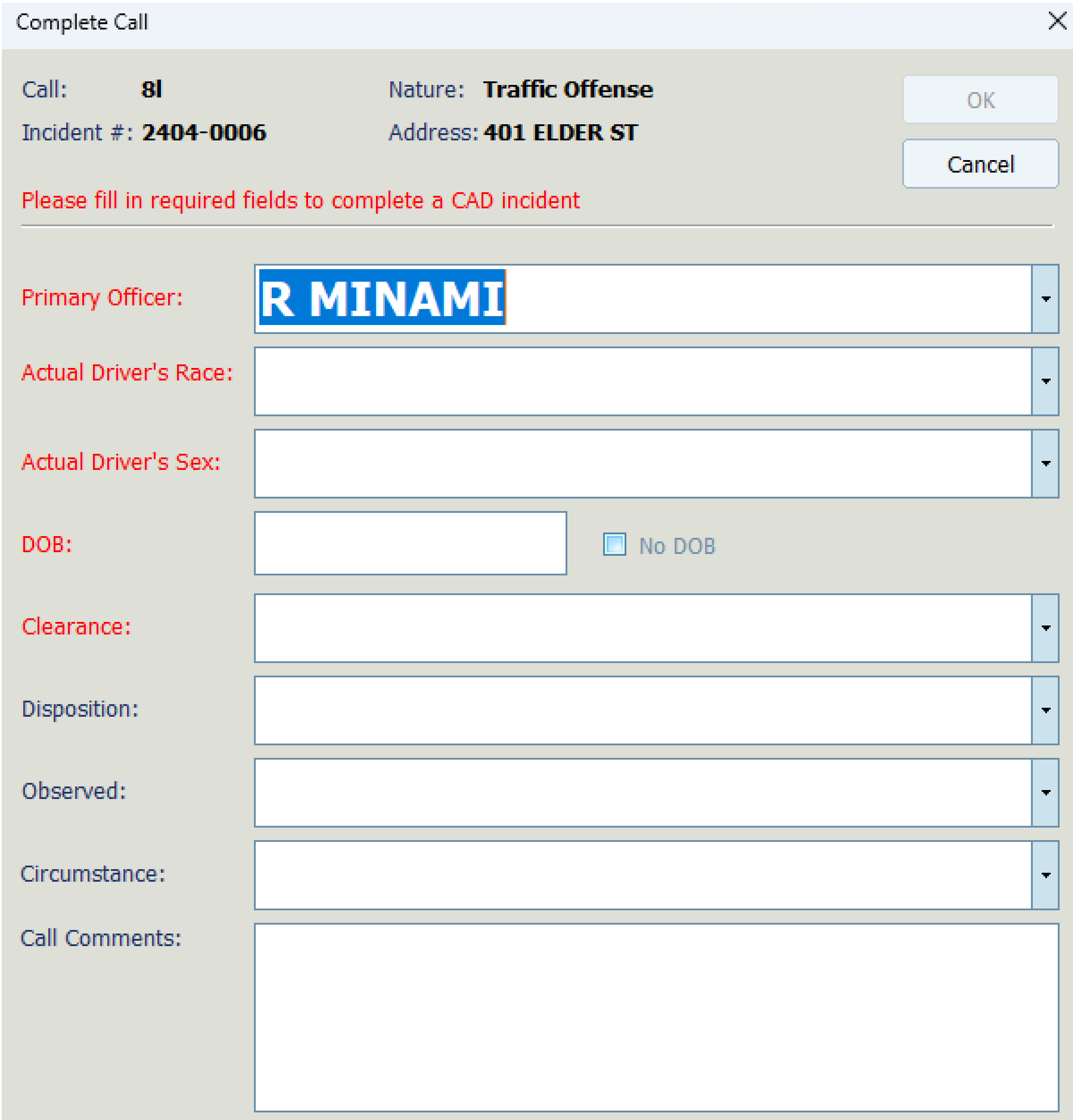
In the **Update Demographics** window, the **DOB** field becomes inactive, so that is not required.

Figure 202: Update Demographics Window with Inactive DOB Field



When you want to complete the call by tapping the **CMPLT** tab, the **No DOB** selection is transferred to the **Complete Call** window.

Figure 203: Complete Call Window with No DOB Selected



If you did not select the **No DOB** check box in the **Update Demographics** window, you can close the call without providing DOB directly in the **Complete Call** window by selecting the **No DOB** check box there.

8.1.2
Validation of the DOB Entry

The introduction of the DOB entry validation helps to eliminate obvious errors.

The general limitation is that the DOB date, either selected from the calendar or entered manually, must be between one (1) and one hundred (100) years in age against the current date. If this formal requirement is not met, a warning message in red appears.

Figure 204: Invalid DOB Date Warning (Wrong Choice from Calendar)

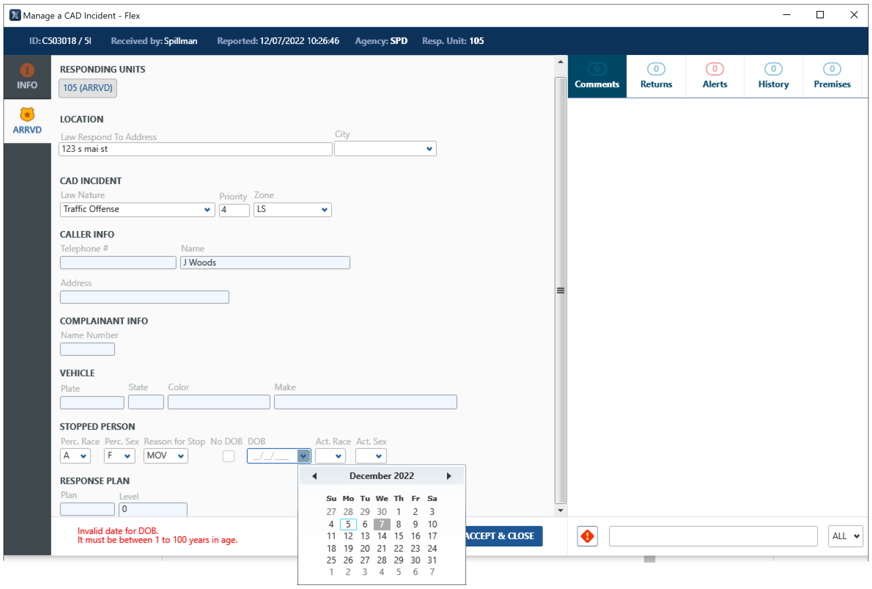
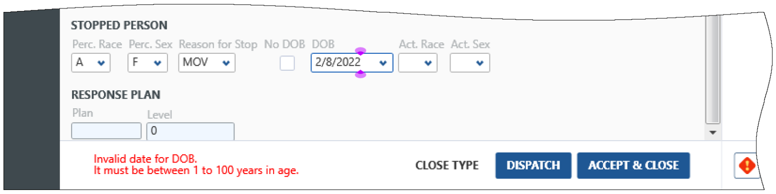


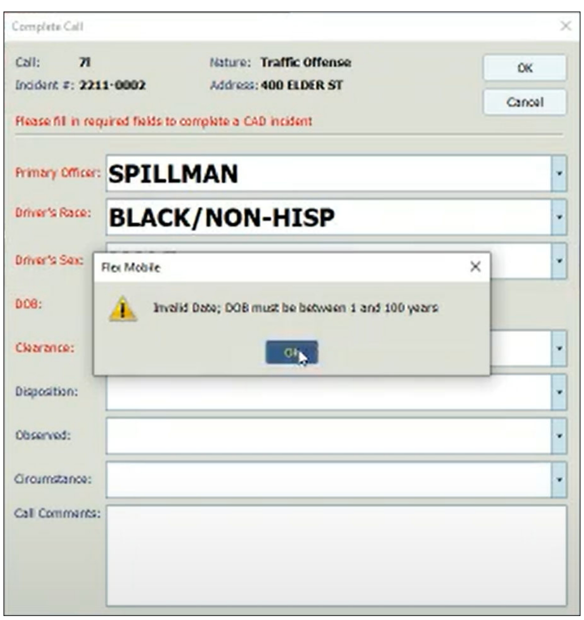
Figure 205: Invalid DOB Date Warning (Wrong Entry)



The invalid date must be corrected, otherwise the DOB field remains empty. In turn, an attempt to change a formally correct date to an invalid one results in keeping the original date.

The relevant warning also appears in the case of an attempt to enter an invalid DOB date in Mobile.

Figure 206: Invalid DOB Date Warning in Mobile



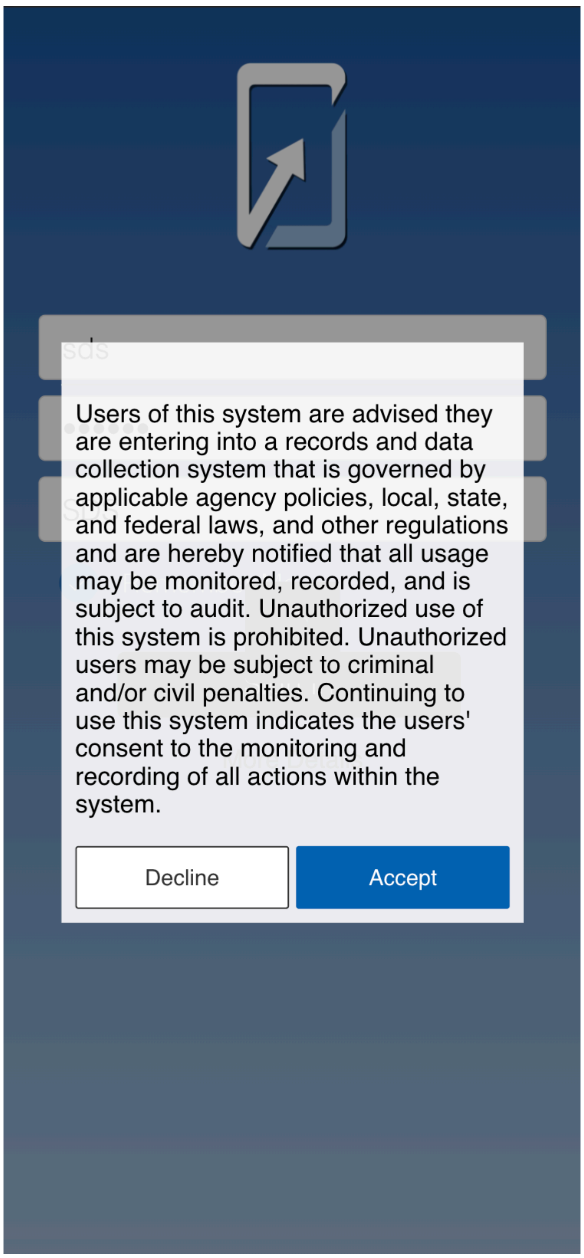
8.2
Hub

8.2.1
System Use Notifications

System Use Notifications are set system-wide within Flex. Agencies can use System Use Notifications to meet FBI CJIS Security Policy 5.5.4 requirements.

Once activated, System Use Notifications take effect upon login for Flex Desktop, Flex Mobile, and Flex Touch.

Figure 207: System Use Notification in Flex Touch



To learn how to set a system use notification, see Setting Up System Use Notification on page 212.

For more details about CJIS message results, see Reviewing System Use Notification Message Acceptance Results on page 212.

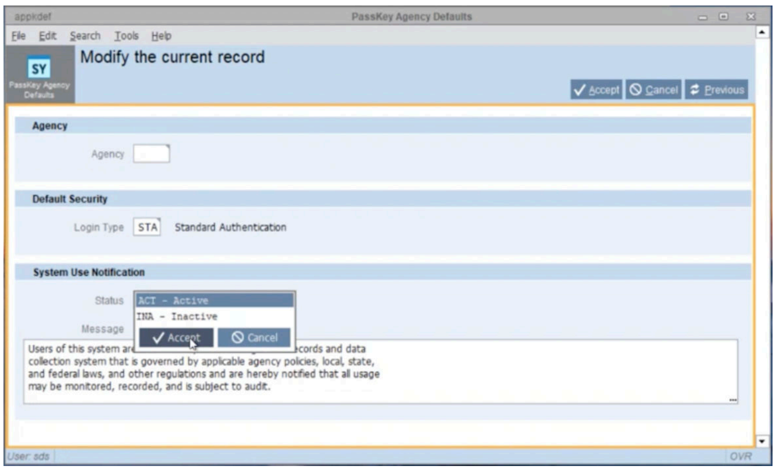
8.2.1.1
Setting Up System Use Notification

You can set up a system use notification for users to accept when they log in to Flex.

Procedure:

1. Open the **appkdef** table.
2. In the **Status** field, switch the **System Use Notifications** field to **ACTIVE** or **INACTIVE**.

   Figure 208: appkdef table

   Users will now see the message in **Message** text box when they first log into Flex Touch.
3. To change the text of the default CJIS message, alter the text in the **Message** text box.

8.2.1.2
Reviewing System Use Notification Message Acceptance Results

For more information, you can review the system use notification message acceptance results in the **aplogin** table.

Procedure:

To review the system use notification message acceptance results, open the **aplogin** table.

The following are examples of system use being accepted.

Figure 209: aplogin Successful Login Message

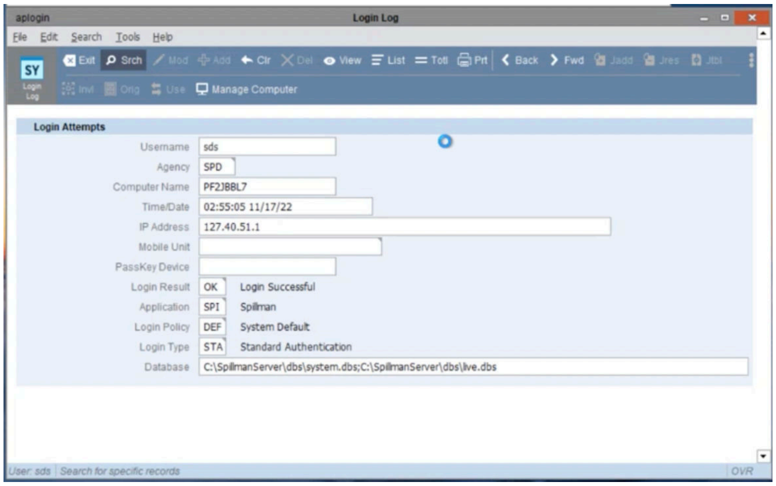
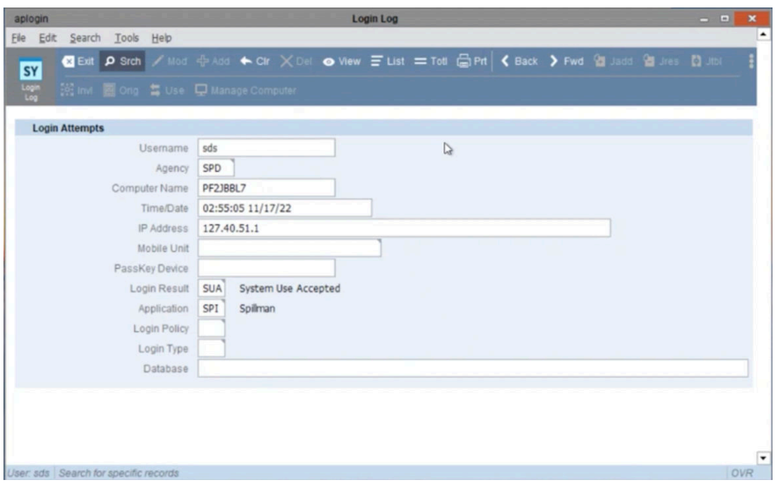
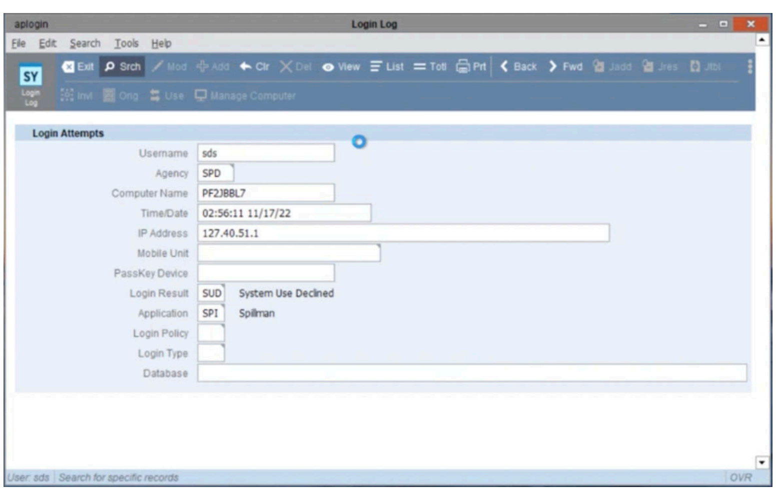


Figure 210: aplogin System Use Accepted



The following is an example of system use being declined.

Figure 211: System Use and Login Declined



8.2.2

Admin: Separate Last/First/Middle Fields in the apnames Table

As of the 2023.1 release, the **Official Names Codes** table (**apnames**) has **Last**/**First**/**Middle** fields below the **Full Name** field. This feature is available by default.

The feature reduces the number of steps needed when adding a new user, as many interfaces and reports require officers First, Last, and Middle names in separate fields.

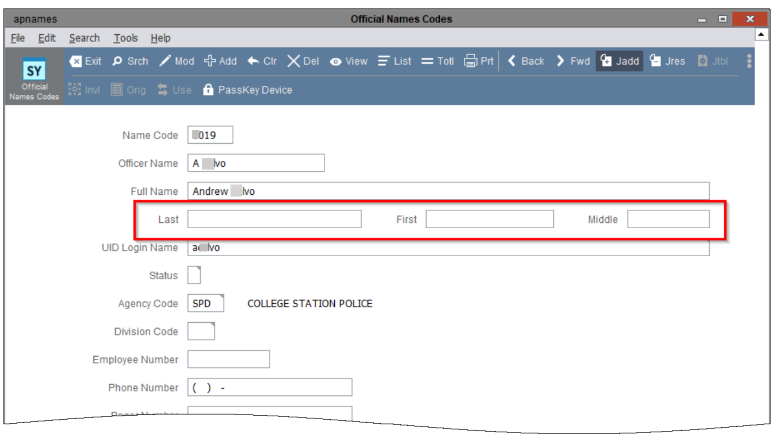
This enhancement places the respective fields from the **Employee Table** (**pemain**) – **Last**, **Fst**, and **Mid** – on the **Official Names Codes** (**apnames**) table. If the **Employee Num** field is already populated with a number, the employee table record with that Employee Number will be automatically updated with changes made to the **Last**, **First**, and **Middle** name fields.

If the **Employee Num** field is blank, and an entry is made in the **Last**, **First**, **Middle** fields, an entry will be created in the **Employee Table** and that employee number will be automatically populated in the **Employee Num** field.

This enhancement does not require the purchase or activation of the Flex Personnel Module.

NOTE: If not previously populated in the **Employee Table**, the data has to be filled in by agency. It will **not** automatically parse from the **Full Name** field.

Figure 212: First, Middle, and Last Names in the apnames Table



8.3

Records

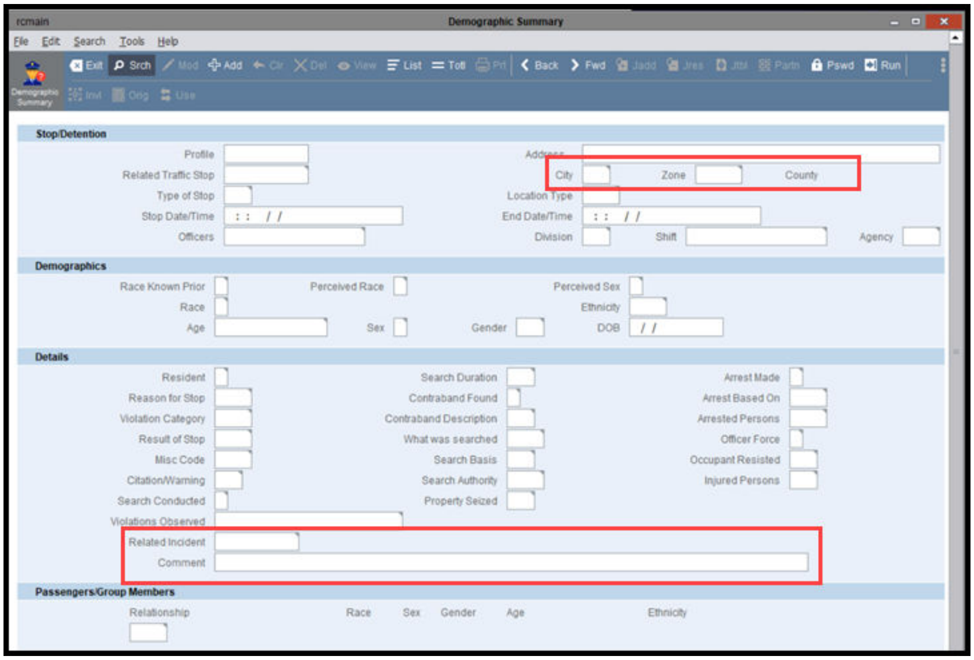
8.3.1

Changes to the Demographics Screen (rcmain)

As of the 2023.1 release, the **Demographics Summary (rcmain)**screen is enhanced with **County** and **Comment** fields, and the **Area** field has been renamed to **Zone** so as to properly name the data field.

As of the 2023.4 release, the **Related Incident** field has been added so users can quickly associate a demographics record with an incident.

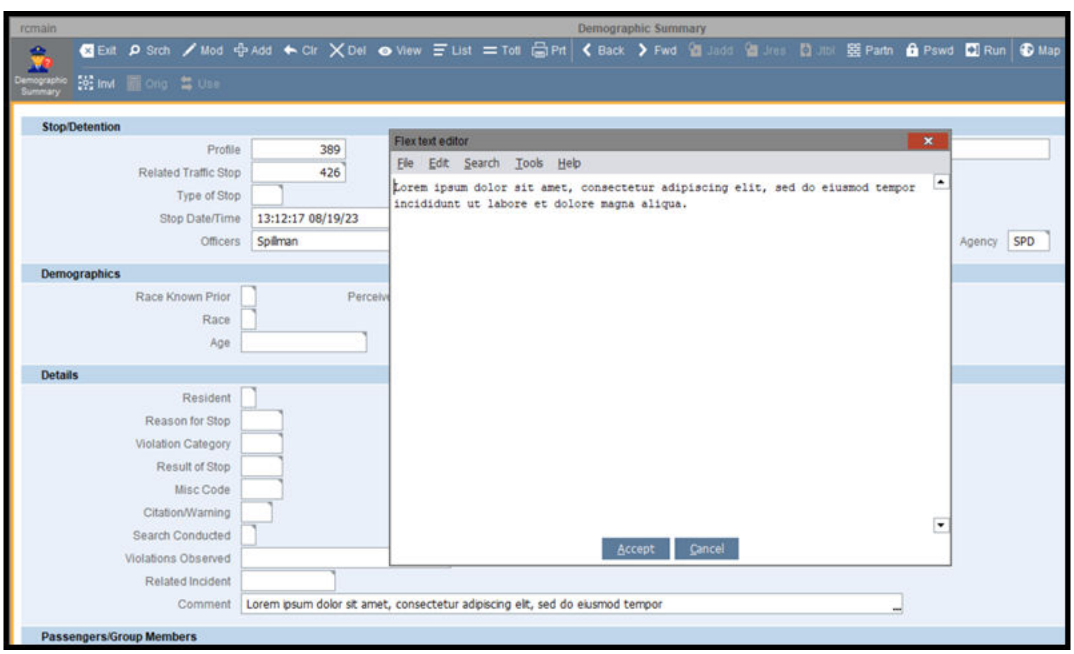
Figure 213: rcmain Screen with Zone, County, Comments, and Related Incident Fields



When an agency has associated counties with cities, and the address is geo-validated, the new **County** field is auto-populated. If the address is not a validated address, or the city is not associated with its respective county, the field is left blank.

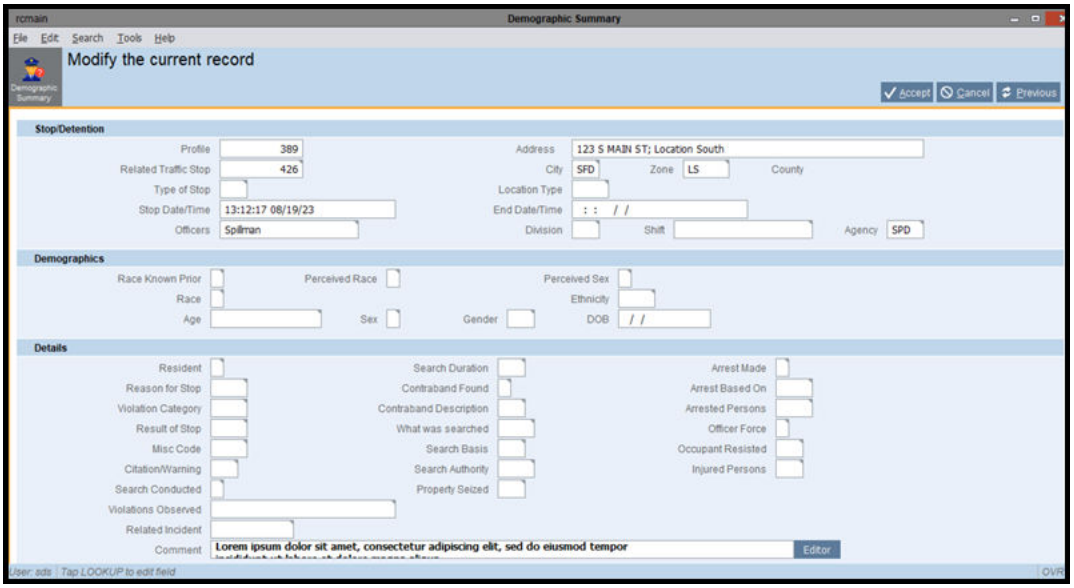
Officers also have the ability to add comments to the stop report in the **Details** section. To add a comment, the officer should click anywhere in the **Comment** field to open the **Flex text editor**. After entering the comment in the editor, they may accept or cancel it.

Figure 214: rcmain Screen with Flex Text Editor Window



After accepting, a short comment or the initial part of a longer one appears in the **Comment** field. To view any longer comment, the user should click the **Editor** tab at the end of the field.

Figure 215: Comment Field with a Piece of Information



8.3.2 Hawaii HIGLS Integration

Hawaii Department of Transportation (HDOT) requires the location of all crashes to be validated against Hawaii Incident Geo-Location Service (HIGLS) database. When creating crash reports, officers are required to validate the Crash Address against the HIGLS database. As of the Flex 2023.1 release, they have this ability.

The feature is fully integrated with the **FR Crash HI** form (STATE OF HAWAII MOTOR VEHICLE ACCIDENT REPORT).

This feature requires the following settings in **admiutil**:

- `Module.FR.Crash.HIGLSValidationURL` – the URL address of the HIGLS service
- `Module.FR.Crash.UseHIGLS` – set to `True`

The both settings can be set at the user level.

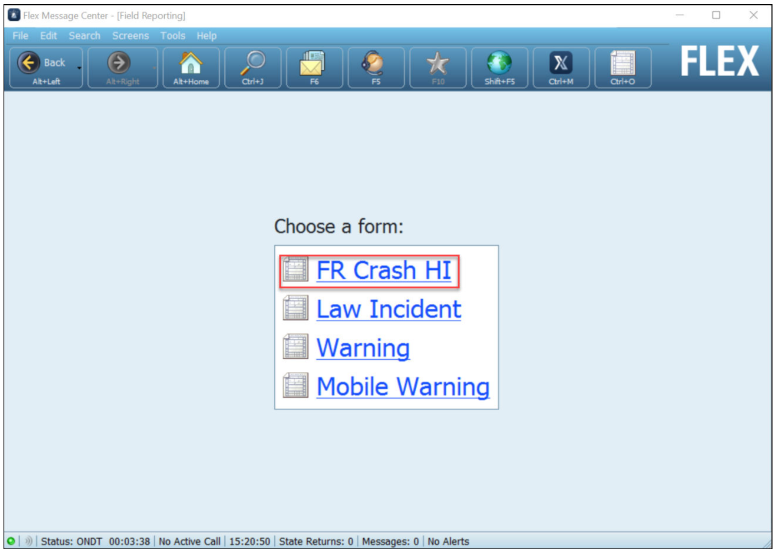
8.3.2.1 Validating a Crash Incident Against HIGLS

With the feature enabled by your admin, as a Hawaii officer you are now able to validate crash incident locations against the HIGLS database.

Procedure:

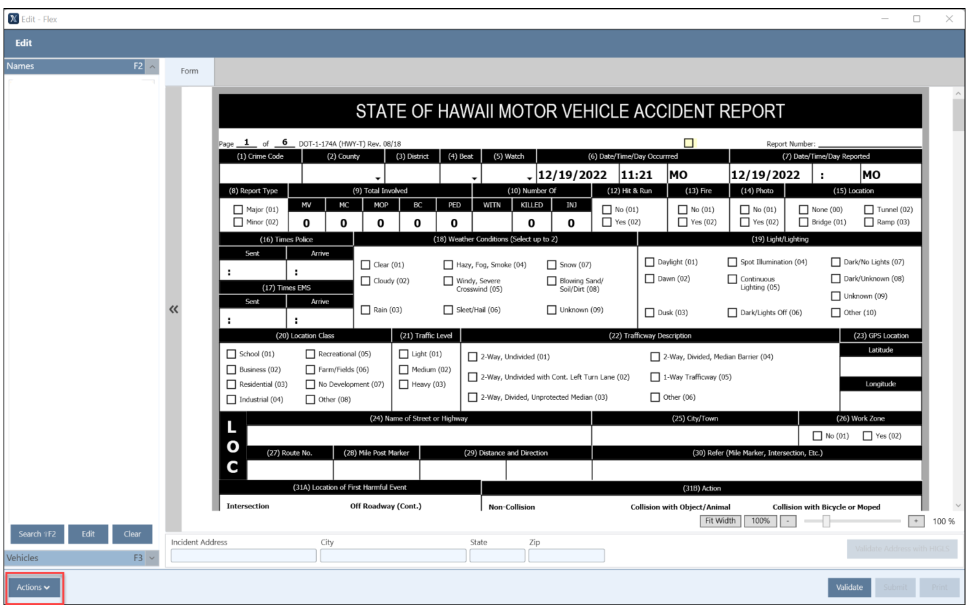
1. From the Flex Message Center select **Field Reports** → **FR Crash HI**.

Figure 216: Field Reporting Screen with FR Crash HI Option



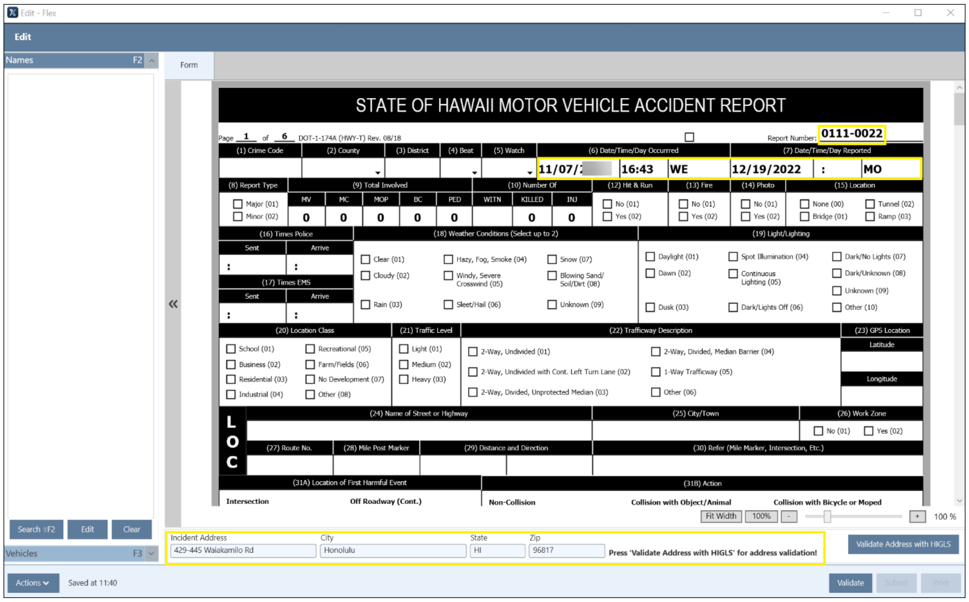
The HI Motor Vehicle Accident Report form appears.

Figure 217: HI Motor Accident Report



2. To import the incident data into the form, select the **Actions** button and from the pop-up menu select the **Import Incident** option.

Figure 218: HI Motor Accident Report with Imported Data

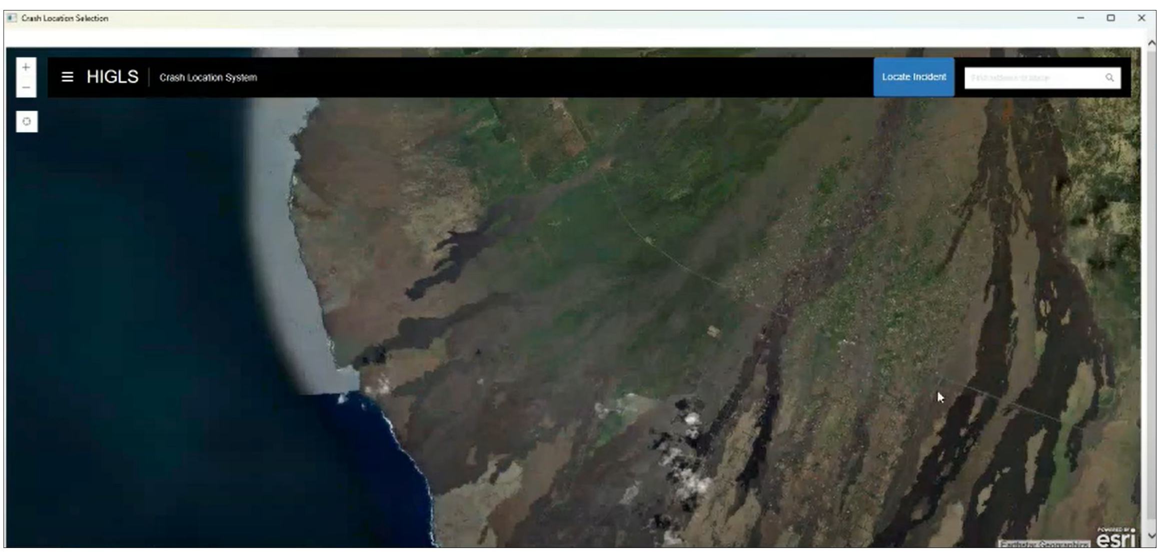


In the example, the imported pieces of data are marked with the yellow frames.

3. Select **Validate address with HIGLS**.

   The **Crash Location Selection** window appears.

   Figure 219: Crash Location Selection Window

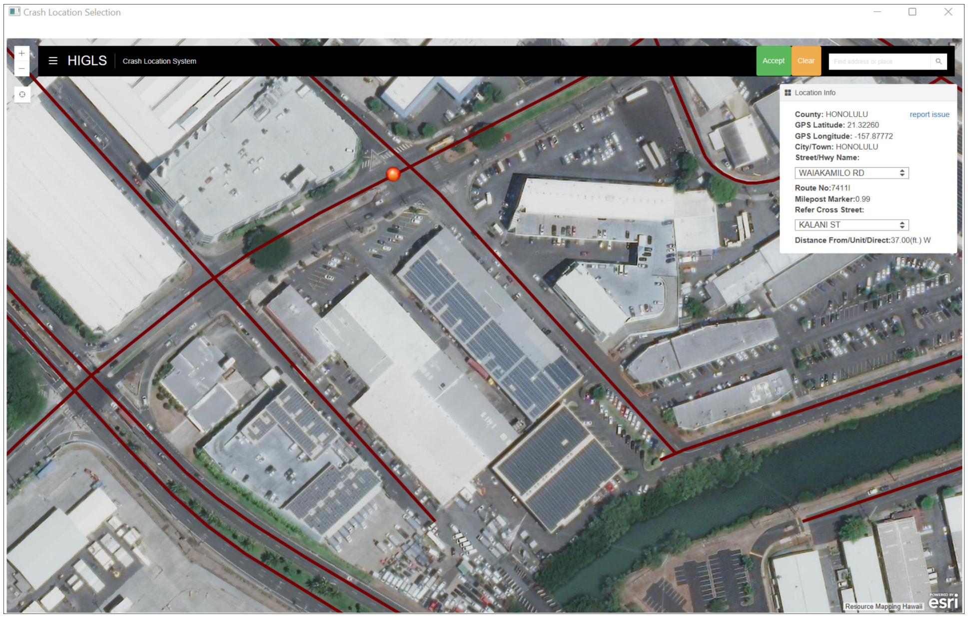


The aim of this figure is to show the **Locate Incident** button used in the next step. In the case of a validated address in Hawaii, the window opens directly on that location.

4. Click the **Locate Incident** button and select the place of the crash.

   Once location is performed, a confirmation window appears.

Figure 220: Location Confirmation Window

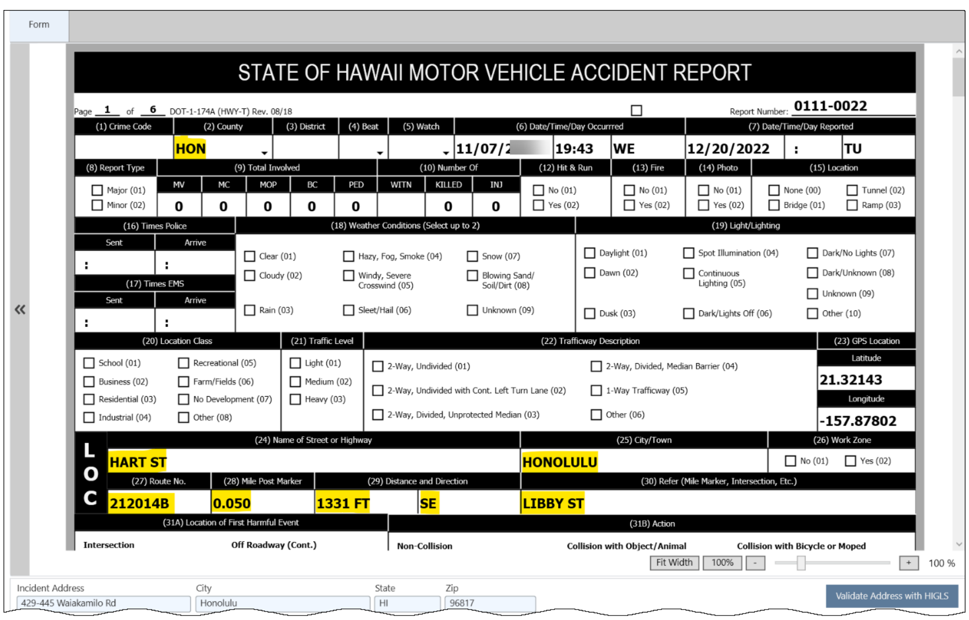


The right upper part of the window contains **Location Info** dialog box. In the box, you are able to correct street names.

5. To confirm the location, click the green **Accept** button.

   Fields from the **Location Info** dialog box are transferred to the HI Motor Vehicle Accident Report form.

   Figure 221: HI Motor Accident Report with Imported Data and Confirmed Location

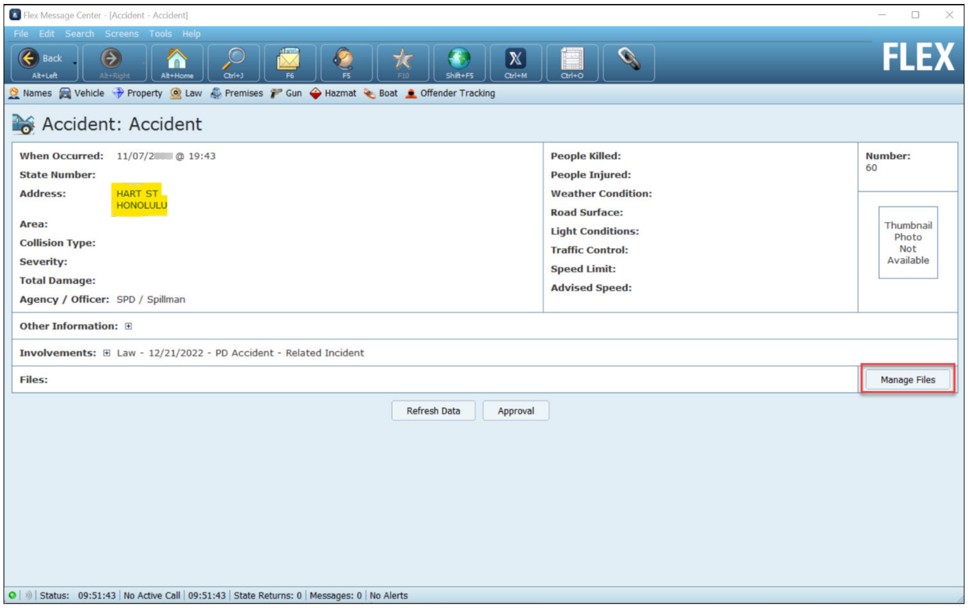


In the figure, the transferred pieces of the location information are highlighted. The **Latitude** and **Longitude** fields are filled with the relevant coordinates. The **Submit** button (not contained in the figure, located below the **Validate Address with HIGLS** button) becomes enabled and active.

6. Click the **Submit** button.

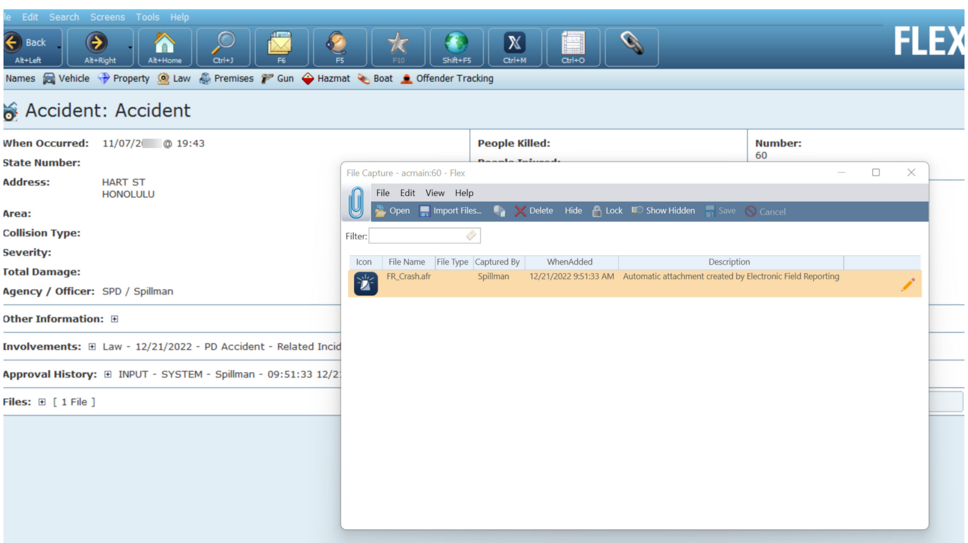
   A new accident is created and displayed in the Message Center.

Figure 222: New Accident in the Message Center



7. To locate the crash form as an attachment ready to be sent, click **Manage Files**.

Figure 223: FR_Crash.afr Attachment



8.4
Jail

8.4.1
Housing Assignment Overrides

Due to the new **nmtbsex** code table, Flex Jail is enhanced to handle situations when an inmate's sex is not Male or Female.

This can be used by jails that have a temporary need to house an inmate with a sex that is not normally allowed in an area without having to have an administrator re-categorize the sex-restrictions for the housing location.

8.4.1.1
Admin: Control of Housing Assignment Override Feature

There is now a new way to prompt users to confirm that they want to move inmates with a sex that is not compliant with the locations sex-restriction. All overrides for movement and housing assignment, including supervisor overrides, are logged.

You can enable this functionality in adminutil:

1. Setting level: **Agency**
   - Setting name: `Module.Jail.Housing.HousingOverrideSexRestrictionsPolicy`
   - Setting Description: Housing sex restrictions overriding policy
   - Drop-down values: `None` (by default), `By_Group`, `All_Users`
2. Setting level: **Group**
   - Setting name: `Module.Jail.Housing.AllowHousingOverrideSexRestrictions`
   - Setting Description: Allows to override Jail Location sex restrictions for Movement and Assign Housing
   - Values: `False` (by default), `True`

Any overrides are logged in sylog, and can be found by clicking the **Additional Info** tab and searching for `*** Housing Assignment Override Information Start ***`

You can find the following information:

- A string of text stating that sex restrictions were overridden
- The sex restrictions of the location the inmate was moved to
- The user who overrode the sex restrictions
- The date and time the user overrode the sex restrictions

8.4.1.2
Housing Assignment Override Feature

If your admin allows you to override housing assignments of inmates with a sex that is not compliant with a locations sex-restriction, you should use the information below.

When you view an inmate in the **Assign Housing** screen and their sex set to **Unknown**, you see that there are limited locations to where you can move the inmate in the **Housing** area. You can display all housing locations in the **Housing** tree menu by selecting the **Show All Housing Locations** check box.

When hovering over this check box, you see a message similar to the following:

`Ignore location Sex Restrictions for non-male and non-female inmates`

If you attempt to move an inmate with the sex of **Unknown** to male or female assigned housing, the **Facility management operation warnings** window appears, alerting you that the location selected does not align with the sex of your selected inmate. You can override this window by selecting the **Override** check box next to inmate you are moving and clicking **Assign**. The **Override Housing Restriction Confirmation** window appears. You can confirm that you want to move your inmate to the desired housing location by clicking **Override**.

Additionally, you can see if the sex-based movement restrictions were overridden at time of movement in the **Housing** tab on the **Inmate** screen. If movement was overridden, a grayed-out **Overridden** check box appears in the **Movement** screen.

You can see if any movement restrictions were overridden at the time of movement by reviewing the last log entry the **Log** tab on the **Inmate** screen. If the movement was overridden, a string of text appears in the **Additional Info** tab, stating the following information:

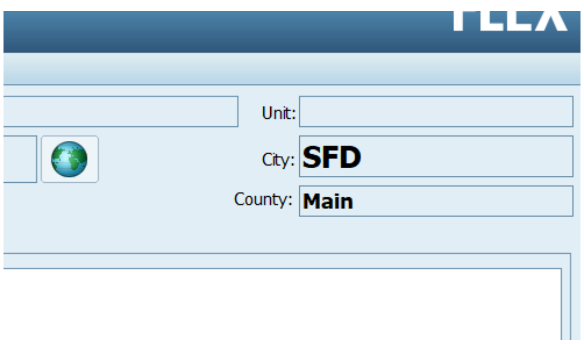
- A string of text stating that sex restrictions were overridden
- The sex restrictions of the location the inmate was moved to
- The user who overrode the sex restrictions
- The date and time the user overrode the sex restrictions

8.5 Mobile

8.5.1 Ability to View the County in Which an Incident Occurs

Depending on your agency settings, for Flex 2023.1 and newer, you can now see the county that a call is located in. The **County** field is displayed by default in the **Mobile CAD Incident** screen underneath the **City** field, and **New Call Record** window.

Figure 224: Mobile CAD Incident View of the County Field



If your agency does not have this feature configured, then the **County** field appears blank.

Figure 225: Mobile CAD Incident View of the Empty County Field

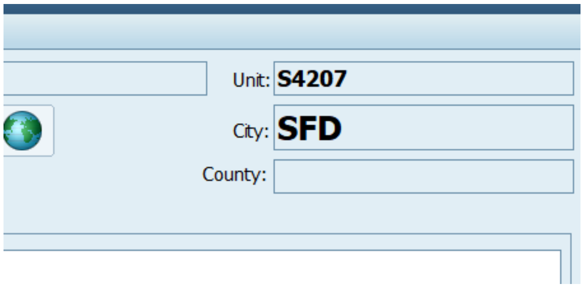
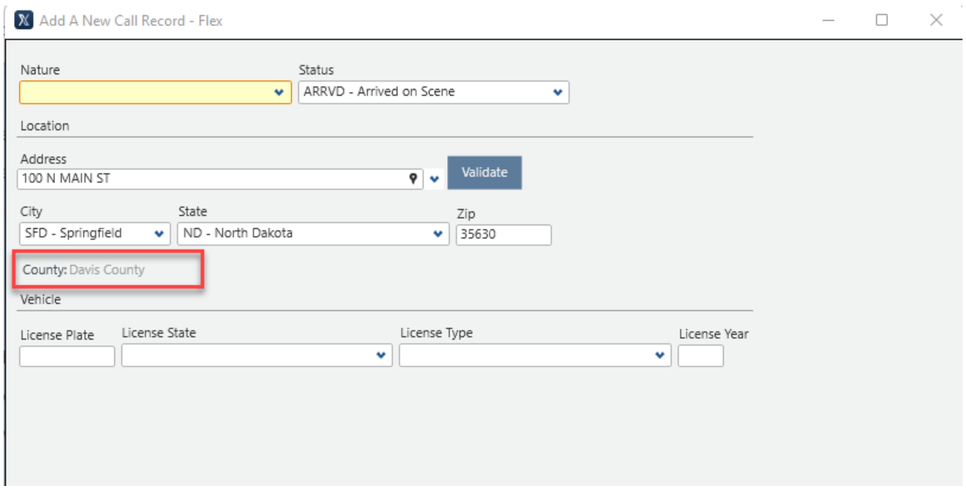


Figure 226: New Call Record Window View of the County Field



8.5.1.1

Admin: Enabling County Column in Mobile CAD

By default, on the Mobile CAD screen the `County` column is not displayed. If you have linked city names to appropriate counties and want the counties to be displayed in Mobile CAD, you must enable that column. If you need information on how to link city names to appropriate counties, see the *Flex CAD Administrator Manual*.

Procedure:

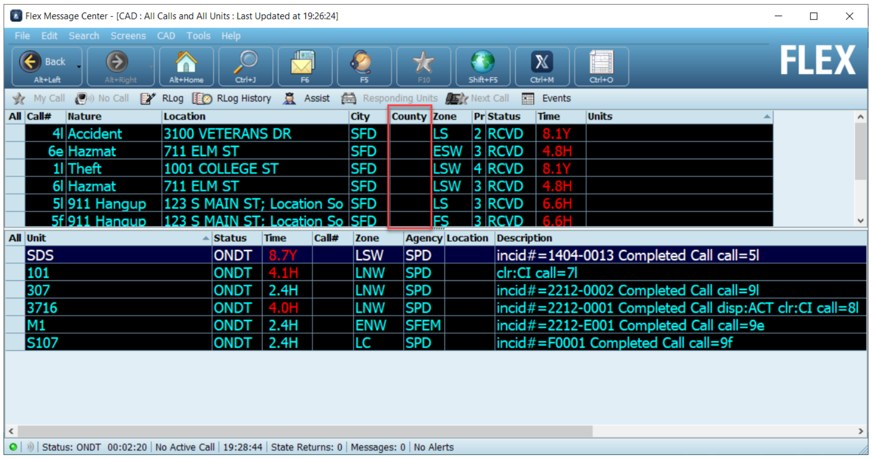
1. At the command line, enter `adminutil`
2. From the tree menu, expand the **Module** folder and click the **Module.Mobile** folder.
3. In the settings window on the right, locate the `ShowCountyColumnInCAD` setting and double-click it.

   The **Enter True/False Value** dialog box opens, with the `False` default value of the `ShowCountyColumnInCAD` setting. By default, the setting is locked at `Agency`.
4. Set the **Value** to `True` and click **OK**.
5. Close the **Administration Manager >> Settings Editor** window.
6. Restart the Flex Mobile client.

   The **Mobile CAD** screen contains the `County` column.

   NOTE: This does not require any Mobile sydaemons or services to be restarted, just the individual Flex Mobile/Message Center clients. When this is first activated, users already logged in will not be affected and will see the change upon their next logon.

Figure 227: Mobile CAD Screen with County Column



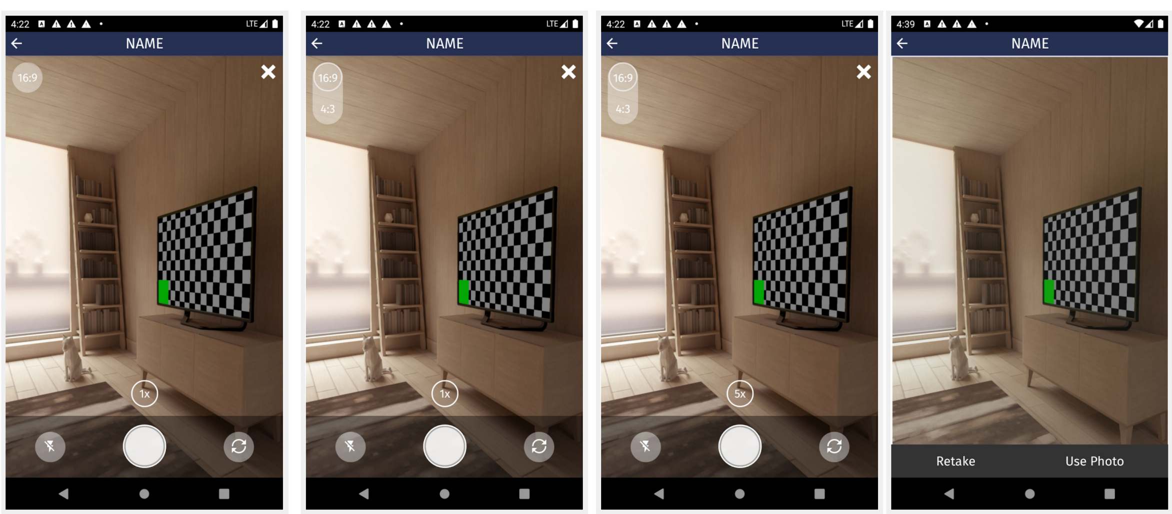
8.6
Touch

8.6.1
Ability for Touch Users to Edit Attachments

If you use an Android or iOS device, you can take photos within the application and attach them to Name, Vehicle, Property and other databases. Before, such a possibility was previously implemented only on iOS devices.

After taking a photo, you can retake it with the same settings, as in the following figure, see the last screen on the right.

Figure 228: Photographic Options of Android Devices in the Touch Application



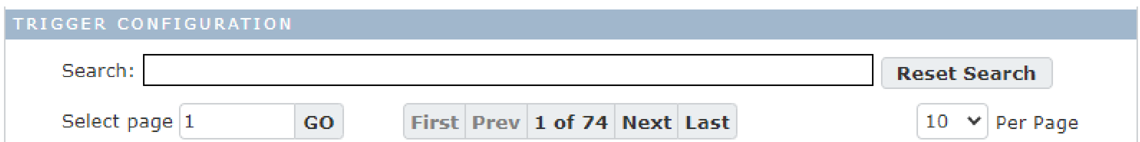
8.7
Rapid Notification

8.7.1
Trigger Configuration Search Features

When configuring your trigger settings for ASTRO, Rapid Notification 2.0, or VESTA, you now have the ability to search through your triggers.

The following fields are now added to ASTRO, Rapid Notification, and VESTA trigger configuration settings:

Figure 229: Trigger Configuration Search Features



The following table lists trigger configuration fields.

Table 40: Trigger Configuration Fields

Field	Description
Unit Status	In this field, select the status you want to monitor.
Search	In this search field, search a specific term or phrase across all of the following fields: • **Unit Status** • **Nature** • **Zone** • **Recipient Group** • **Action**
Reset Search	To delete the text entered into the **Search** field and reset the search, click this button.
Select Page	In this field you can enter the number of the page listed that you want to navigate to. For example, if you have 74 pages of results, you can navigate to the sixth page by entering `6` and clicking **GO**. **Figure 230: Trigger Configuration Fields Detail.** 
GO button	To go to the page number entered in the **Select Page** field, click this button.
First button	To go to the first page of results, click this button.
Prev button	To go to the previous page of results, click this button.
Next button	To go to the next page of results, click this button.
Last button	To go to the last page of results, click this button.

Field	Description
Per Page drop down menu	To select how many results you want displayed at once, click this drop down menu and select one of the following options: • 10 • 50 • 100

These search functions are also available in different ways for the following delivery methods: Broadcast Group, Pre-Alerts, Rapid Notification, Runtime, Station Alerting, VESTA.

Chapter 9

Release 2022.4

This chapter presents changes made to Flex for the 2022.4 release.

9.1 CAD

9.1.1 Ability to Link City Names to Counties

Dispatch centers that cover multiple counties might have the same city names in two or more of them. As of the 2022.4 release, they can validate addresses along with the county where a city (or its part) is located.

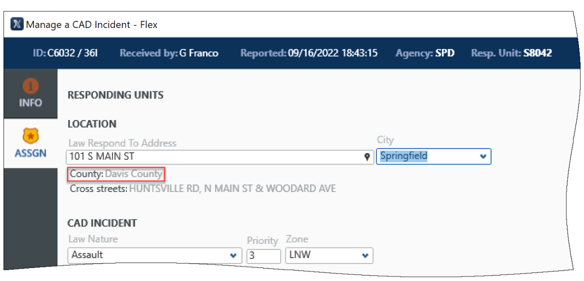
Administrators can now link each city name to the correct county, so that users will not select cities in wrong counties. For this purpose, a new `apcounty` table is added to Flex. See Admin: Linking City Names to Appropriate Counties on page 229.

Then, dispatchers who enter calls for service throughout all of the jurisdictions can ensure that they send units to the correct addresses. See:

- Adding the County Column to the GeoValidation Address Selection Window on page 232.
- Adding the County Column to Undispatched Calls and Dispatched Calls Windows on page 233

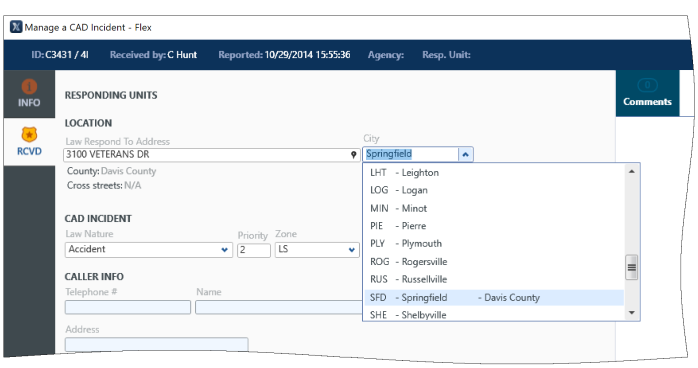
The Manage a CAD Incident screen can now include the **County** field.

Figure 231: County Field on the CAD Incident Screen



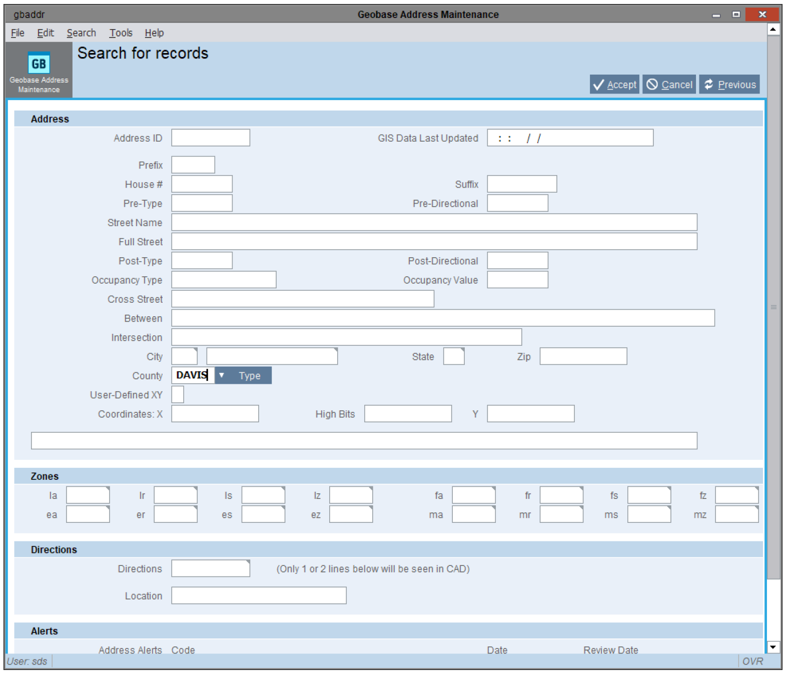
In the **City** drop-down list, the city linked to its county appears together with the name of that county. In the case of two or more cities with the same name, it allows dispatchers to select the right one.

Figure 232: County Information in the City Drop-down on the CAD Incident Screen



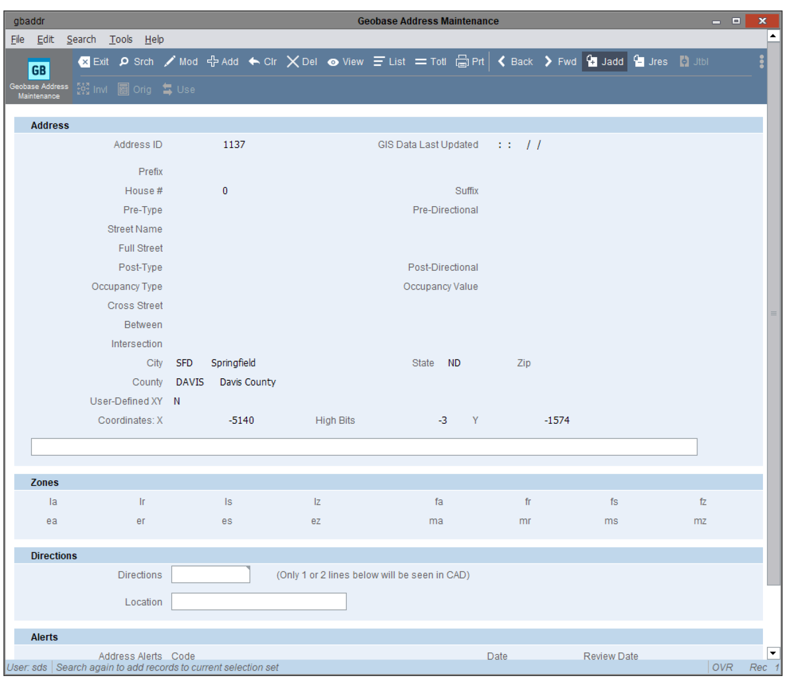
The Geobase Address Maintenance screen (`gbaddr` table) now also contains the **County** field. The search for records may include searching by a county code.

Figure 233: Search for Records by County Code



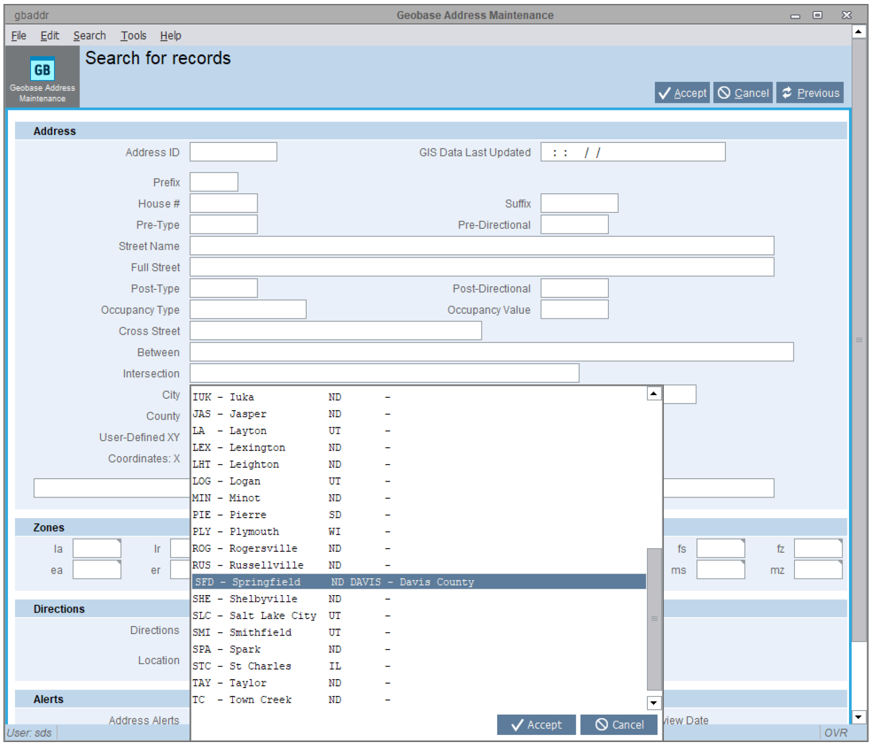
Without additional data, the search results for an entered county code include the full name of the county, and the code and full name of the city linked to that county.

Figure 234: Search Results for a County Code



To select the city associated with the right county, the user can search for it from the Geobase Address Maintenance screen by expanding the **City** drop-down. For each city associated with its county, the additional information will include the county code and full name of the county. In the following example, the drop-down shows the Springfield city linked to Davies County.

Figure 235: County Information in the City Drop-down



9.1.1.1 Admin: Linking City Names to Appropriate Counties

As an administrator in a large agency that covers multiple counties where some city names are identical, you should link those city names to the appropriate counties so users can easily distinguish and select the correct addresses. The feature is available beginning with the 2022.4 release.

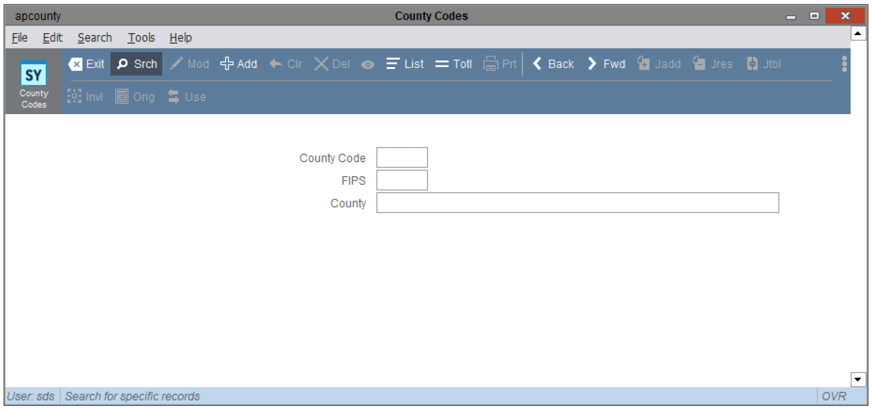
Prerequisites: Check which counties within your agency's jurisdiction include cities with the same or very similar names, or cities with areas located in different counties. These counties should be added to the **County Codes** table first, and then associated with those cities.

Procedure:

1. At the command line, enter `apcounty`

   The new **County Codes** table appears.

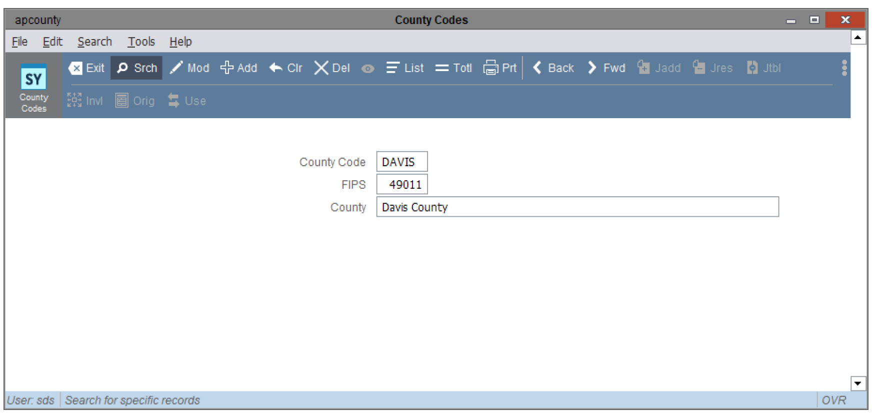
Figure 236: County Codes Table



2. For each relevant county, in the County Codes table (`apcounty`) click **+ Add**, enter a **County Code**, and the **County** name. Click **Accept**.

   The entry in the **County Code** field is of your choice, but is limited to five characters. The entry in the **FIPS** field (FIPS code of the county) is optional.

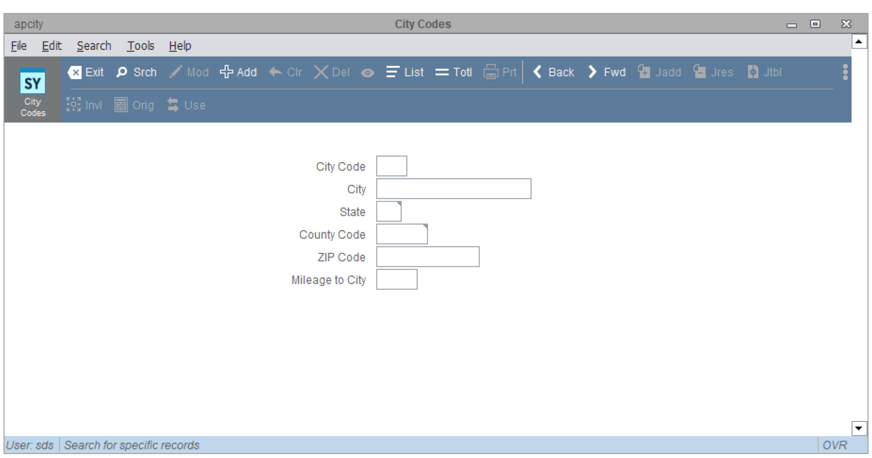
   Figure 237: County Data Example



3. At the command line, enter `apcity`

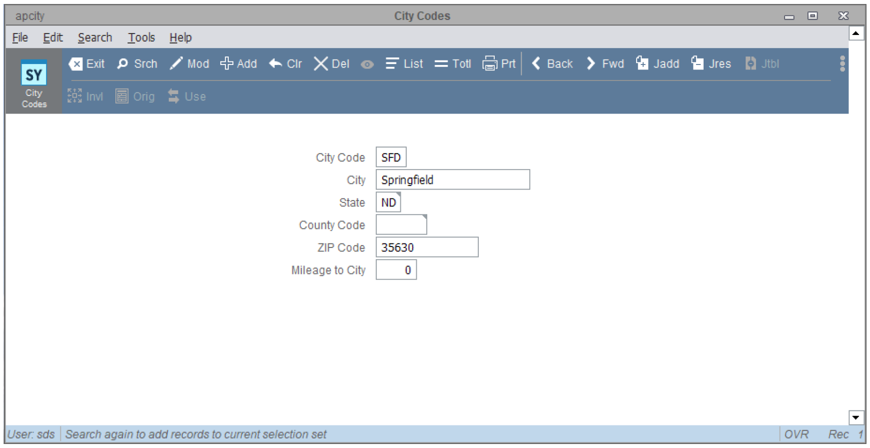
   The **City Codes** table appears. Note that the **City Codes** table has a new field: **County Code**.

   Figure 238: City Codes Table with County Code Field



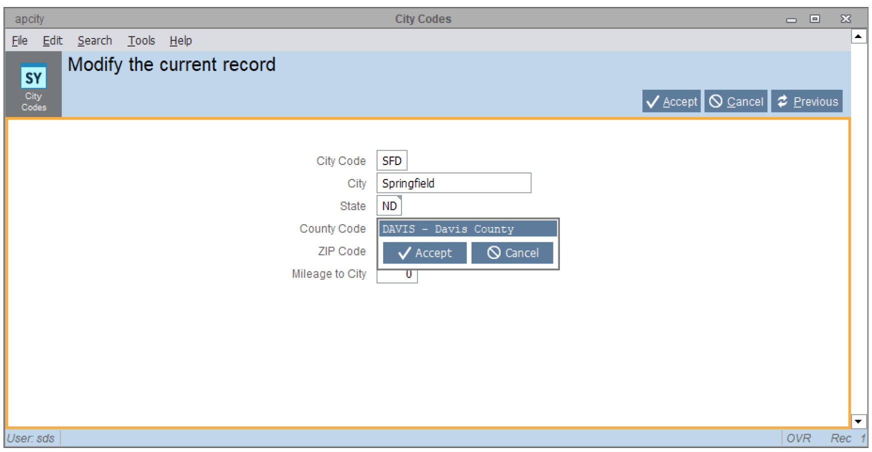
4. In the **City Codes** table, search for a city you want to link to the appropriate county.

Figure 239: Search Result Example in the City Codes Table



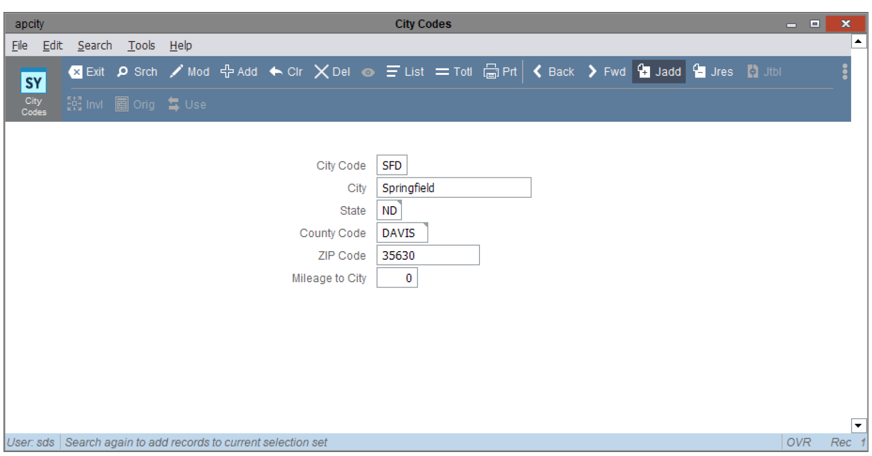
5. In the **City Codes** table, select and accept the right **County Code**.

Figure 240: City Codes Table – Choice of the County Code



6. In the window header, click **Accept**.

Figure 241: City with the County Code Assigned



The city is associated with its county.

Postrequisites: Repeat the procedure for all cities that you want to associate with their counties.

9.1.1.2
Adding the County Column to the GeoValidation Address Selection Window

As of the Flex 2022.4 release, the customization of columns of the **GeoValidation Address Selection** window also includes the ability to add the new **County** column. The column facilitates the validation of addresses, especially when some city names are identical in several counties within your jurisdiction. This column is **not** displayed by default, and must be added to include county information into the **GeoValidation Address Selection** window.

Prerequisites: Ask your admin if city names have been associated with their respective counties.

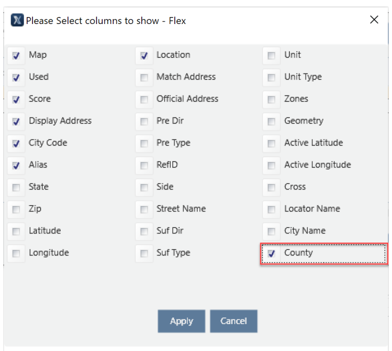
Procedure:

1. At the command line, enter `addr`
2. In the **Address Information** window, in the **Address** field, enter any address.

   The **GeoValidation Address Selection** window appears.
3. In the **GeoValidation Address Selection** window, hover your mouse cursor over the existing column names and right-click there.

   The **Please Select columns to show** pop-up window appears.

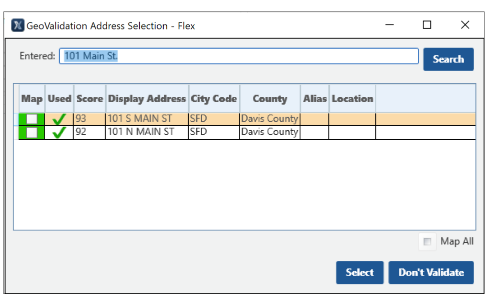
   Figure 242: Please Select columns to show Window

4. Select **County** and click **Apply**.

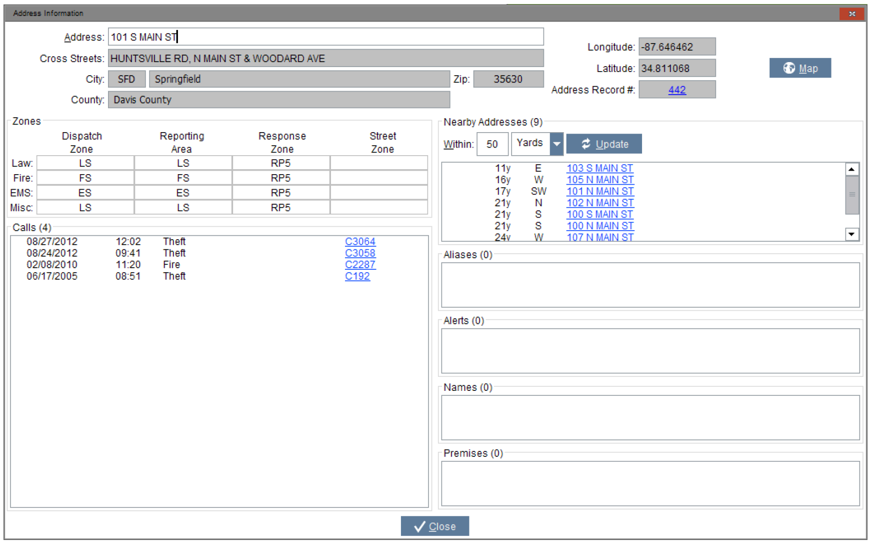
   The new **County** column appears in the **GeoValidation Address Selection** window. You can drag the column name to locate it by the **City Code** (or **City Name**, if selected for displaying).

   Figure 243: GeoValidation Address Selection Window with the County Column

   For each valid address in a city linked to its county, the **GeoValidation Address Selection** window will include the county name. When you accept an address in that city, the **Address Information** window shows the county name below the **City** field.

Figure 244: Address Information Including the County Name



9.1.1.3

Adding the County Column to Undispatched Calls and Dispatched Calls Windows

As of the 2022.4 release, you can add the **County** column to **Undispatched Calls** and **Dispatched Calls** windows. Such modification of the CAD status windows is especially useful when your agency covers counties with some identical city names and your admin has associated city names with their respective counties.

The procedure is the same for the both windows, so that it is shown for the **Undispatched Calls** window only. You can follow the same steps in the **Dispatched Calls** window.

Prerequisites: Ask your admin if city names have been associated with their respective counties.

Procedure:

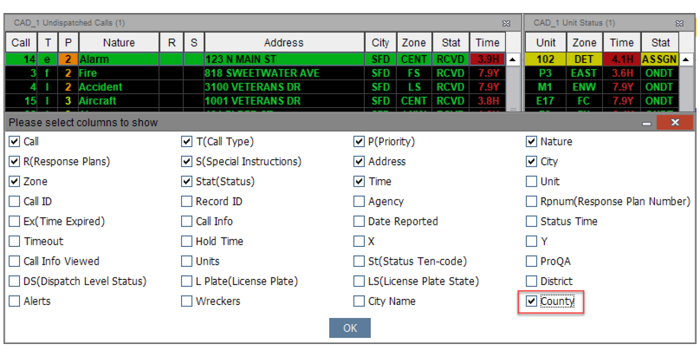
1. Right-click the header of any column in the **Undispatched Calls** window.

   A menu appears.

2. Select **Column Chooser**.

   The **Column Chooser** dialog box appears.

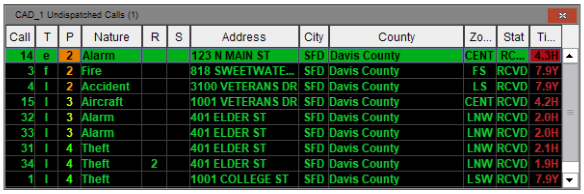
   Figure 245: Column Chooser with the County Option

3. Select the **County** check box.
4. Click **OK** to close the dialog box.

5. Optional: You can move the **County** column to be adjacent to the **City** column.

Figure 246: Undispatched Calls Status Window with the County Column


CAD_1 Undispatched Calls (1)

Call	T	P	Nature	R	S	Address	City	County	Zo...	Stat	Ti...
14	e	2	Alarm			123 N MAIN ST	SFD	Davis County	CENT	RC...	4.3H
3	f	2	Fire			818 SWEETWATE...	SFD	Davis County	FS	RCVD	7.9Y
4	l	2	Accident			3100 VETERANS DR	SFD	Davis County	LS	RCVD	7.9Y
15	l	3	Aircraft			1001 VETERANS DR	SFD	Davis County	CENT	RCVD	4.2H
32	l	3	Alarm			401 ELDER ST	SFD	Davis County	LNW	RCVD	2.0H
33	l	3	Alarm			401 ELDER ST	SFD	Davis County	LNW	RCVD	2.0H
31	l	4	Theft			401 ELDER ST	SFD	Davis County	LNW	RCVD	2.1H
34	l	4	Theft	2		401 ELDER ST	SFD	Davis County	LNW	RCVD	1.9H
1	l	4	Theft			1001 COLLEGE ST	SFD	Davis County	LSW	RCVD	7.9Y

9.2
Hub

9.2.1
Admin: Configurable Sex Codes

As of the 2022.4 release, administrators can add options to the list that identifies the sex of a person in a case report or person's record. Dispatchers, officers, record clerks, and correction officers can work from a common set of sex codes that are compliant with state and local laws.

A newly configurable code table **nmtbsex** can be accessed through the Administration Manager or the command line by entering `nmtbsex`. Administrators can add, remove, and edit sex codes.

NOTE: The default codes Female, Male, Unknown, and Nonbinary cannot be deleted or modified. Only codes that have been added in addition to the four default codes can be changed.

The addition of sex codes does not change existing state name records nor does the change of a sex code in a record affect the historical records. The date and user responsible for the change are recorded.

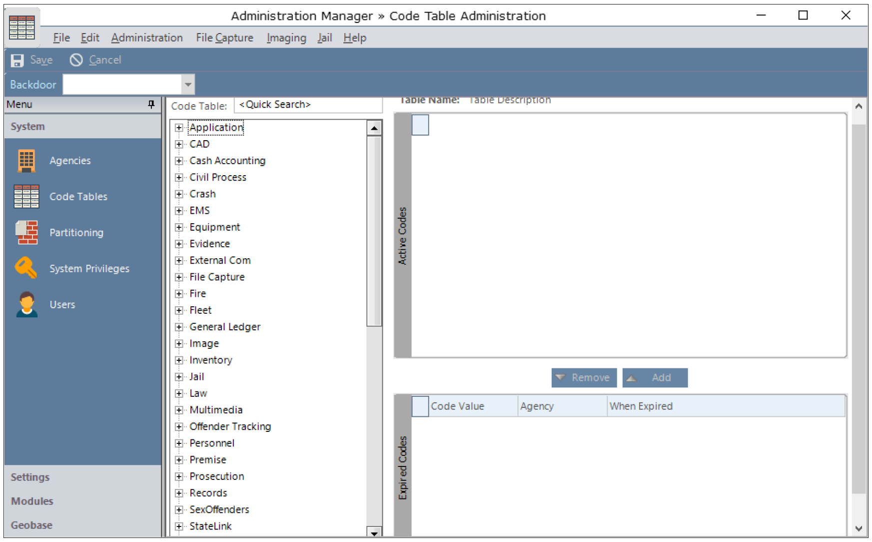
9.2.1.1
Admin: Configuring Sex Code Tables in the Administration Manager

Procedure:

1. From the Administration Manager, click **System** → **Code Tables**.

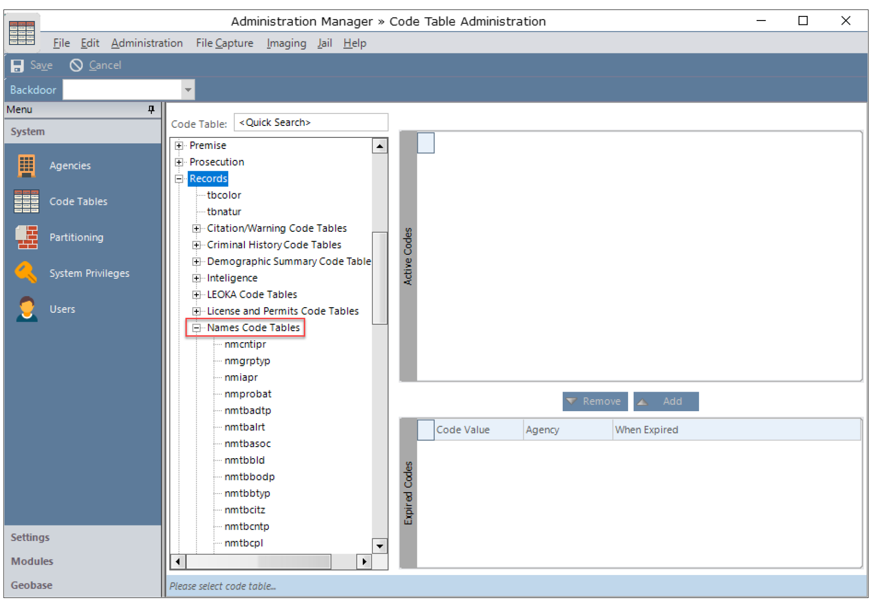
   The **Code Table Administration** screen opens. The code tables are displayed in a tree menu organized by module.

Figure 247: Code Table Administration Screen



2. In the **Code Tables** tree, navigate to **Names Code Tables** → **Records**.

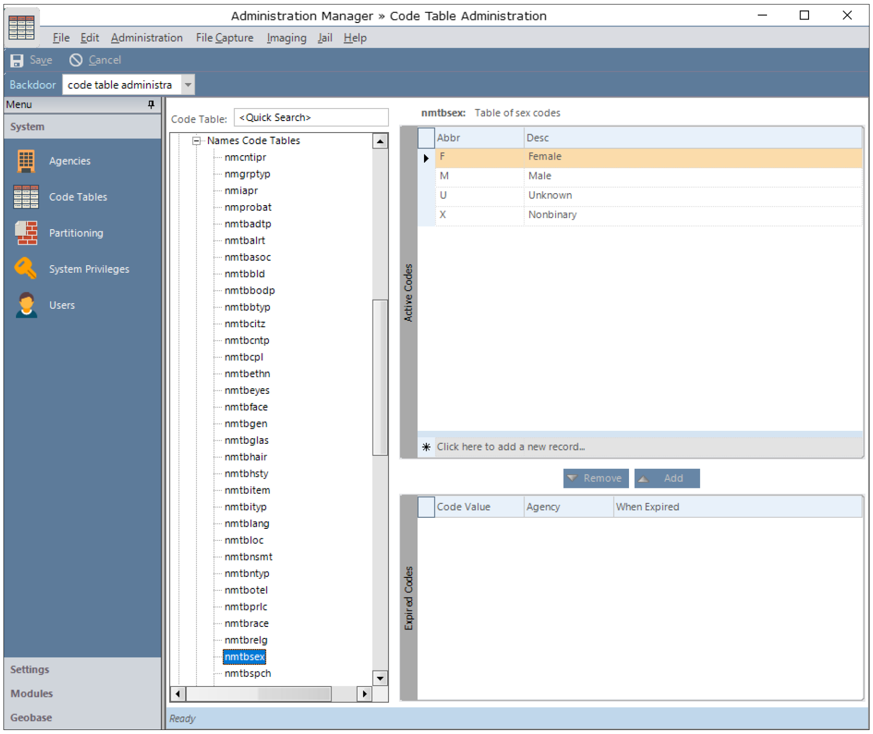
Figure 248: Names Codes Tables



3. In the **Names Code Tables** list, click the **nmtbsex** table.

   The list of current sex codes and their descriptions appear.

Figure 249: Table of Sex Codes (nmtbsex)



4. In the **Active Codes** table, click **Click here to add a new record**.
5. In the active **Abbr** and **Desc** fields, enter the sex code (single letter or digit) and its description.
6. Press CTRL+S to save the record.
7. If you want to edit the code, click the code, enter your changes, and press CTRL+S.
8. If you want to remove the code, select the code, click **Remove**, and press CTRL+S.

   The removed record appears in the **Expired Codes** table.

9.2.1.2

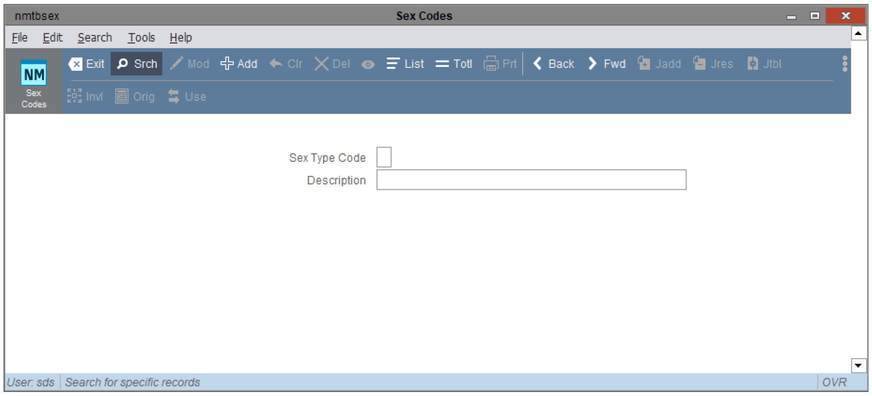
Admin: Configuring Sex Codes from the Command Line

Procedure:

1. At the command line, enter `nmtbsex`

   The **Sex Codes** table window opens.

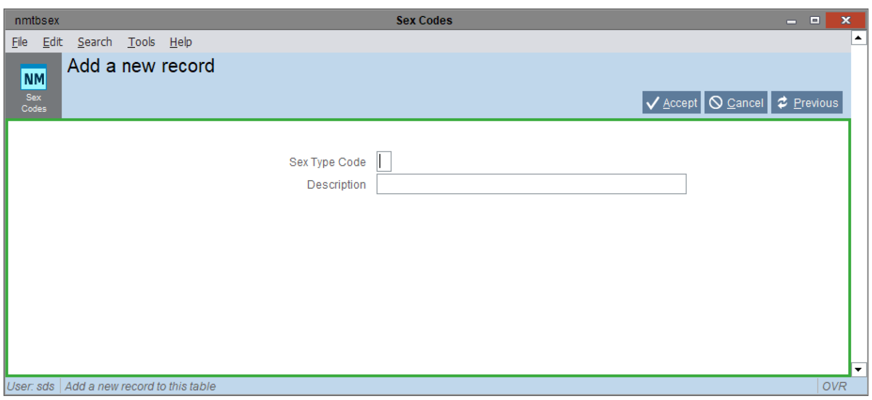
Figure 250: Sex Codes Table Window



2. Click **Add**.

   The **Add a new record** view opens.

   Figure 251: Add a New Record View



3. In the **Sex Type Code** box, enter the new sex code.
4. In the **Description** box, enter a description of the new code.
5. Click **Accept**.

9.3

Records

9.3.1

Access to WatchGuard Recordings and to Digital Evidence in a Folder Structure

Flex users are now able to access and open WatchGuard content uploaded to CommandCentral Evidence. They can do the same with other files loaded to CommandCentral Records, including digital evidence in a folder structure. This new feature is available for Flex customers who host the Flex server with the latest

2022.1 and any newer version. For shared agencies on a host server, the feature is available beginning with the 2022.4 release.

WatchGuard recordings that are uploaded from devices to CommandCentral Evidence, and other files loaded to CommandCentral Records, can be listed in Flex in the incident **File Capture** window. Any digital evidence should be tagged with the related Flex law Incident Number. The window can be opened from the toolbar of the Law Incident Table (`lwmain` record) by selecting **Files**. From the **File Capture** window, Flex users can select any of the folders or files to view the content on the CommandCentral Evidence page in a browser.

NOTE:

- Each relevant folder/file in CommandCentral should be associated with Flex by assigning its **Incident ID** as the Flex **Incident Number**.
- Users must be logged in to CommandCentral, otherwise they are prompted to log in.

9.3.2
Admin: Sex Codes

Admin: Sex Codes

The following code table contains the code used for booking and inmate management screens. This code table is contained in the **Records** group, under the **Names Code Tables** group.

Table 41: Sex Code Table

Code Table	Description
nmtbsex	The Sex code table contains the codes used in the **Circumstances** tab in the **Arrest** screen. The four default options are **Female**, **Male**, **Unknown**, and **Nonbinary**. You can add more sex code options that users can select from.

For more information about how admin can configure the new sex code table, see Admin: Configuring Sex Code Tables in the Administration Manager on page 234 or Admin: Configuring Sex Codes from the Command Line on page 236.

9.4
Evidence Management

9.4.1
Ability to Download Evidence Management Application from the Google Play Store

We are now enabling the Evidence Management Android app to be downloaded from the Google Play Store!

Please search for "Flex Evidence" in the Google Play store to easily download this app, or manage it through your agency's Mobile Device Management service.

Going forward, all future updates to the Evidence Management app will be provided through the Google Play Store.

9.4.2

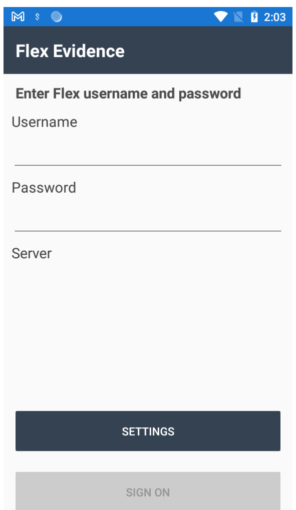
Admin: Setting Up Server Connection Settings in Evidence Management Application

As of the 2022.4 release, entering in the Flex server information in the Flex Evidence Mobile Application has been simplified.

Procedure:

1. Tap the arrow to open the Server section on the homepage of the Evidence Management app.
2. In the **Username** field, enter your username.

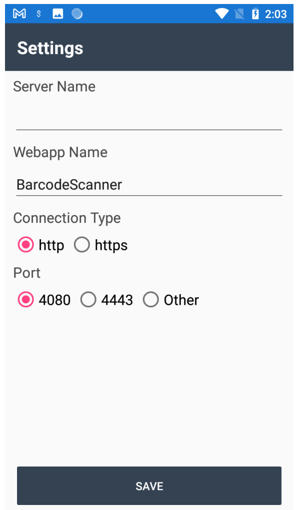
   Figure 252: Flex Evidence Application Server Screen

3. In the **Password**, enter your password.
4. In the **Server** drop-down menu, complete the following fields, and tap **SAVE**:

Table 42: Server Options

Field	Description
Server Name	In this field, enter the Flex host server name. When you enter information into this field, it is formatted into an final output in the following way: ***<Connection Type><Server Name><Port><Webapp Name>*** where the application substitutes each variable with the information for each respective field. You will not be able to log in to the application until the Server Name is entered.

Field	Description
	Figure 253: Server Settings 
Webapp Name	The default value is `BarcodeScanner`. Do not change anything in this field unless you have modified the name of the webapp. Webapp Name is required.
Connection Type radio button	Choose between the following two connection types: ● **http** ● **https** If you select **https**, a message similar to the following appears with a link to Motorola instructions on importing certificates to Flex: `Instruction on importing certificate`
Port radio button	Choose one the following port types: ● **4080** ● **4443** ● **Other** Port value is required if Port type is Other.

5. To sign on to the Evidence Management app in the barcode scanner, tap **Sign On**.

9.5 Jail

9.5.1 Ability to Download Jail Barcode Scanning Application from the Google Play Store

We are now enabling the Jail Barcode Scanning Android app to be downloaded from the Google Play Store!

Please search for "Flex Jail" in the Google Play store to easily download this app, or manage it through your agency's Mobile Device Management service.

Going forward, all future updates to the Jail Barcode Scanning app will be provided through the Google Play Store.

9.5.2 Admin: Sex Codes

Admin: Sex Codes

The following code table contains the code used for booking and inmate management screens. This code table is contained in the **Records** group, under the **Names Code Tables** group.

Table 43: Sex Code Table

Code Table	Description
nmtbsex	The Sex code table contains the codes used in the **Circumstances** tab in the **Arrest** screen. The four default options are **Female**, **Male**, **Unknown**, and **Nonbinary**. You can add more sex code options that users can select from.

For more information about how admin can configure the new sex code table, see Admin: Configuring Sex Code Tables in the Administration Manager on page 234 or Admin: Configuring Sex Codes from the Command Line on page 236.

9.5.3 Admin: Addition of OffensesUseParentPermissions

A new setting, OffensesUseParentPermissions, has been added. This setting prevents users from modifying the offenses of an arrest or booking record without the Modify privilege to the booking record.

You can turn on this setting by setting **Module.Jail.Offense.OffensesUseParentPermissions** to **True**.

The Flex system checks if users have Modify permission to the Booking table/record. If a user has permission to the parent booking record, then the user is also allowed to modify the offense records of the booking record. However, the ability is based on the user's permission to the booking/arrest table, not to the offense.

This setting is turned off by default. This change applies to versions 2022.2 and newer.

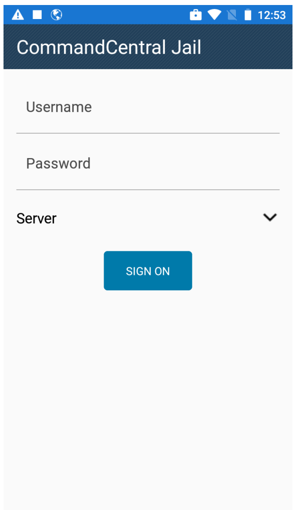
9.5.4

Admin: Setting Up Server Connection Settings in Jail Android Application

Procedure:

1. Tap the arrow to open the Server section on the homepage of the Jail app.
2. In the **Username** field, enter your username.

   Figure 254: Jail Android Application Server Screen

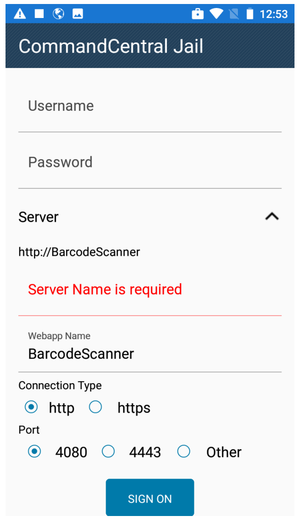
   

3. In the **Password**, enter your password.
4. In the **Server** drop-down menu, complete the following fields, and tap **SAVE**:

Table 44: Server Options

Field	Description
Server Name	In this field, enter the Flex host server name. When you enter information into this field, it is formatted into an final output in the following way: ***<Connection Type><Server Name><Port><Webapp Name>*** where the application substitutes each variable with the information for each respective field. You will not be able to log in to the application until the Server Name is entered. If there is no information in this field, a message similar to the following will appear in red: `Server Name is required.`

Figure 255: Server Name Needed



Field	Description
Webapp Name	The default value is `BarcodeScanner`. Do not change anything in this field unless you have modified the name of the webapp. Webapp Name is required.
Connection Type radio button	Choose between the following two connection types: ● **http** ● **https** If you select **https**, a message similar to the following appears with a link to Motorola instructions on importing certificates to Flex: `Instruction on importing certificate`
Port radio button	Choose one the following port types: ● **4080** ● **4443** ● **Other** Port value is required if Port type is Other.

5. To sign on to the Jail app in the barcode scanner, tap **Sign On**.

9.6
Mobile

9.6.1
Instant Message Carriage Return

The **Instant Message** window now enables a user to type on a new line by pressing Ctrl + Enter.

Previously, pressing Enter would immediately send the Instant Message and there was no way to start typing on a new line.

9.6.2

Report a Problem Tool

You can now use the client log submission tool which is designed to collect, compress, and upload all Flex-related client logs to the server upon user request through the **Report a Problem** link.

The Report a Problem tool is intended to collect all necessary information to diagnose an issue as soon as possible after the issue happened, to reduce the risk of information loss in the case that an administrator is not available to log in and collect logs in a timely manner. The resulting zip file is stored on the server for later retrieval.

NOTE: Reporting a problem from Mobile will collect all Flex logs, not just logs relating to Mobile.

9.6.2.1

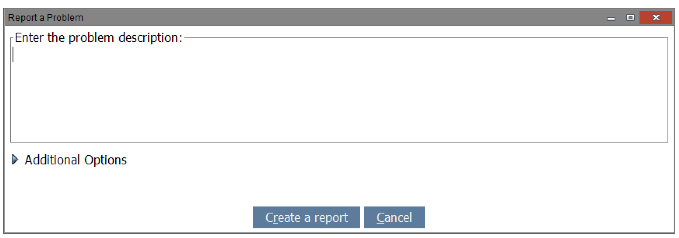
Using the Report a Problem Tool

Procedure:

1. From the Flex Mobile **Help** menu, select **Report a Problem**.

   The **Report a Problem** window appears.

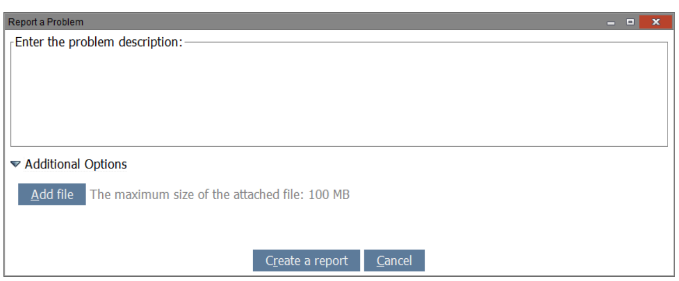
   Figure 256: Report a Problem Window

2. Enter a description of the problem to explain the context of the issue reported.

   Be as specific as you can about what you encountered, including information about what you were doing when the error occurred and about all its symptoms and displayed messages.
3. Optional: To add a file to the problem report, click the **Additional Options** toggle arrow.

   Figure 257: Report a Problem Window with Add File Option

   As the tool automatically uploads log files, this additional option is meant to upload other files such as screenshots, which can be helpful in showing the issue from the user perspective and give the administrator and support personnel more information about the issue being reported.

4. Once you are ready to submit the report, click the **Create a report** button.

The Flex software uploads the files in a `.zip` file, which is saved to `$SPILLMANDIR/reports/{username}/{username}-{date}.zip`

$SPILLMANDIR generally evaluates to `/sds/app/client` on Linux systems and `SpillmanServer\app\client` on Windows systems.

The following logs are collected as part of the operation of this tool:

```
%localappdata%\Spillman\Spillman\{App Version}\Logs\*
%localappdata%\Spillman\CommandCentral Jail\{App Version}\Logs\*
%localappdata%\Spillman\Spillman\Launcher.log
%localappdata%\Spillman\Mobile\Mobile.log
C:\ProgramData\MSI\Map\Logs\*
```

NOTE:

- `{App Version}` is replaced with the actual application version number in the file paths.
- Where asterisks are included in the file path, all logs contained within that directory are included.
- This tool does not configure log levels or turn logs on. It only collects what is in these locations. Log configuration must be done according the specifications of each product.

9.6.3
Admin: Client Logs Retrieval

You can now retrieve client logs from the server to better understand users' problems.

9.6.3.1
Retrieving Client Logs from the Server

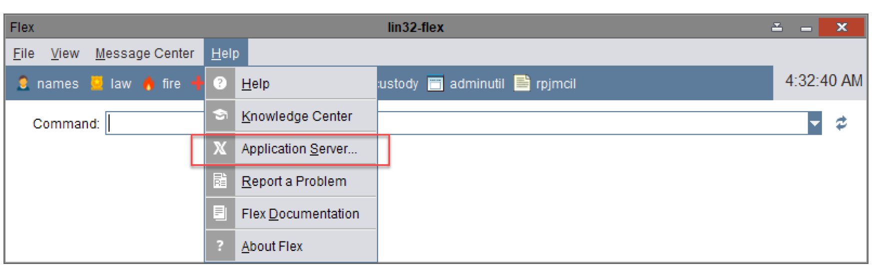
The logs submitted by the Report a Problem tool can either be manually transferred from the server, or retrieved from the Log File Viewer in the Spillman web app by performing the following actions.

Procedure:

1. To navigate to the web app administration page from the Flex **Help** menu, click the **Application Server...** link.

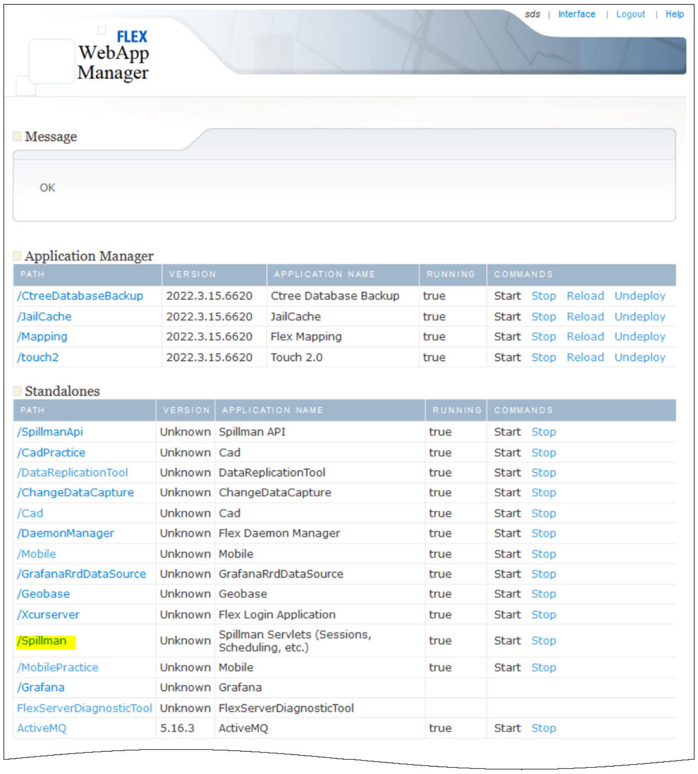
   NOTE: You must be an admin to log into the Application Server.

   Figure 258: Application Server Link

2. On the FLEX WebApp Manager page, click the **/Spillman** link.

Figure 259: FLEX WebApp Manager Page

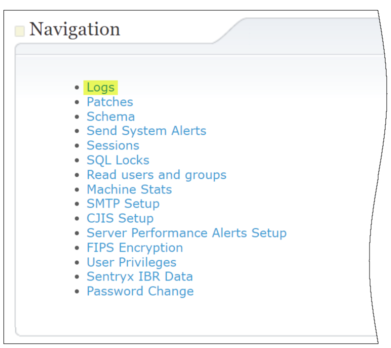


PATH	VERSION	APPLICATION NAME	RUNNING	COMMANDS
/CtreeDatabaseBackup	2022.3.15.6620	Ctree Database Backup	true	Start Stop Reload Undeploy
/JailCache	2022.3.15.6620	JailCache	true	Start Stop Reload Undeploy
/Mapping	2022.3.15.6620	Flex Mapping	true	Start Stop Reload Undeploy
/touch2	2022.3.15.6620	Touch 2.0	true	Start Stop Reload Undeploy

PATH	VERSION	APPLICATION NAME	RUNNING	COMMANDS
/SpillmanApi	Unknown	Spillman API	true	Start Stop
/CadPractice	Unknown	Cad	true	Start Stop
/DataReplicationTool	Unknown	DataReplicationTool	true	Start Stop
/ChangeDataCapture	Unknown	ChangeDataCapture	true	Start Stop
/Cad	Unknown	Cad	true	Start Stop
/DaemonManager	Unknown	Flex Daemon Manager	true	Start Stop
/Mobile	Unknown	Mobile	true	Start Stop
/GrafanaRrdDataSource	Unknown	GrafanaRrdDataSource	true	Start Stop
/Geobase	Unknown	Geobase	true	Start Stop
/Xcurserver	Unknown	Flex Login Application	true	Start Stop
/Spillman	Unknown	Spillman Servlets (Sessions, Scheduling, etc.)	true	Start Stop
/MobilePractice	Unknown	Mobile	true	Start Stop
/Grafana	Unknown	Grafana		
FlexServerDiagnosticTool	Unknown	FlexServerDiagnosticTool		
ActiveMQ	5.16.3	ActiveMQ	true	Start Stop

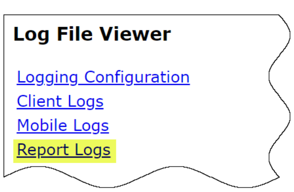
3. On the **Navigation** pane, click the **Logs** link.

Figure 260: Logs Link on the Navigation Pane



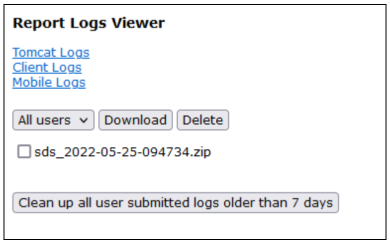
4. On the Log File Viewer page, click **Report Logs**.

Figure 261: Report Logs Link in Log File Viewer



A list of submitted logs appears.

Figure 262: Submitted Logs in the Report Logs Viewer



From this page, you can select and download the report submissions, and delete them, also by using the **Clean up all user submitted logs older than 7 days** option.

9.7

Rapid Notification

New functionality was added to give users more options for how to display the date, time, city, and complainant information in **Mapping** settings.

In the **Output** area for all Runtime message settings, the following new fields are included in the default text:

- `City: {city}`
- `Complainant Name: {contact}`
- `Complainant Phone: {contact_phone}`

For SMTP, long, short, and printer format messages, the following date and time formats have been added as new keys in the **Keys** section of the **Mapping** settings:

- `{current_date_Time (DOW MONTH DAY HH:mm:ss yyyy)}`
- `{current_date_Time (HH:mm:ss MM/dd/yyyy)}`
- `{current_date_Time (MM/dd/yyyy HH:mm:ss)}`
- `{reported (DOW MONTH DAY HH:mm:ss yyyy)}`
- `{reported (HH:mm:ss MM/dd/yyyy)}`
- `{reported (MM/dd/yyyy HH:mm:ss)}`
- `{comments (MM/dd/yyyy HH:mm:ss) }`
- `{comments (HH:mm:ss MM/dd/yyyy)}`
- `{comments (MM/dd/yyyy HH:mm:ss)}`

Chapter 10

Release 2022.3

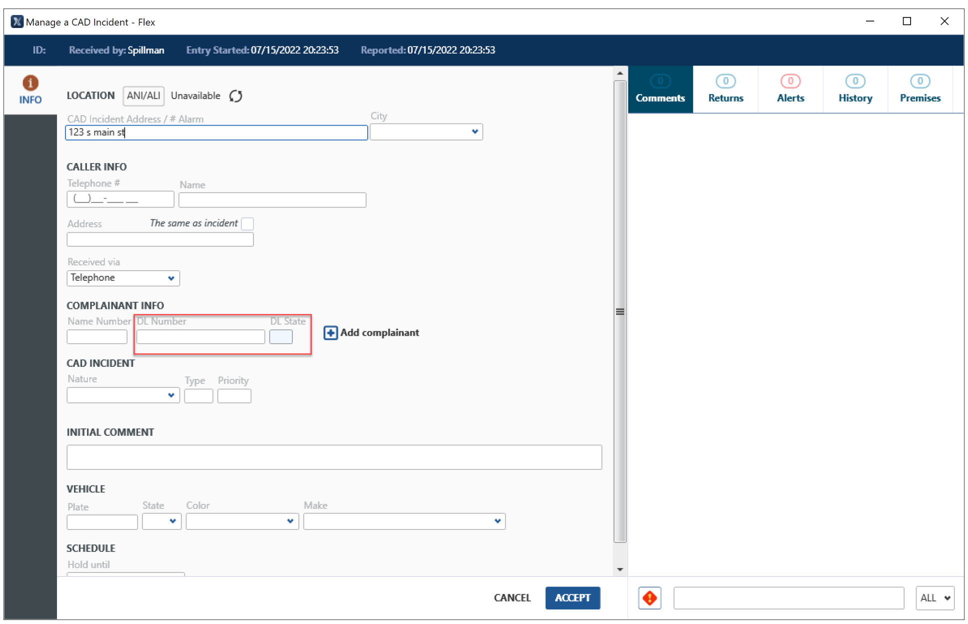
This chapter presents changes made to Flex for the 2022.3 release.

10.1 CAD

10.1.1 DL Number and DL State Fields in the Complainant Area of the CAD Incident Screen

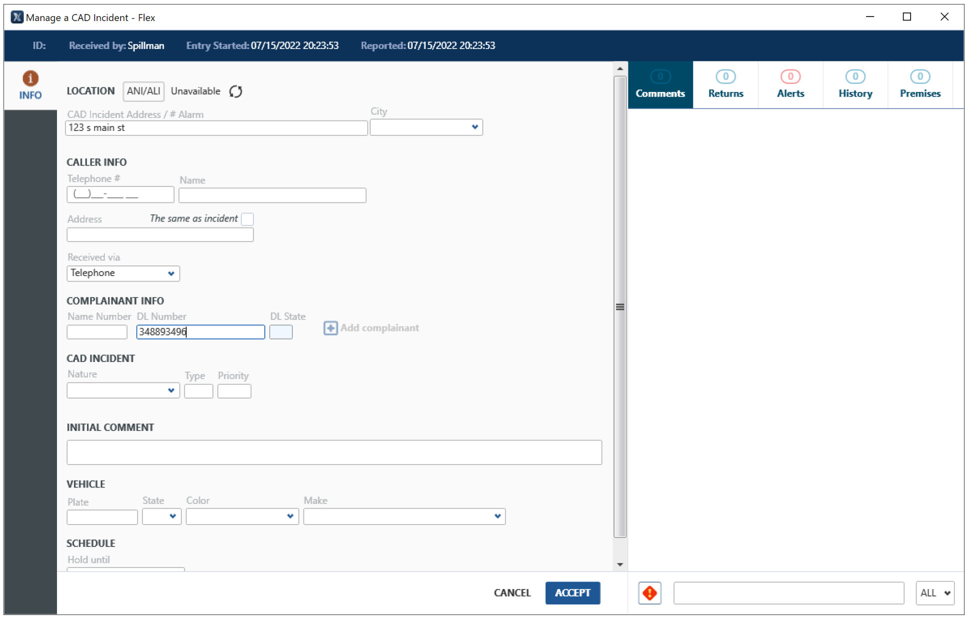
As of the 2022.3 release, two fields are added to the **COMPLAINANT INFO** area of the Manage a CAD Incident screen, **DL Number** (driver license number) and **DL State** (driver license state). This enhancement allows you as a call taker to search and add complainants quickly, just by using Driver License Numbers, if known.

Figure 263: Manage a CAD Incident Screen with DL Number and DL State Fields



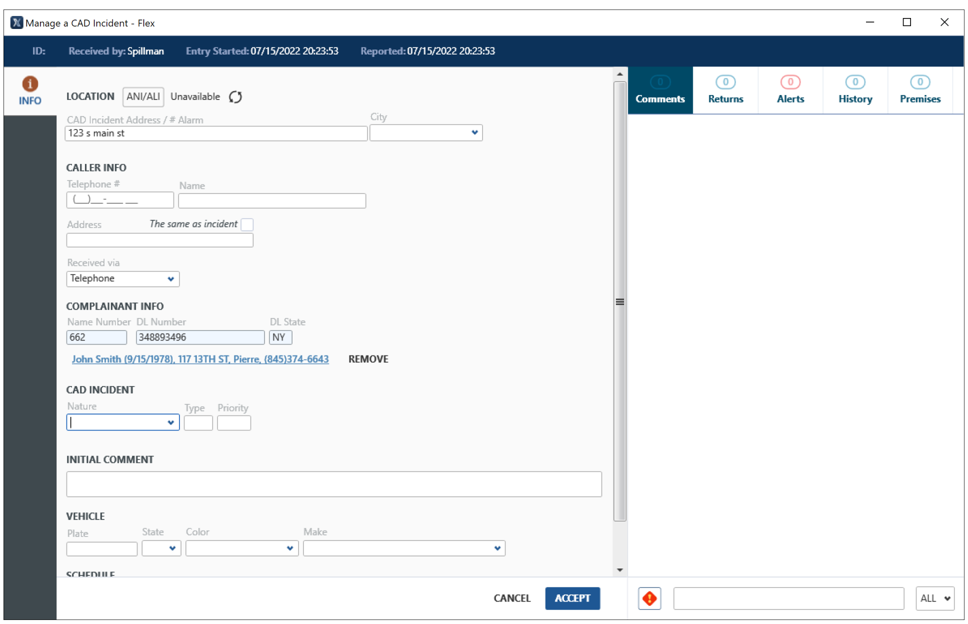
DL Number is searchable. It can be entered by the dispatcher but also automatically populates when corresponds to a **Name Number** used to search the Names Table. The **DL State** field is automatically filled when a result comes back and is read-only.

Figure 264: Search by DL Number Example



When you enter a DL Number and press ENTER, the screen automatically populates with the matching data.

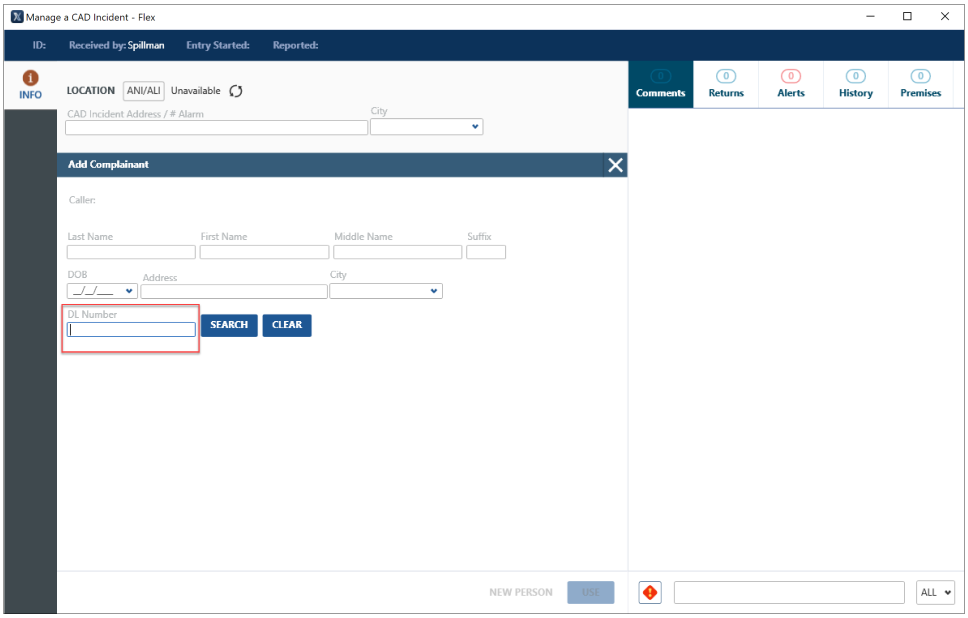
Figure 265: Search by a DL Number Result Example



By clicking the person's link, you can open the Names Table with the name record.

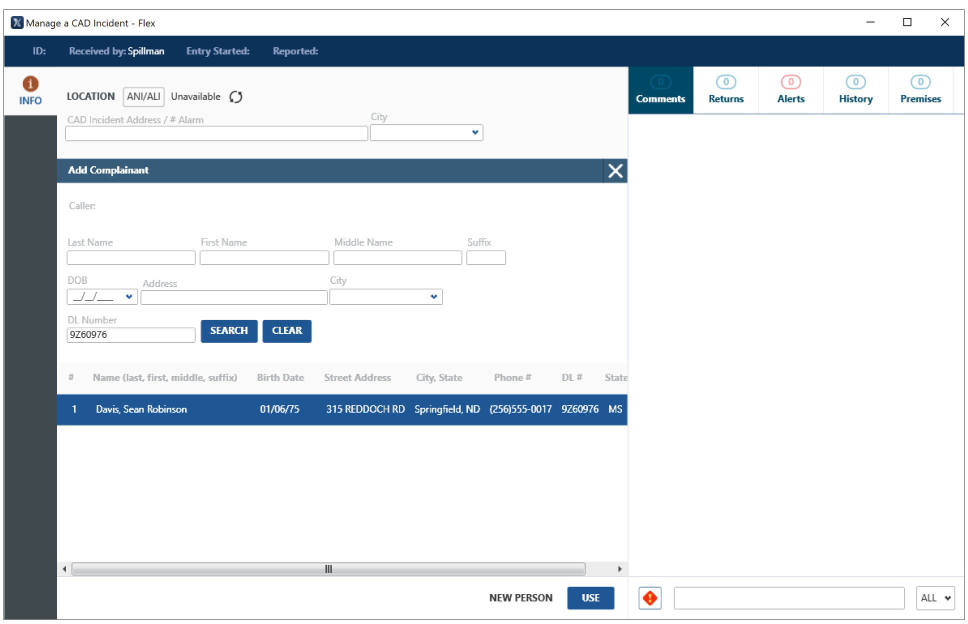
The **DL Number** field is also added to the **Add Complainant** window and can be used to search for a name record. You open the window by clicking the **[+] Add complainant** tab in the **COMPLAINANT INFO** area (see **Figure 1**).

Figure 266: Add Complainant Window with the DL Number Field



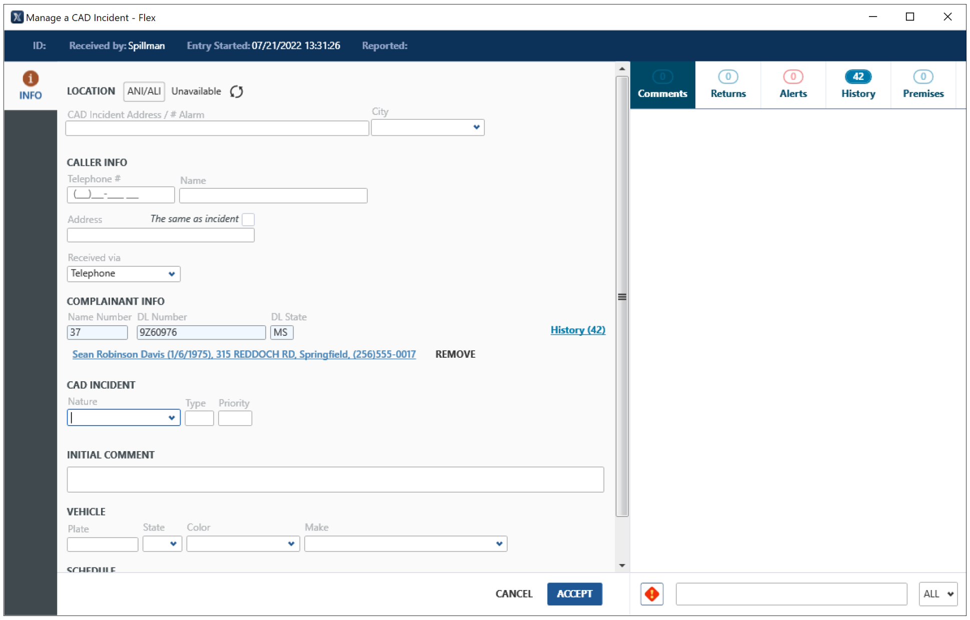
When you fill in the **DL Number** field with a DL Number and click **SEARCH**, you get the search result.

Figure 267: Search Result in the Add Complainant Window



By clicking **USE**, you transfer the result to the **INFO** screen.

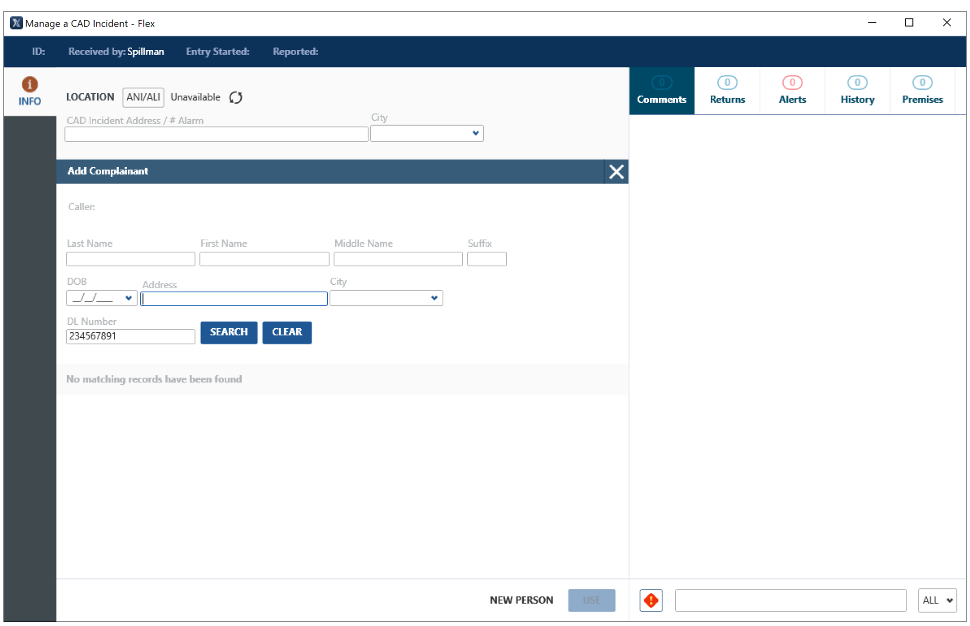
Figure 268: INFO Screen with Auto-Populated COMPLAINANT INFO Area



“Add a New Person as a Complainant” Window with DL Number

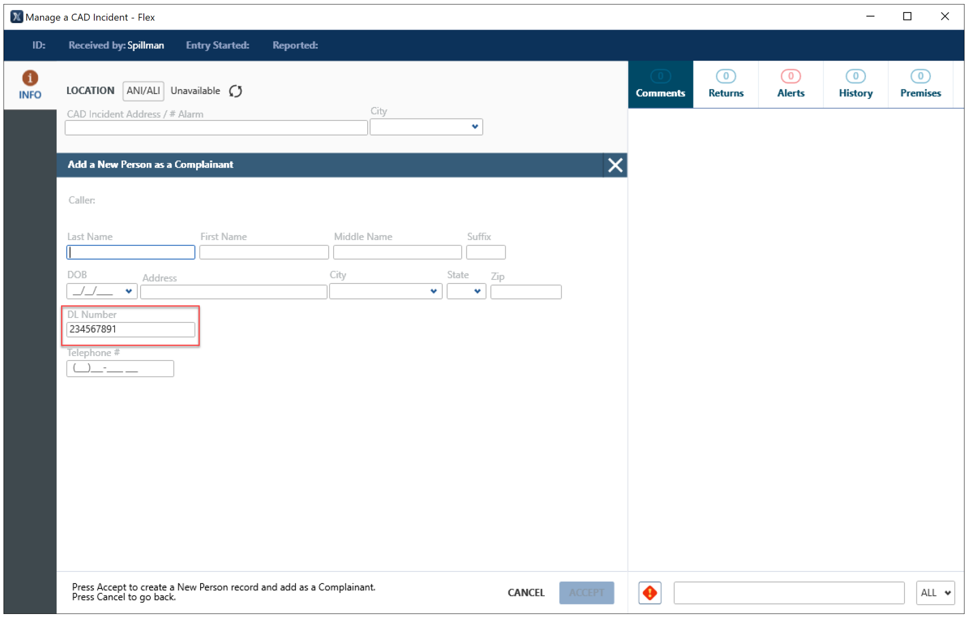
If you are not satisfied with the results in the **Add Complainant** window or receive the `No matching records have been found` message, you should start to create a new record. You can do from the **Add Complainant** window by clicking the **NEW PERSON** tab.

Figure 269: Add Complainant Window with No Matching Results



The **Add a New Person as a Complainant** window that appears also contains the **DL Number** field.

Figure 270: Add a New Person as a Complainant



You should enter the data concerning the new person and click **ACCEPT**. The new complainant information will appear on the **INFO** screen.

10.1.2 Traffic Stop Enhancements

Traffic Stop enhancements streamline the work of officers (Flex Mobile) and call takers (Flex CAD). They also improve the quality of Racial Profiling data.

New features:

- Ability to enter/update demographic information before closing the call from Flex Mobile – see Traffic Stop Demographic Enhancements in Mobile on page 260.
- Improved usability of the DOB (Date Of Birth) field – see Traffic Stop Demographic Enhancements in Mobile on page 260.
- Limited ability to copy Perceived Race and Perceived Sex to actual Race and Sex from CAD Incident screen – see Admin: New Adminutil Setting – trafficStopCopyRaceSex on page 252.
- Prevention of using invalid demographic data from the Traffic Stop screen – see Admin: New Adminutil Setting – trafficStopFieldValidation on page 253.

10.1.2.1 Admin: New Adminutil Setting – trafficStopCopyRaceSex

As an agency's admin, you can change the workflow of the Traffic Stop demographics data in CAD by using the `Module.CAD.trafficStopCopyRaceSex` setting.

The default value of the setting is `True`, and the **Race** and **Sex** fields are populated with perceived values on Call completion. By changing the value to `False`, you prevent copying **Perc. Race** and **Perc. Sex** to **Race** and **Sex** fields on Call completing for a Traffic Stop.

10.1.2.2
Admin: New Adminutil Setting – trafficStopFieldValidation

As an agency's admin, you can change the value of the `Module.CAD.trafficStopFieldValidation` setting to enable validation of three fields on the Traffic Stop screen.

The default value of the setting is `False`, and the system does not validate any fields on the Traffic Stop screen. After you change the value to `True`, if someone types in an invalid value into the **Driver's Race**, **Driver's Gender**, or **Reason for Stop** field, when exiting the field they will see a drop-down allowing them to make a correct choice.

10.2
Hub

10.2.1
Client Log Submission Tool (Report a Problem)

The client log submission tool is designed to collect, compress, and upload all Flex-related client logs to the server upon user request through the **Report a Problem** link.

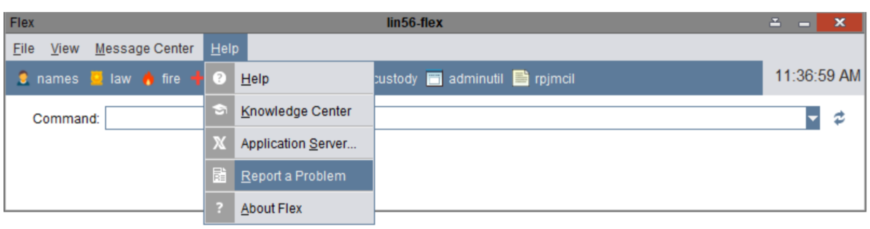
The Report a Problem tool is intended to collect all necessary information to diagnose an issue as soon as possible after the issue happened, to reduce the risk of information loss in the case that an administrator is not available to log in and collect logs in a timely manner. The resulting zip file is stored on the server for later retrieval.

10.2.1.1
Using the Report a Problem Tool

Procedure:

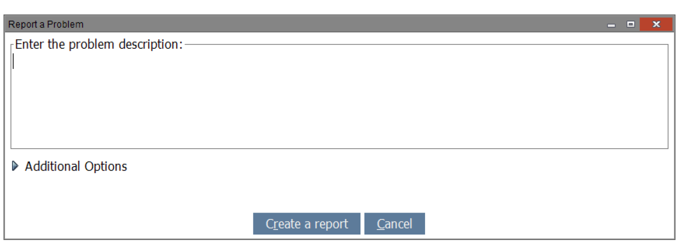
1. From the Flex Mobile **Help** menu, select **Report a Problem**.

   Figure 271: Report a Problem Link Selection

   The **Report a Problem** window appears.

   Figure 272: Report a Problem Window

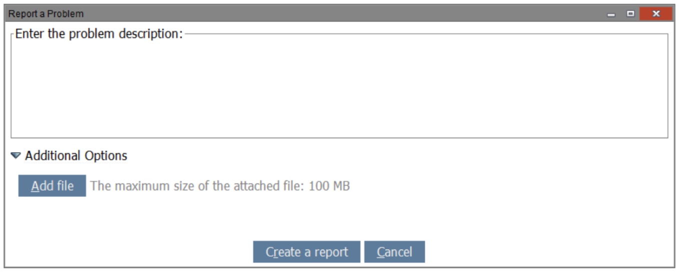
   

2. Enter a description of the problem to explain the context of the issue reported.

   Be as specific as you can about what you encountered, including information about what you were doing when the error occurred and about all its symptoms and displayed messages.

3. Optional: To add a file to the problem report, click the **Additional Options** toggle arrow.

   Figure 273: Report a Problem Window with Add File Option

   As the tool automatically uploads log files, this additional option is meant to upload other files such as screenshots which can be helpful in showing the issue from the user perspective and give the administrator and support personnel more information about the issue being reported.

4. Once you are ready to submit the report, click the **Create a report** button.

The Flex software uploads the files in a `.zip` file, which is saved to `$SPILLMANDIR/reports/{username}/{username}-{date}.zip`

$SPILLMANDIR generally evaluates to `/sds/app/client` on Linux systems and `SpillmanServer\app\client` on Windows systems.

The following logs are collected as part of the operation of this tool:

```
%localappdata%\Spillman\Spillman\{App Version}\Logs\*
%localappdata%\Spillman\CommandCentral Jail\{App Version}\Logs\*
%localappdata%\Spillman\Spillman\Launcher.log
%localappdata%\Spillman\Mobile\Mobile.log
C:\ProgramData\MSI\Map\Logs\*
```

NOTE:

- `{App Version}` is replaced with the actual application version number in the file paths.
- Where asterisks are included in the file path, all logs contained within that directory are included.
- This tool does not configure log levels or turn logs on. It only collects what is in these locations. Log configuration must be done according the specifications of each product.

10.2.1.2

Retrieving Client Logs From the Server

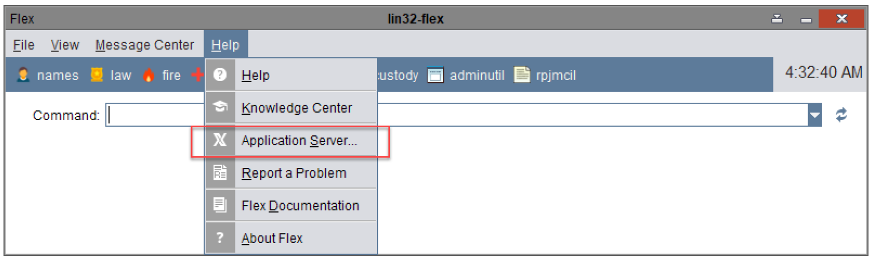
The logs submitted by the Report a Problem tool can either be manually transferred from the server, or retrieved from the Log File Viewer in the Spillman web app by performing the following actions.

Procedure:

1. Navigate to the web app administration page from the Flex **Help** menu by clicking the **Application Server...** link.

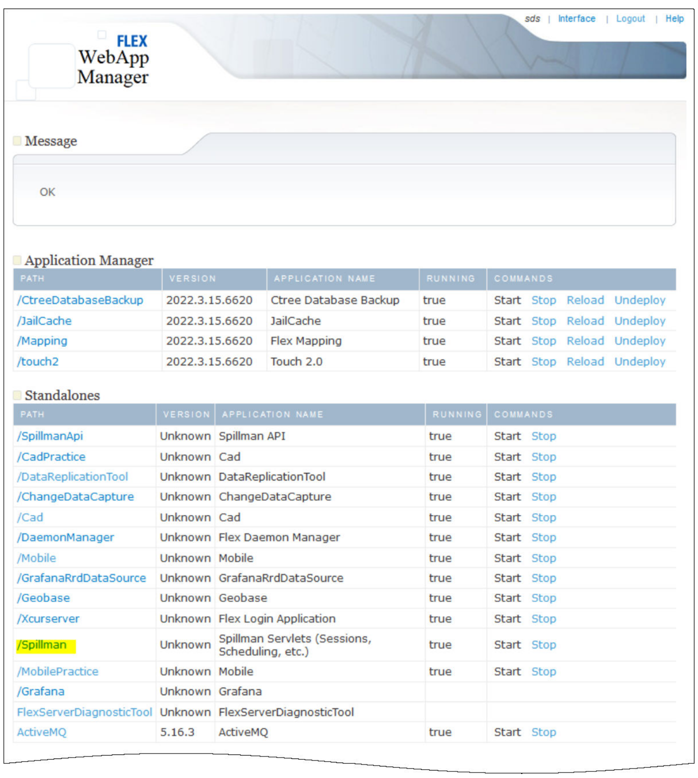
   NOTE: You must be an admin to log into the Application Server.

   Figure 274: Application Server Link

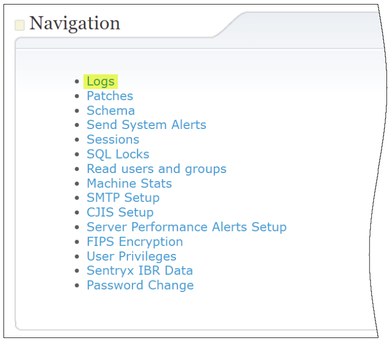
2. On the FLEX WebApp Manager page, click the **/Spillman** link.

   Figure 275: FLEX WebApp Manager Page

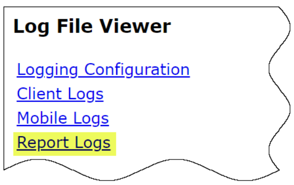
3. On the **Navigation** pane, click the **Logs** link.

Figure 276: Logs Link on the Navigation Pane



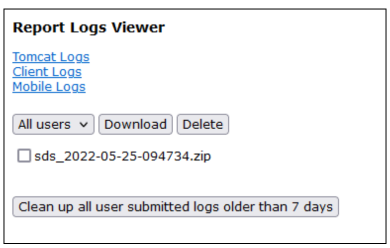
4. On the Log File Viewer page, click **Report Logs**.

Figure 277: Report Logs Link in Log File Viewer



A list of submitted logs appears.

Figure 278: Submitted Logs in the Report Logs Viewer



From this page, you can select and download the report submissions, and delete them, also by using the **Clean up all user submitted logs older than 7 days** option.

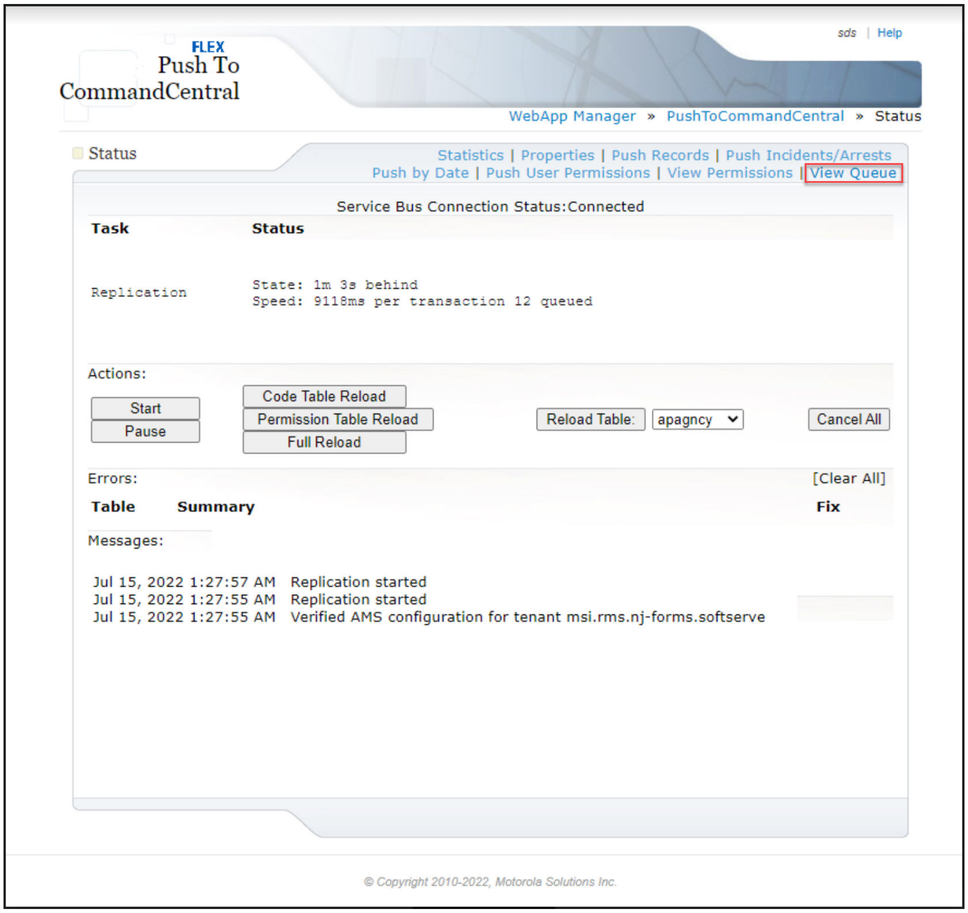
10.3 Records

10.3.1 Ability to View PushToCommandCentral Queue

The PushToCommandCentral webapp is extended with the option of viewing the progress of pushing multiple records to the CommandCentral cloud.

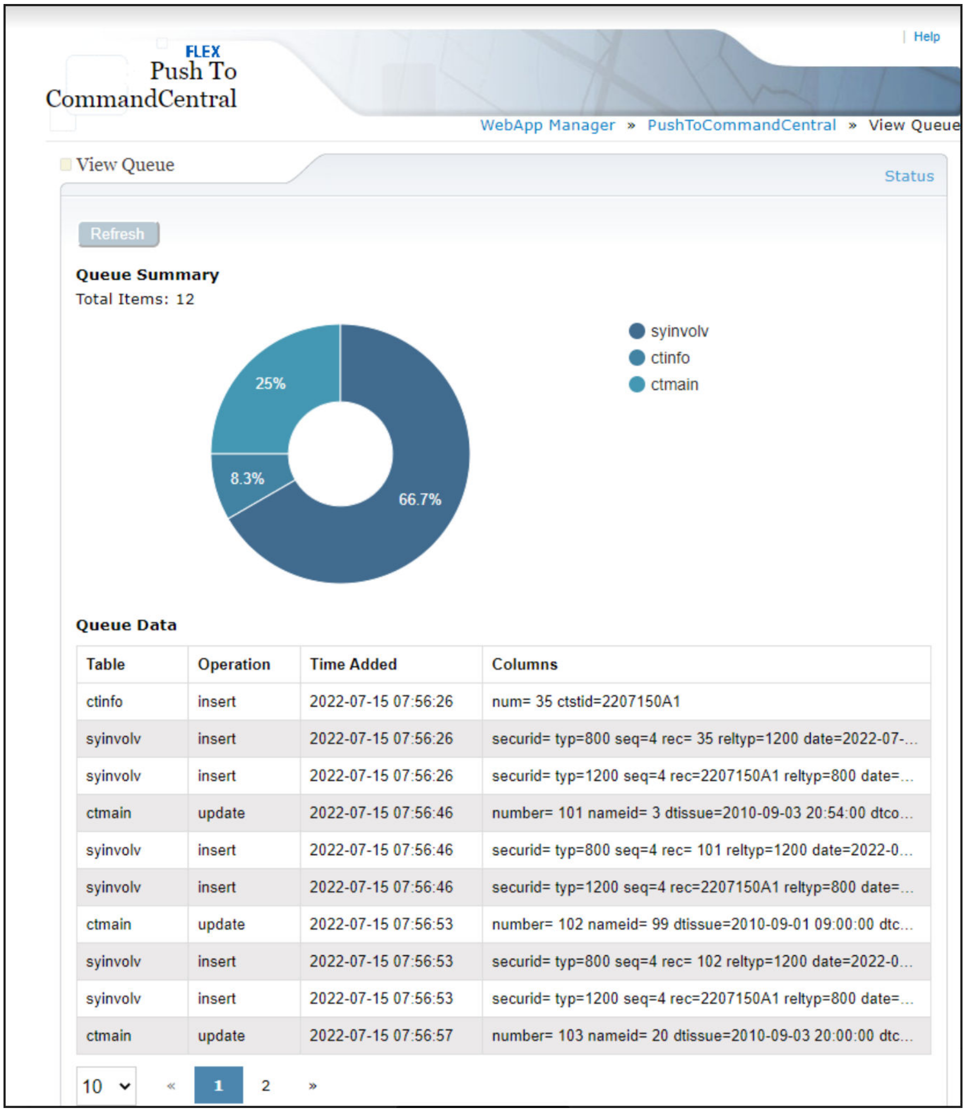
The **WebApp Manager** → **PushToCommandCentral** → **Status** page now contains the **View Queue** tab.

Figure 279: View Queue Tab



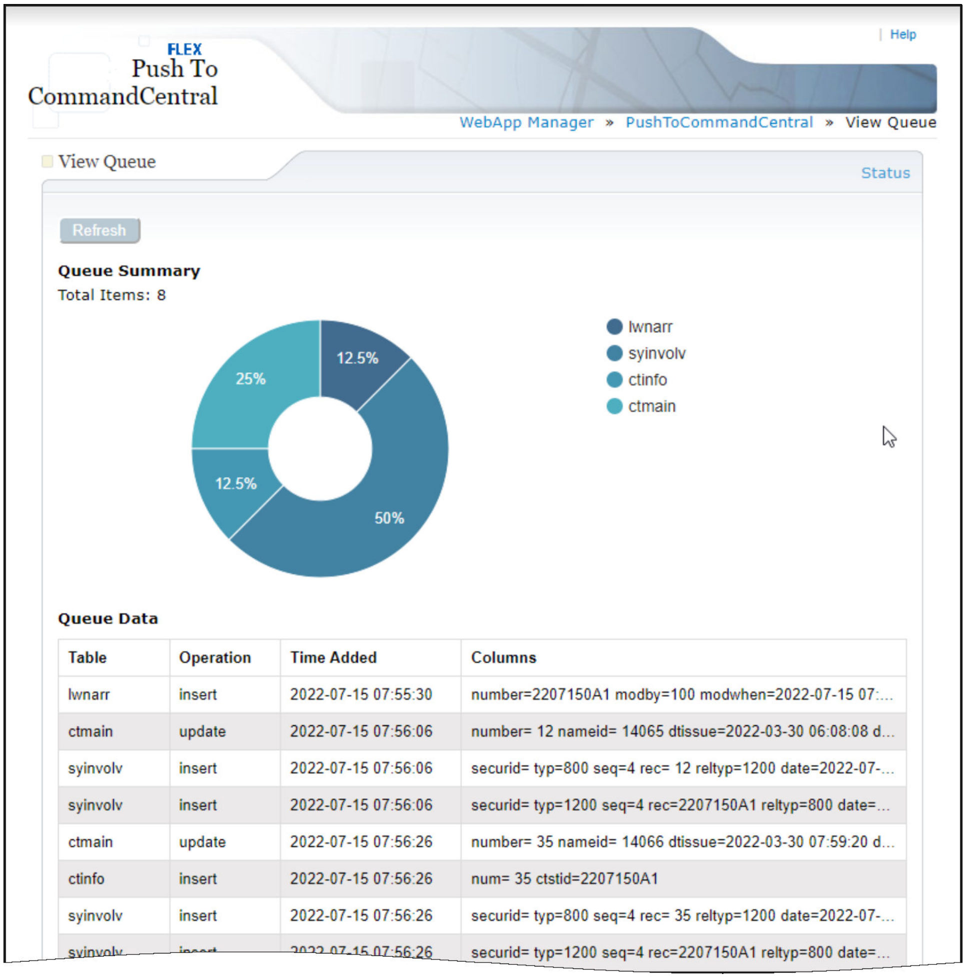
In addition to the **Status** (`State` and `Speed`) data, by clicking the **View Queue** tab you can get access to a range of information about the progress of the data being pushed from the Flex system to the CommandCentral cloud.

Figure 280: View Queue Page



The **Queue Summary** is given in the form of a pie chart with sectors representing proportions of the record types shown in the legend on the right. In addition to the percentages, by hovering your cursor over a sector you can see the number of the queued records of the given type. As the displayed page is a snapshot, you can refresh it at any time by clicking the **Refresh** button.

Figure 281: Refreshed View Queue Page



The **Queue Data** table provides details about the **Table** name, kind of **Operation**, **Time Added** (to the queue), and **Columns** (of the **Table**, with the detail items being updated).

The toolbar with pagination at the bottom of the page is helpful in the case of large amounts of records (the limit is 20,000).

10.3.2
Separate Complaint/Allegation and Incident Number Fields in Pennsylvania Criminal Complaint Forms

A new field called **Complaint Number** or **Allegation Number** (depending on whether the arrestee is an adult or juvenile, respectively) is added to Flex Mobile screen when a specific criminal section is triggered. It is a free text field with a 15-character limit. These changes are available for Pennsylvania Flex agencies having the PA Criminal Complaint feature, after they patch their Flex system to the latest 2022.3 version and use Flex to generate the Pennsylvania Criminal Complaint forms.

A user will be able to manually enter a Complaint Number or Allegation Number. Depending on the specific form to be generated, the system will fill in either the Complaint Number or the Allegation Number in the print outputs, based on the user data entry to this field in Flex.

The relevant forms generated as PDFs will show the numbers separately. The Complaint Number or the Allegation Number will be shown before the Incident Number on the same row of the relevant forms once the forms are printed.

Additionally, the revision (rev) number of each page of the relevant forms have been updated to 12/21. Every page of all of the criminal complaint forms will be updated with the most recent rev number.

10.4 Jail

10.4.1 Transfer of All Name Updates from Flex Jail to P1 RMS

When an arresting agency uses PremierOne Records Management System (P1 RMS), the system always pushes all of the name records changes from Flex Jail to P1 RMS. Previously, name records changes were sent to P1 RMS only during active booking in Flex Jail.

Any changes to a name record are also sent to P1 RMS when the name record in Flex is not associated with any booking record. This way, the name, offense, and disposition information of the inmate is synchronized between the two databases.

If the arresting agency is mapped to the P1 RMS interface, all name updates are sent to the arresting agency. Otherwise, a Flex Jail admin can select an arresting agency that will be the default P1 RMS agency to push name record updates to.

10.5 Mobile and Touch

10.5.1 Traffic Stop Demographic Enhancements in Mobile

During traffic stops, police officers need to record demographic information about the stopped person while they have the driver's license with them. Admins in those agencies can enable a new interim Demographics window within their agency's status process, which allows the officers to enter the data while the call is still open.

Mobile Interim Demographics Window

A new **INTRM** status code allows the interim Demographics to be entered within the agency's status process. Then, the user can customize the main toolbar (**Edit** → **Toolbars** → **Customize**) to add the **Demographics** button.

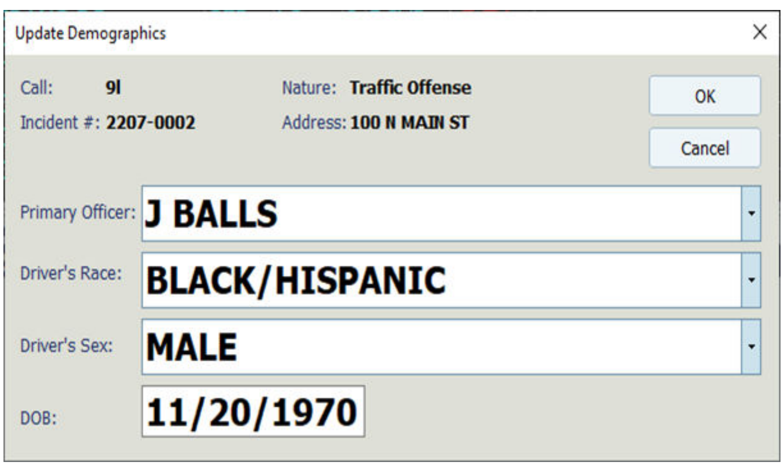
The **Demographics** button on the mobile CAD toolbar automatically appears when the feature is turned on.

Figure 282: Mobile CAD Screen with the Demographics Button

The **Demographics** button on the CAD toolbar on the Mobile CAD screen allows the officer to open the interim **Update Demographics** window.

The **Update Demographics** window contains only the **Primary Officer**, **Driver's Race**, **Driver's Sex**, and **DOB** (Date Of Birth) fields to be filled in by the officer.

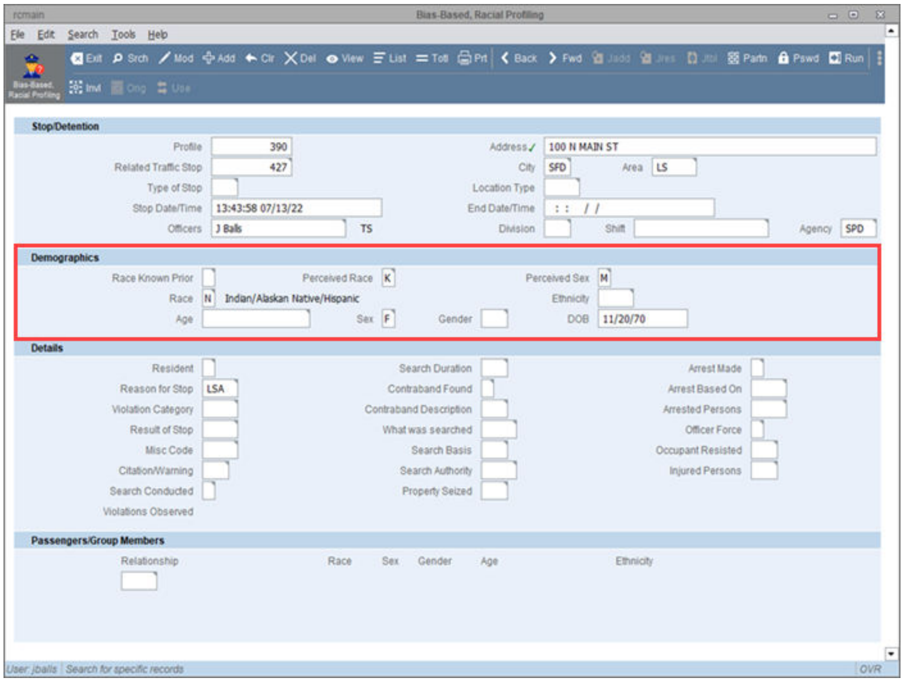
Figure 283: Interim Demographics – Update Demographics Window



In the **DOB** field, the officer can enter the date in any of the `MMDDYY`, `MM/DD/YY`, `MMDDYYYY`, `MM/DD/YYYY`, `M/D/YY`, `M/D/YYYY` formats. If a two-digit year is entered, the correct four-digit year is calculated, and the date is always displayed as `MM/DD/YYYY`.

If the call dispatcher enters information in the CAD traffic stop, that information auto-populates in the **Race** and **Sex** fields on the **Bias-Based, Racial Profiling** screen in the **Demographics** area.

Figure 284: Bias-Based, Racial Profiling – Demographics Area



When the primary officer receives a call, they can use the **Update Demographics** window to enter the actual race, sex, and DOB in the **Age**, **Race**, and **DOB** fields. The information entered by the officer overwrites the information in the **Race** and **Sex** fields entered by the dispatcher.

For example, if the call dispatcher enters `K - Black/Hispanic` as the **Race**, the value is **K**. If the primary officer enters `N- Indian/Alaskan Native/Hispanic` as the **Race**, this overwrites the **Race** value and becomes **N**.

10.5.1.1

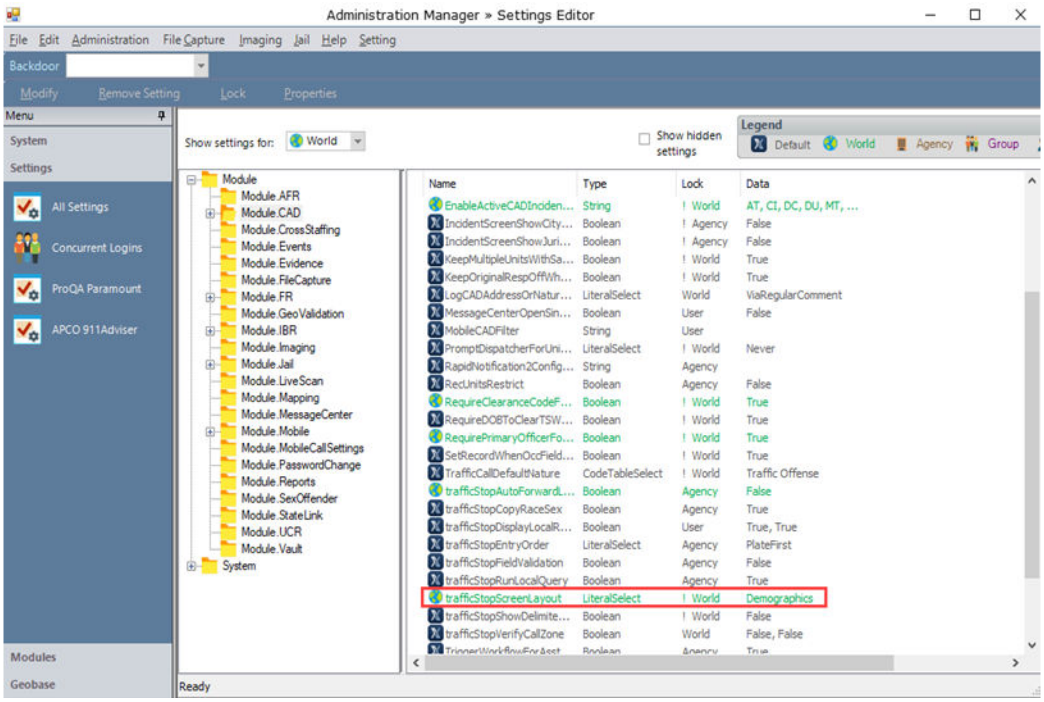
Admin: Enabling the Interim Demographics Feature

Police officers need to record demographic information about a person who was stopped while they have their driver license when the Call is still open. As an admin of the agency that wants to include the interim Demographics within the agency's status process, you must perform the following procedure.

Procedure:

1. In the **Administrator Manager** window, select **Module** → **Module.CAD**.
2. In the **Name** pane, select **trafficStopScreenLayout**.

Figure 285: trafficStopScreenLayout Selection



The **Enter Selection Value** dialog box appears.

3. In the **Enter Selection Value** dialog box, from the drop-down menu, select **Demographics** or **All**, and click **OK**.
4. If your agency wants to use the ***<tb10code>*** in the process, in the **Unit Status Ten-Codes** window, for **INTRM** change the **Send to Mobile** option to `Y`.

   This option makes the code available in Mobile.
5. Update the correct **Responding Units Status Order** (`cdstatse`) to include **INTRM** as a part of the CAD Status Order.

10.6 GeoValidation/Mapping/Quickest Route

Admin: Support for ESRI ArcGIS Server 10.9.1

As of the 2022.3 release, the supported ESRI ArcGIS servers are 10.7.1, 10.8.1, and **10.9.1**. Please pay attention to the new **minimum** hardware requirements for a GIS server:

- CPU: 4 cores
- RAM: 32 GB
- Disk: 100 GB

For more details, see *Flex Hardware Requirements Release 2022.3*.

Chapter 11

Release 2022.2

This chapter presents changes made to Flex for the 2022.2 release.

11.1 Records

11.1.1 Admin: PushToCommandCentral - Push by Date

The PushToCommandCentral **Push by Date** button allows agency administrators and Technical Services to push incidents and arrests to the cloud by selecting a date and time range. The time is relevant to the local time of the server. The feature allows the relevant Flex tables and involvements of the incidents and arrests to be ingested into the cloud.

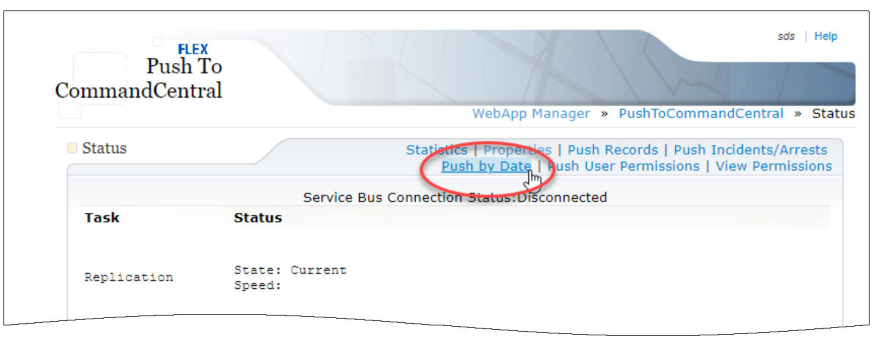
The feature is useful for agencies that use CommandCentral forms in the cloud and might encounter problems with opening the forms. When the PushTo CommandCentral is queued up, it allows the incident data to be ingested more quickly, so that the CommandCentral forms can be opened after the ingest is done. It can help the administrators and Technical Services to analyze and fix users' problems.

11.1.1.1 Using Push by Date

Procedure:

1. Open the **WebApp Manager** → **PushToCommandCentral** → **Status** page.

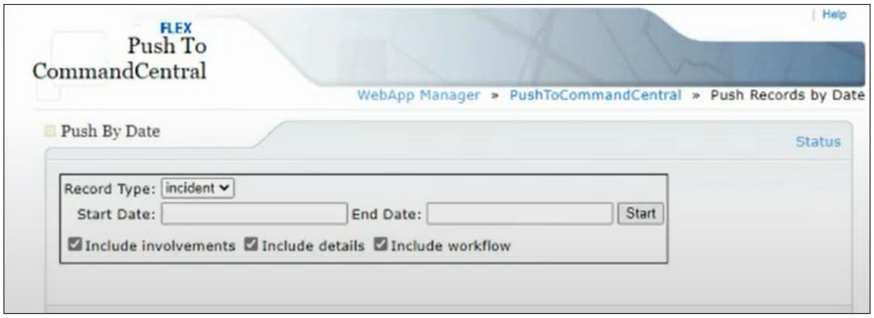
   Figure 286: Push by Date Link

2. Click the **Push by Date** link.

   A dialog with selection options opens up.

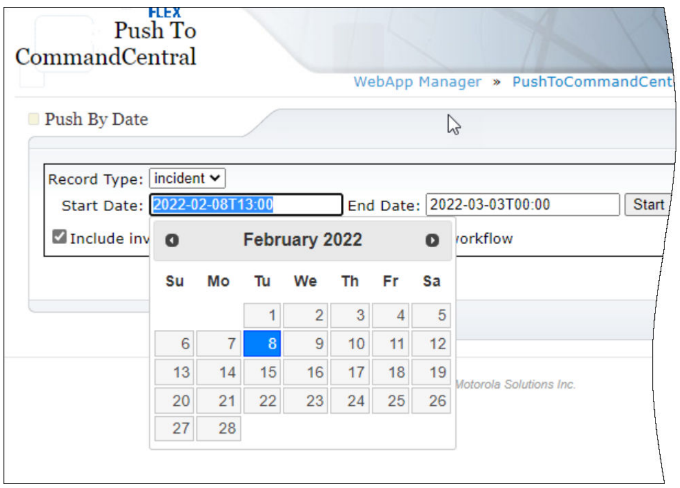
Figure 287: Push by Date Selection Options



3. Choose the **Record Type** (mostly **incident**), select the items to include, and input the **Start Date** and **End Date** of the required time period.

   When you begin to enter the dates, the calender view appears as an input option.

   Figure 288: Calendar View

4. To begin the upload, click the **Start** button to the right of the **End Date** field.

   The CommandCentral forms can be opened after the ingest is done.

11.1.2 Admin: Vault Integration – Setup of Deleting Files from Disk in Flex

The Vault Integration setting that allows for deleting files from the disk has been moved to Flex settings. The functionality is now available as of the Flex 2021.4 release.

The setting is located in the **Module.Vault** folder

Default Settings

The current default settings are:

- **DeleteFromDisk** is set to `False`
- **DeleteFromDiskPeriod** is set to `30` days

- **ShowInactiveUsers** is set to `True`

NOTE: With the default settings, the feature, including the 30-day retention period, is **not** active

DeleteFromDisk Functionality

The functionality is activated by setting the **DeleteFromDisk** setting to `True`. If the default retention period of 30 days is not appropriate for your agency, you can change it to the required number of days (positive integer). If you put 0, it means that there is no delay, and the files are deleted from the disk just after the upload to the Vault.

NOTE: The other time units that were available in the webapp are not supported. The time unit of **DeleteFromDiskPeriod** is one day.

11.1.3 Admin: Vault Integration – Default Retention Period

The default retention period for offense tags has been changed from permanent hold to 9999 days. This allows the files to be purged in Vault. The functionality is now available as of the Flex 2021.3 release.

11.1.4 Jail

11.1.4.1 Biometrics for Temporary Release

The ability to verify the stored fingerprints of the inmate during a temporary release has been added. The functionality is available as of the Flex 2022.2 release.

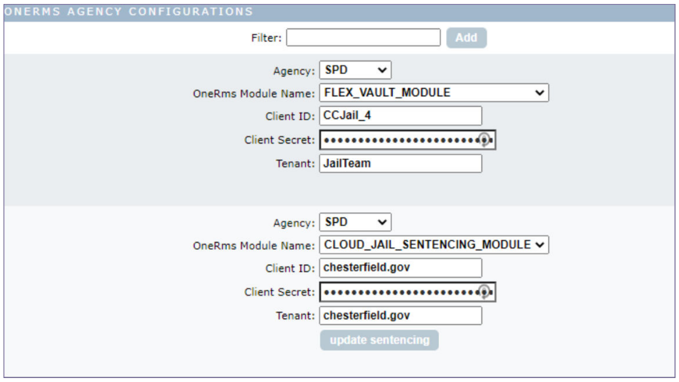
The feature does not require any new settings (they are leveraged from the existing settings for the biometrics for the permanent release). If your agency has the biometrics for the permanent release today, once it upgrades to 2022.2, it will get the biometrics for temporary release automatically without having to contact Motorola Solutions.

11.1.4.2 Admin: Automatic Good Time Calculation

This setting allows the calculation of the good time credits automatically in Flex Jail, based on the initial sentence. The functionality is available as of the Flex 2022.2 release.

The sentencing details can be updated in Flex for any agency on one-time basis through **ONERMS AGENCY CONFIGURATIONS** of the cloud sentencing service.

Figure 289: ONERMS AGENCY CONFIGURATIONS Page



The solution must be adapted to the needs of the agency and requires specific symodules and settings:

- `Cloudsentence` = `Y`
- `Module.Jail.Sentence.GoodTime.automaticGoodTime` = `True`

Following code tables are needed:

- Felony class (flex: jail.offense.crime.class)
- Exempt from credit (flex: tblaw, tboff)

To configure and implement the solution, you must contact Technical Services.

11.2 CAD

11.2.1 CAD Incident Screen Enhancements

New CAD screens are now 98.5% faster (on average). The tested screens include AC, AT, and CI. Thanks to faster screens and functions in CAD, call takers and dispatchers are not waiting for CAD to respond.

The reduction of the response times is mainly the result of using client machines for most operations and minimizing the number and time of connections to servers. For optimal operation, Motorola Solutions also recommends client machines with 16 GB RAM, and changes the minimum requirements from 4 GB to 8 GB.

11.2.1.1 Admin: Setting Up the New Workflow for CAD Screens

The `ClientCommandLineParser` setting allows you to toggle between the original and new workflow for loading CAD incident screens.

The setting determines whether the AC, AT, CI, DC, DU, MC, UC, or UU command opens the screen without calling to Hub, which reduces the screen loading time, or the workflow does not change. This setting is located in the **Module.CAD** folder. The default value is `False`.

Procedure:

1. At the command line, enter `adminutil`
2. From the tree menu, expand the **Module** folder and double-click the **Module.CAD** folder.
3. In the setting window on the right, locate the `ClientCommandLineParser` setting and double-click it.

The **Enter True/False Value - for world** dialog box opens, with the `False` default value of the `Module.CAD.ClientCommandLineParser` setting.

4. Set the **Value** to `True` and click **OK**.
5. Close the **Administration Manager >> Settings Editor** window.

11.2.2

Response Plans with Zone Stacking

The new configuration allows for creating response plans similar to run cards.

Figure 290: Run Card Example

Run Card 123 Main St				
Alarm	Engine	Ladder	MED	Chief
1st	Sta 1	Sta 1	Sta 1	Sta 3
2nd	Sta 4	Sta 3	Sta 4	Sta 6
3rd	Sta2	Sta 2	STA 2	
4th	Sta3		Sta3	

Law, Fire, and EMS agencies will be able to configure response assignments based on response areas. The configurations performed by administrators can provide accurate recommendations for dispatchers. Recommendation plans for a covering zone also support working with `Module.CAD.FlexUnitRecommendations.EnableSmartRecommendations` setting.

The presentation rules on the CAD screen are as follows:

- Recommendation plans for covering zones are displayed as dropdowns at the level under that for the call zone.
- Response/Recommendation plans for covering zones are proposed in the order of their sequence in **cdcvzone** table, but always after plans for the main (covered) zone.

11.2.2.1

Admin: Configuring Response Plans by Using Zone Stacking

After the configuration, FLEX will search for a response/recommendation plan also by using covering zones.

Procedure:

1. At the command line, enter `adminutil`
2. From the tree menu, expand the **Module** and **Module.CAD** folders.
3. Click the **Module.CAD.FlexUnitRecommendations** subfolder.
4. In the setting window on the right, locate the `EnableCoveringZones` setting and double-click it.

The **Enter True/False Value - for world** dialog box opens, with the `False` default value of the `Module.CAD.FlexUnitRecommendations.EnableCoveringZones` setting.

5. Set the **Value** to `True` and click **OK**.
6. Close the **Administration Manager >> Settings Editor** window.

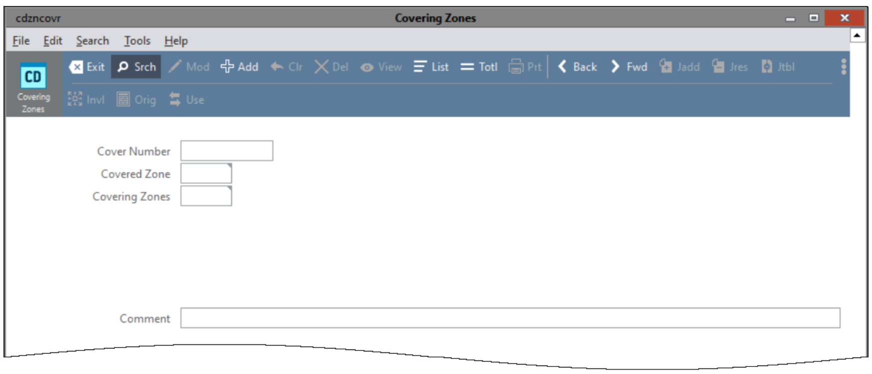
11.2.2.2 Setting Up Covering Zones

With the covering zones feature enabled by your administrator, you can set up the zones.

Procedure:

1. From the command line, open the **cdzncovr** screen.

   Figure 291: Covering Zones Screen



2. For each **Cover Number** and **Covered Zone**, add, modify, or delete the **Covering Zones**.

   NOTE: The zone fields require a valid zone keyed from the **tbzones** table.

   There are two new tables:

   - **cdzncovr** – the main covering zone table
   - **cdcvzone** – the covering zones detail table

11.3 Touch and Mobile

11.3.1 Filtering and Sorting Functions for Call Comments in Touch

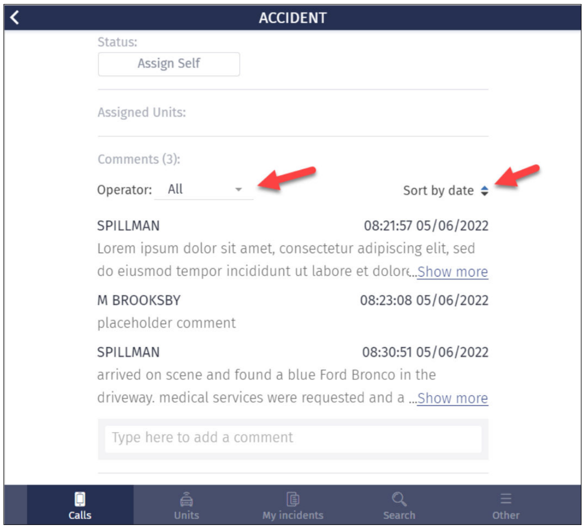
Touch users now have the ability to filter and sort call comments. The filtering is based on the choice of the author. The sorting is based on date, which allows users to find specific call comments they are looking for much quicker.

The functionality is available as of the Flex release 2022.2 and Touch application version 1.7.

You can perform filtering of comments by selecting a name in the **Operator** drop-down list. Only comments from that person will appear on the screen. The **All** option means no filtering.

You can also sort comments by date, by scrolling through the dates with the up and down chevrons.

Figure 292: Filtering and Sorting Call Comments



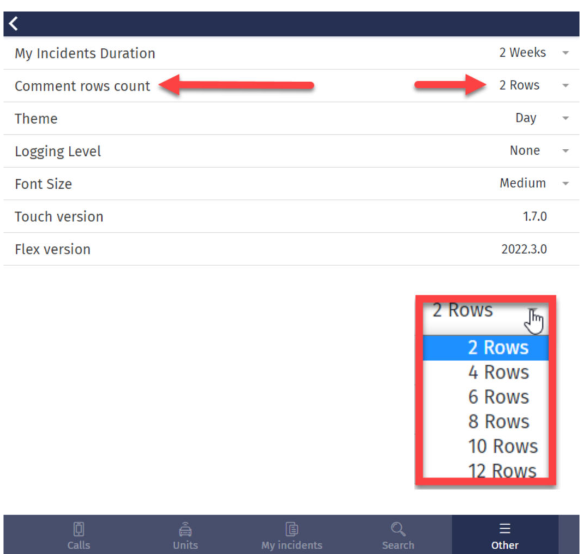
11.3.2 Row Number Selection for Call Comments in Touch

You can now determine how many lines you want to display in the list. This should help you to clean up the list and scroll it more easily, or see the full body of the comments, if you want.

The functionality is available as of the Flex release 2022.2 and Touch application version 1.7.

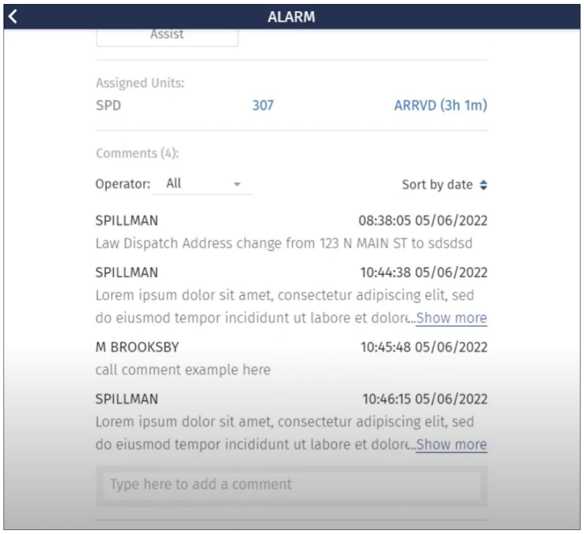
You can configure the setting in the Touch application by tapping **Settings** → **Other** → **Comment rows count**, and selecting the number of rows.

Figure 293: Comment Rows Count Setting



You can set 2, 4, 6, 8, 10, or 12 rows. If not all lines of a comment are displayed, they will appear when you tap **Show more** at the end of the last line.

Figure 294: Touch Screen Example with Comments



Chapter 12

Release 2022.1

This chapter presents changes made to Flex for the 2022.1 release.

12.1 Records

12.1.1 Admin: Limiting the Number of Displayed Involvements in MFRs

Mobile Field Reports (MFRs) concerning law incidents can contain many involvements. If users in your agency are experiencing performance issues with such reports, you can limit the number of the initially displayed involvements to five records per tab (category).

The limit is controlled by the **Module.FR.LimitDetailItems** setting.

Procedure:

In the Administration Manager (**adminutil**), in the **Module.FR** folder, set the value of the `LimitDetailItems` setting to `True`

By default, the value of the setting is `False`

NOTE: The feature becomes available as of Flex 2021.2. The limit of five records is not configurable.

12.1.2 Using MFRs with the Limit on the Number of Displayed Records

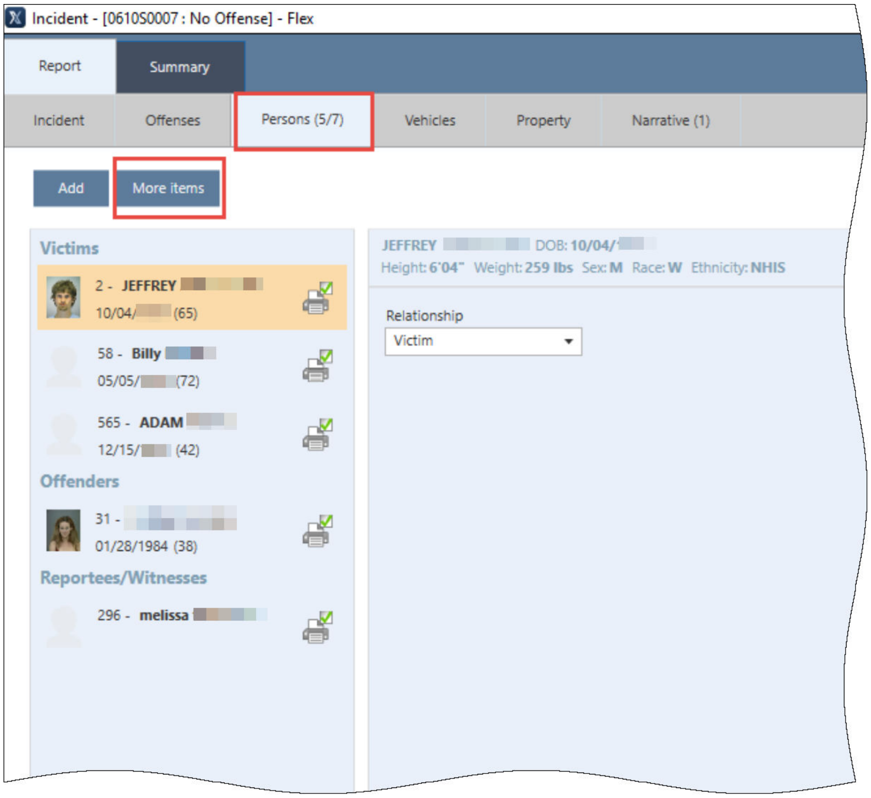
This information is applicable only if your admin decided to limit the number of records initially displayed in Mobile Field Reports (MFRs) to five for each category.

Procedure:

1. When you run the MFR for an incident, open a category tab you are interested in.

   If the category contains more than five involvements (records), only the first five of them appear on your screen. You see the **(5/x)** indicator on the category tab, where **x** means the total number of the existing records. To the right of the **Add** button, you can notice the **More items** button.

Figure 295: Initial List of Records with the First Five Items



In the example figure, the changes are highlighted by red frames. The **Report** tab for **Persons** shows five out of the total of seven records: Persons (5/7).

2. If the category contains more than five records, perform one of the following actions:
   - When you are not interested in the rest of the records in this category, switch to another tab of your interest.
   - When you want to display all records in this category, tap the **More items** button.

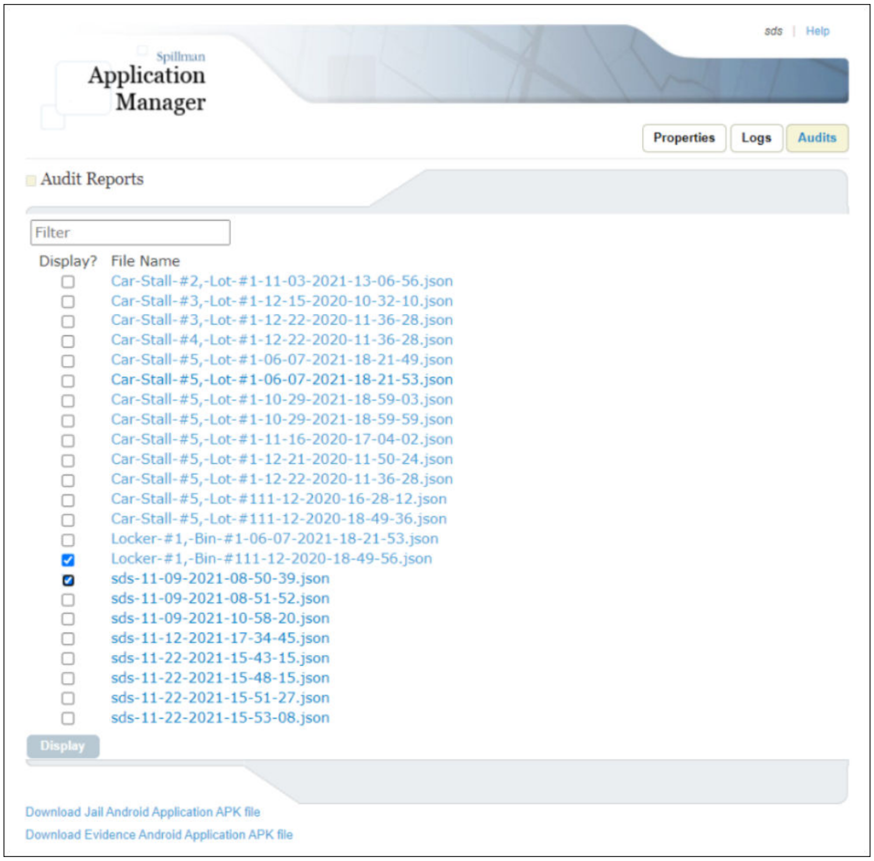
   NOTE: If you omit the rest of the records in any category, and you open the **Summary** tab, a prompt message informs you that only the records displayed will be visible in the Summary report. The prompt gives you the option to load all the remaining records.

12.1.3
Admin: Evidence Audit Reports

Agencies using Datalogic Memor 10 scanners can now view their evidence inventory audit reports also in the BarcodeScanner web application. The reports generated from the application have a similar form to that obtained with the use of the previous scanners. The feature becomes available as of Flex 2021.2, and currently requires administrative privileges.

The list of reports is available after selecting the new **Audits** tab in the upper right corner of the BardcodeScanner web application page.

Figure 296: Inventory Audit Reports



The list allows for selecting any number of items that should be included in a report. The report with these items is generated and displayed after clicking the **Display** button.

Figure 297: Inventory Audit Report Sample

Evidence Scanner Inventory and Movement

Pierre Police Department

Importing files: ["Locker-#1,-Bin-#111-12-2020-18-49-56.json","sds-11-09-2021-08-50-39.json"]

Inventory Data Analysis:

Location: LOCKER #1 Locker #1, Bin #1

Item #	Description	Error
4	RCA Television	Item present in database, but not scanned
6	Evidence	Item present in database, but not scanned
test	*<Unknown>*	Item scanned, but not present in database
1	One Rape Kit	Item scanned in LOCKER #1, but evmain.lct is CAR STALL #5

Number of items scanned in this location: *<Unknown>*
Number of items belonging in this location: *<Unknown>*
Number of errors reported in this location: 4

Location: LOCKER #4 Locker #4, Bin #1

Item #	Description	Error
300	*<Unknown>*	Item scanned, but not present in database
1	One Rape Kit	Item scanned in LOCKER #4, but evmain.lct is LOCKER #5

Number of items scanned in this location: 3
Number of items belonging in this location: 1
Number of errors reported in this location: 2

Results of Inventory Analysis

Number of locations inventoried: 2
Number of items scanned: 3
Number of errors encountered: 6

NOTE: The reports from the BardcodeScanner web application will cover Memor 10 audits performed **after** deploying the feature in your agency.

12.1.4

California Stop Records Module (CA RIPA)

The California (CA) Legislature passed the Assembly Bill (AB) 953 (the Racial and Identity Profiling Act of 2015) requiring all city and county local law enforcement agencies that employ peace officers in CA to collect stop data and to annually report to the CA Department of Justice (DOJ).

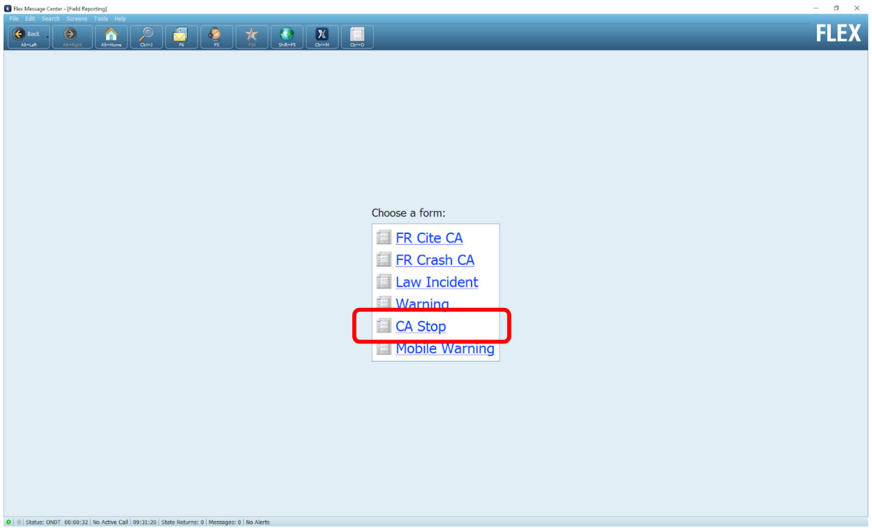
To help our customers be compliant to AB 953, the California Stop Records Module is made available as a cloud solution allowing officers to collect the stop data and to send the data to a statewide repository hosted by the CA DOJ. Our solution contains built-in validation tools to drive compliance, and its conditional logic accelerates the entry of data.

The Module offers full workflow review for data completeness and Personal Identifiable Information (PII) exclusion, and it enables the records clerks to submit the data to the DOJ system directly via SFTP.

The California Stop Records Module is available within the CommandCentral Records cloud application, and is integrated with Flex Records to streamline the workflow. Officers can create stop records in the California Stop Records Module for law incidents created in Flex.

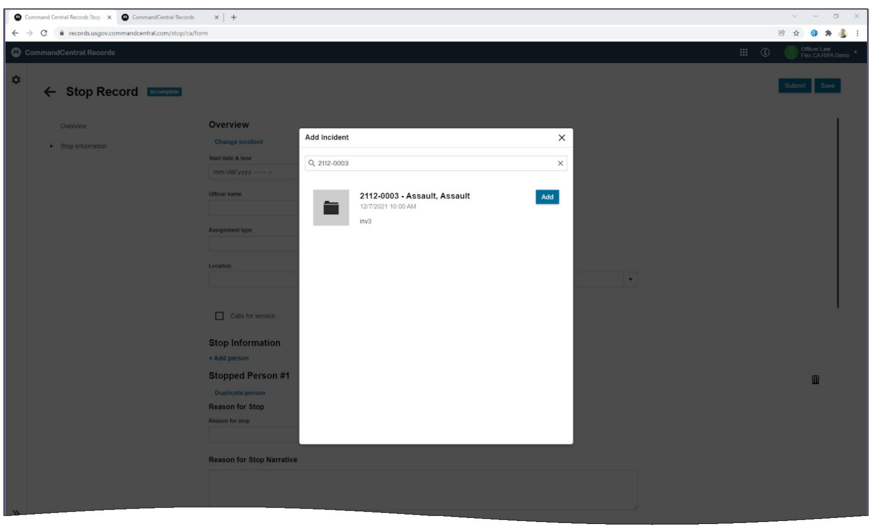
The access to the module is possible through Flex Mobile, or directly from *records.commandcentral.com*, after a CA agency is configured for CommandCentral capabilities. In both cases, user credentials for CommandCentral are needed.

Figure 298: Flex Mobile CA Stop Option



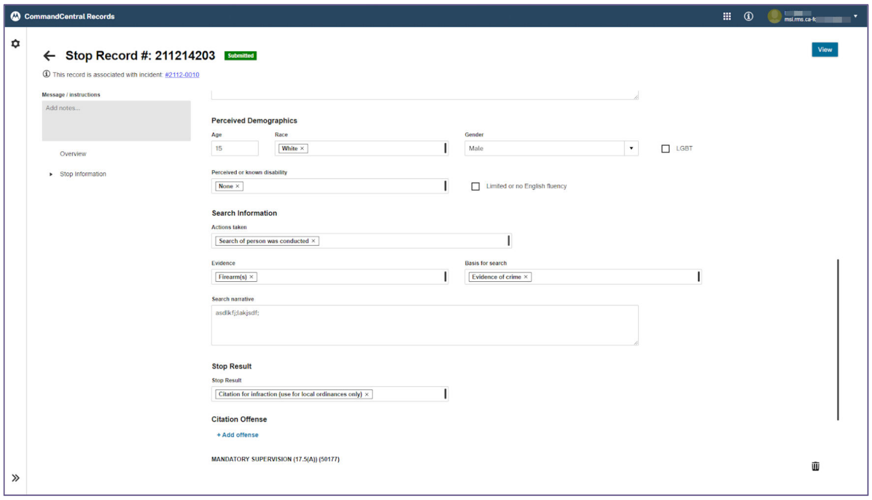
The authorized users get access to the CA Stop forms in a web browser. The users (officers) can search for Flex law incidents they want to associate with the stops, can search for names, offenses, and so on. In the following example, the officer found an associated incident by its number, so that some information can be transferred to the Stop Record form.

Figure 299: Flex Incident Associated with CA Stop



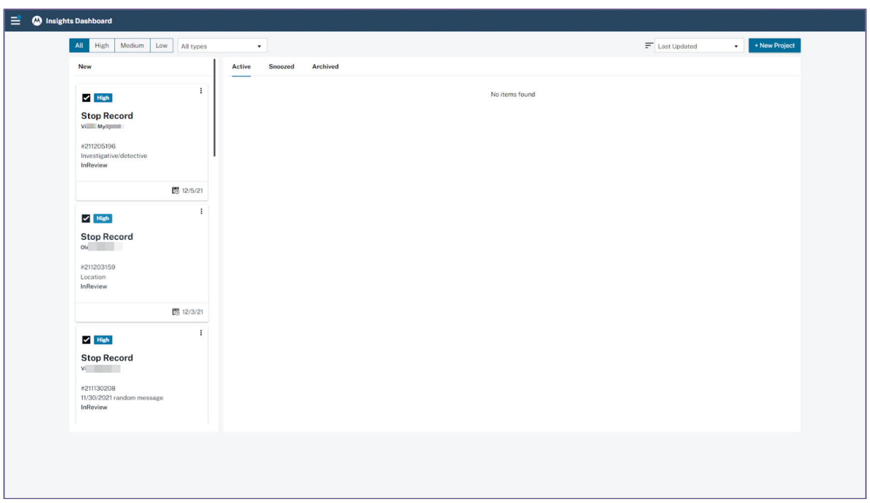
However, most data needs to be entered directly by officers, with the restrictions on identifying information. All the CA stop information is stored in CommandCentral hosted on Azure Gov Cloud, and is **not** synchronized with Flex databases.

Figure 300: CA Stop Record Example



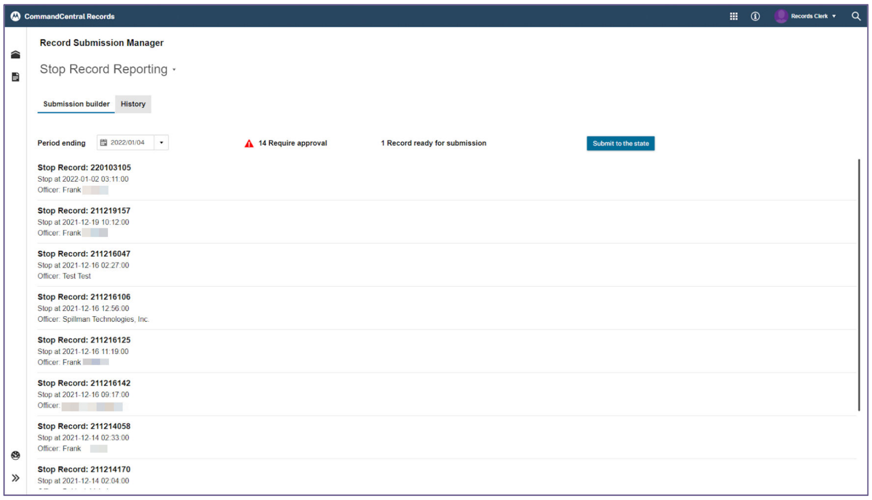
The Stop Record form uses CommandCentral workflow and reporting. The users can see assignments in the CommandCentral Insights Dashboard.

Figure 301: Stop Records in the CommandCentral Insights Dashboard



Records Clerks have access to the CommandCentral Record Submission Manager and can view records that still need to be approved.

Figure 302: CommandCentral Record Submission Manager



Depending on the one or two-step workflow in the agency, the records approved by the supervisor and ready for submission can be submitted to the state by the submission manager with the appropriate permissions. The current submission method is using SFTP.

The **History** tab provides a view of all submitted records, allowing for audits required by the state, and for identifying Stop Records that for some reason failed the DOJ verification.

For more information on California Stop Records Module and its configuration in CommandCentral Admin, see the *California Stop Records Module User Guide*.

12.2 Mapping

12.2.1 Admin: Accelerating the Address Maintenance Process

The new capability of running Address Maintenance on a defined extent, limiting the number of processed gbaddr records only to those within that extent, allows you to significantly reduce the time of the maintenance process. The feature is now available of the 2021.2 release.

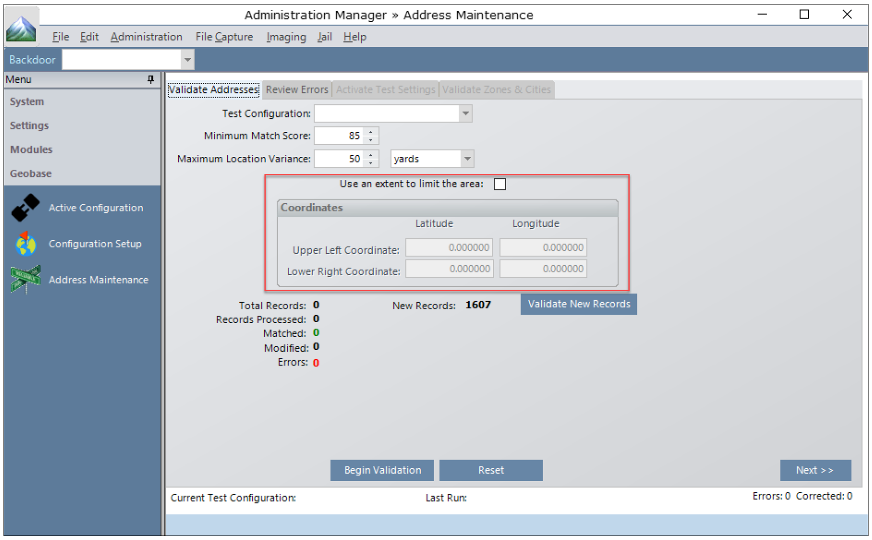
When you want to run address maintenance for the specified extent needed for your agency, perform the following actions.

Procedure:

1. Open Administrator Manager (**adminutil**) and click **Geobase**.
2. From the **Menu** pane, click **Address Maintenance**.

   The Address Maintenance screen with the **Validate Addresses** tab opens, with new UI elements and updated layout.

Figure 303: Validate Addresses Tab with a New UI

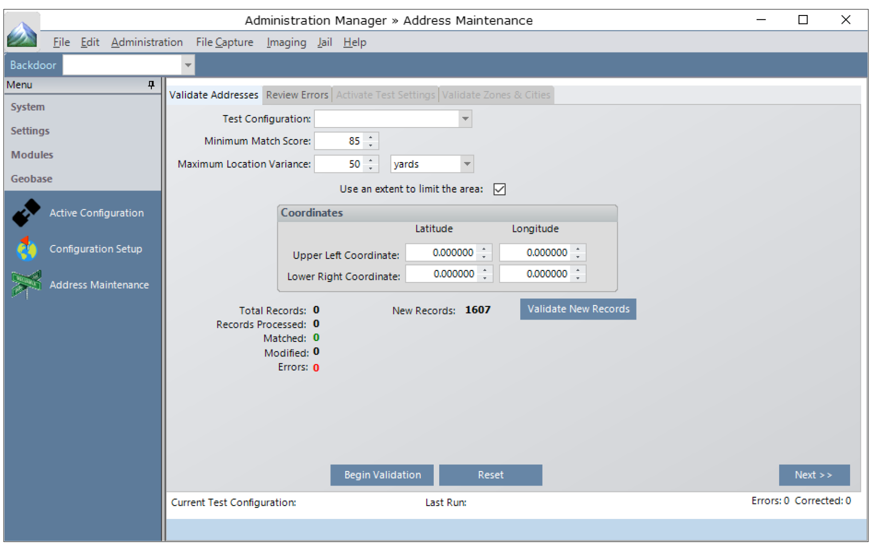


In the figure, the new elements are highlighted by the red frame.

3. Select the **Use an extent to limit the area** check box.

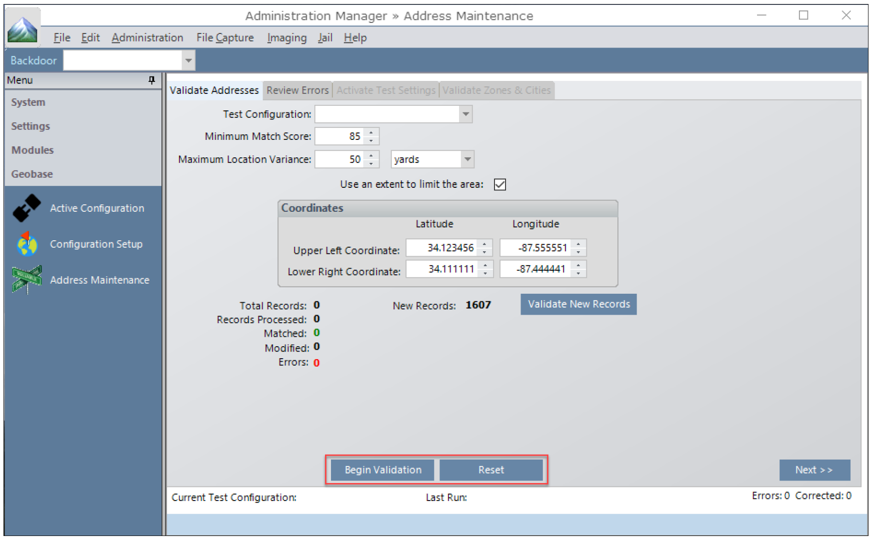
   The **Coordinates** area becomes active along with the numeric fields.

Figure 304: Validate Addresses Tab with Active Coordinates Area



4. Specify the extent for address maintenance.

Figure 305: Validate Addresses Tab with a Defined Extent



In the figure, the **Begin Validation** and **Reset** buttons framed in red can change their names and functions in further processing.

NOTE:
If you enter invalid values, for example use upper left coordinates instead of lower right coordinates, a notification appears like:

```
Invalid value(s) for extent

Latitude for the upper left corner of the extent should be greater than
latitude for lower right corner. Longitude for the upper corner of the
extent should be less than longitude for lower right corner.
```

To proceed, you must correct the data.

5. Click **Begin Validation**.

   The address maintenance process begins.

   NOTE: If you click the **Reset** button, all the Address Maintenance fields, logs, and files are cleared.

   During validation, the **Begin Validation** button changes to **Pause Validation**, and the **Reset** button to **Cancel Validation**.

   If you click the **Pause Validation** button, it pauses the process at the current record, and the button changes to **Resume Validation**. By clicking this button, you can resume the process, unless you want to cancel it by clicking the neighboring **Cancel Validation** button.

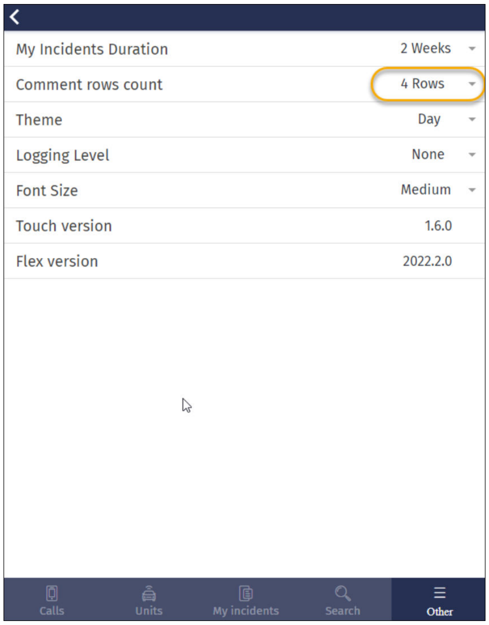
12.3 Touch

12.3.1 New Setting for Call Comments

The new setting allows you to choose the number of rows that a comment takes on the screen of your mobile device.

You can configure the setting in the Touch application by tapping **Settings** → **Other** → **Comment rows count**, and selecting the number of rows.

Figure 306: Comment Rows Count Setting



In the figure, the value of the setting is framed yellow. You can select 2, 4, 6, 8, 10, or 12 rows.

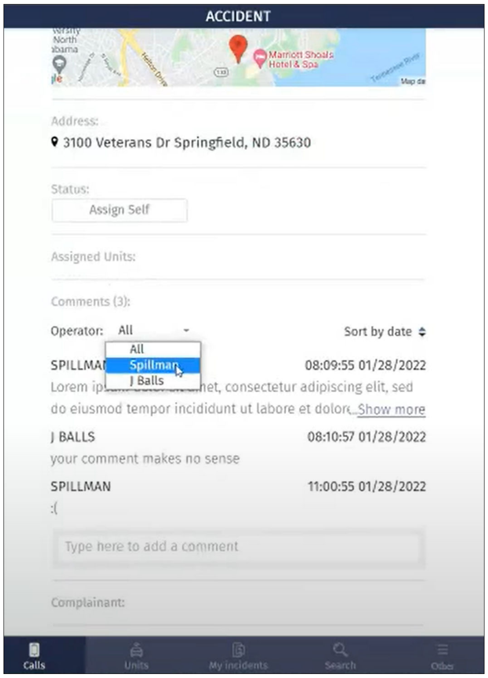
12.3.2 Filtering Capability for Call Comments

You are now able to filter comments in the Touch application.

You can perform filtering of comments by selecting a name in the **Operator** drop-down list. Only comments from that person will appear on the screen. The **All** option means no filtering.

If a comment is longer than the set rows count, you can view the whole content of the comment by tapping **Show more** at the end of the last displayed row.

Figure 307: Call Comments Filtering Options



Chapter 13

Release 2021.4

This chapter presents changes made to Flex for the 2021.4 release.

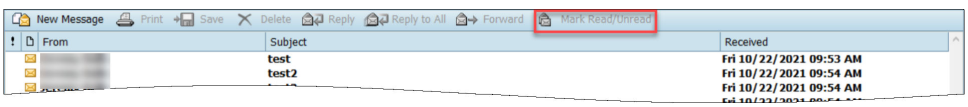
13.1 Mobile

13.1.1 Ability to Mark a Message as Read or Unread

This functionality was added to help the users keep track of the messages they want to read again.

You can mark a message with the **Mark Read/Unread** button on the toolbar. In the following figure, the button is marked with a red frame.

Figure 308: Mark Read/Unread Button



Features of this functionality

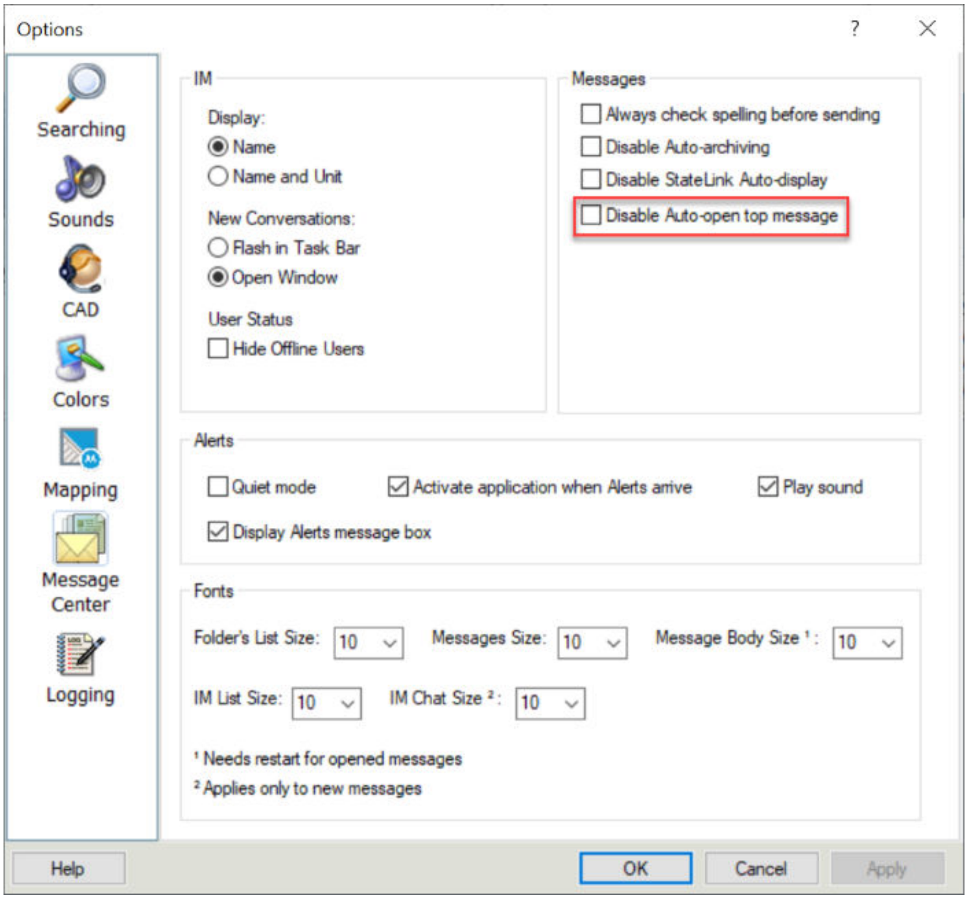
- Mark Read/Unread is available with Messages and Local Returns
- Multiselect option is currently not supported

13.1.2 Option to Disable Auto-Open Top Message

After opening Message Center, it automatically selects the first message and marks it as read.

This behavior can be changed by selecting in the **Messages** pane the **Disable Auto-open top message** check box. In the following figure, the check box is marked with a red frame.

Figure 309: Disable Auto-Open Top Message Option



When the **Disable Auto-open top message** option is selected, the message will **not** be marked as read until you select the message.

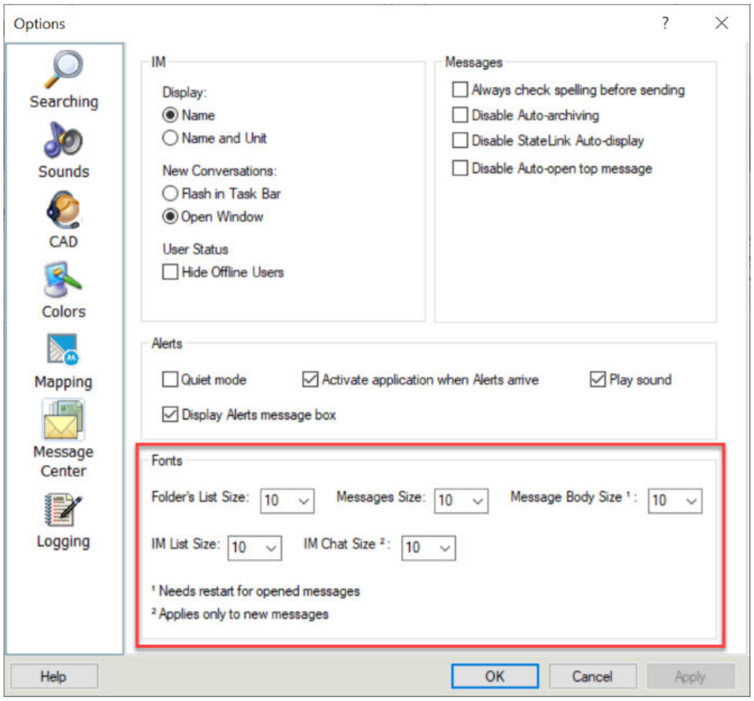
13.1.3
Adjusting the Font Size in the Message Center

Some users have reported that they have problems with reading information because of too small fonts. The problems can now be eliminated by increasing the font size for each section in the Message Center.

Procedure:

1. From the Flex Message Center, select **File** → **Options** → **Message Center**.

Figure 310: Fonts Pane with Font Size Adjustment Fields



2. Select the required font size for any section listed in the **Fonts** pane.

   The default size is 10, which is the minimum size. The available size range is 10–22.
3. After selecting the font size for some or all sections, click **OK**.

13.2
Jail

13.2.1
Jail Enhancement with Group Intake

The CommandCentral Jail software has been enhanced to include the ability to move inmates as a group.

Group Intake Features

- Intake of multiple inmates as a group, instead of individuals
- All selected inmates must initially be moved to the same location
- Validation of movement restrictions and separation rules
- Ability to set single intake type, officer, arrival time and arrival credit for the group

13.2.1.1
Using the Group Intake Feature

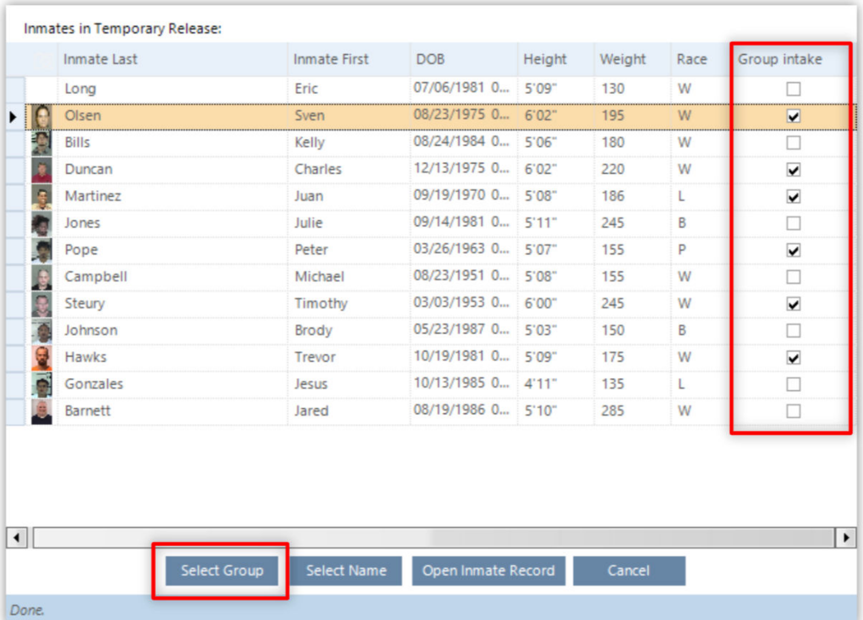
After successful completion, movement screen opens with all inmates in the group selected for movement or return to housing.

Procedure:

1. From the Jail main menu, select **Intake and Release** → **Intake**.

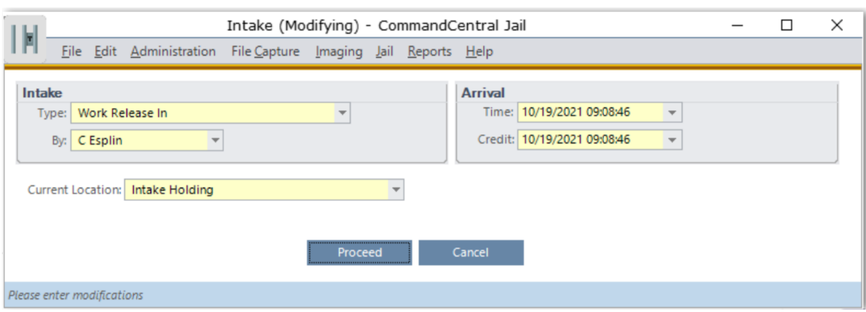
2. In the **Group intake** far right column, choose all inmates you want to include in the group intake by selecting the relevant check boxes.

Figure 311: Selecting Inmates for a Group Intake



3. Click **Select Group**.

Figure 312: Intake (Modifying) Window



The **Intake (Modifying) - CommandCentral Jail** window opens.

4. If needed, adjust values in the **Intake** and **Arrival** panes.
5. Click **Proceed**.

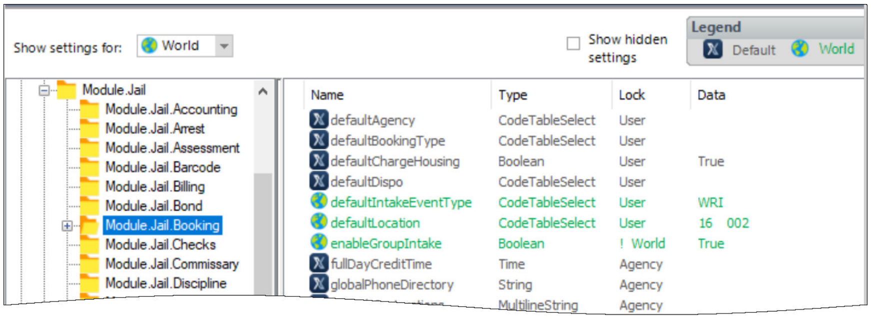
   The movement and *keep separate* restrictions are validated. If the validation passes, a movement window opens. If the validation does not pass, a window indicates a movement or a *keep separate* restriction error.

13.2.2 Admin: New Setting for Enabling Group Intake

The new `Module.Jail.Booking.enableGroupIntake` setting allows agency administrators to enable the Group Intake feature. By default, the value of the setting is set to `False`. As an administrator, set it to

True to enable this feature and the related interface elements: the column for Group Intake check boxes, and the **Select Group** button.

Figure 313: The enableGroupIntake Setting in the Module.Jail.Booking



Chapter 14

Release 2021.3 Update

This chapter presents additional changes made to Flex for the 2021.3 release. For enhancement information, see Release 2021.3 on page 301.

14.1

StateLink

This section lists the issues resolved for StateLink.

Table 45: StateLink Update Resolutions

Issue	Issue Resolved
California - LA County. Cannot enter in alpha values in license plate year field on EVS screen. SL-6852	Users can now enter alpha values in the license plate year field on the EVS screen.
Indiana - License Plate Year (LIY) fields need to allow for NX for non-expiring registrations. SL-6831	Added in an extra condition for License year that checks if the value is NX first.
California - Imperial County. There is a typo on the StateLinkCA property page spelling Encryption as "Ecryption". SL-6816	This issue has been resolved.
California - San Bernardino, If you enter (via mobile) a license plate less than 7 characters, it appears that the license year becomes part of the license plate. SL-6729	Solved by padding the license plate if it is in state and is less than 7 characters, and throwing an error if greater than 7.
Wisconsin - For vehicle registration returns where the plates are owned by a dealership, owner detail does not import to CAD call comments. SL-6661	Added owner detail for company-owned plates in the text record parser for RQ responses in Wisconsin.
New York - Not all fields on the DriversLicenseInquery are being parsed. SL-6637	Fixed by parsing additional fields from the original XML response.
Indiana - out of state DQ returns script Error. SL-6536	Added validation for a purpose code on NLETS transactions.
Indiana - Name Search for out-of-state Driver License queries required Name with Driver License when Driver License should be sufficient. SL-6535	Validation was updated to ensure the correct options were being checked (OLN; or NAM, DOB, SEX).
Ohio - DQP generating null jpgs and continued to store them in a Spillman directory. SL-6530	Added a null check before writing an image to disk. The null images will no longer collect in a Flex directory.
Ohio - When StateLink is not able to bind to the state server's port, it continues without shutting down or restarting and fills the logs. SL-6441	The Ohio Protocol Interface checks whether a bind error occurred when attempting to bind the socket to a defined port on the state's server. If the sock-

Issue	Issue Resolved
	et cannot bind, the StateLink application closes and must be restarted.
Ohio - StateLink handled bad image responses from New Jersey incorrectly which caused future returns from the state to be blocked. SL-6371	This issue has been resolved by handling the bad image return correctly and acknowledging the response from Ohio.
Idaho - Address on some queries is not importing into Flex. SL-6350	Issue resolved, fixed the queries that were not importing the address.
Texas - The purpose code in the query caused problems with the RSDWW transaction. SL-6119	Removed the sending of the purpose code in the RSDWW transaction.
Wisconsin - Mixing some state responses with NCIC results. SL-5840	The issue has been resolved by reading the header correctly for multi-record returns.

14.2
Mapping

This section lists the issues resolved for Mapping.

Table 46: Mapping Update Resolutions

Issue	Issue Resolved
WMS services will not load in mobile map. MAP-1871	This issue has been resolved
Closing call screen with Geovalidation window open causes errors. MAP-1848	This issue has been resolved.
Uploaded AVL Icons not displaying on CAD/Mobile Map. MAP-1847	The issue has been resolved.
Locking Mobile with the map open causes it to not open when you unlock. MAP-1840	This issue has been resolved.
Mobile Map randomly crashing on startup. MAP-1832	This issue has been fixed.
Closures time would change after choosing dates.MAP-1822	This issue has been resolved.
Mapping does not allow multiple 911 tokens for multiple agencies on the same server. MAP-1813	E9-1-1 Notification API Token field on the properties page of the Mapping web application now can accept multiple agency-token pairs in order to support multi-PSAP setups. Tokens for agencies must be specified in the following format: agency1=token1;agency2-token2. For single-PSAP setups just a token must be specified.
When adding a call it might show incorrect cross streets when the Disablegbaddrupdatetime is true. MAP-1799	This issue has been fixed.
Devices which report GPS data too often can overwhelm the database / server and cause issues. MAP-1769	This issue has been fixed.

Issue	Issue Resolved
The Flex Mobile Map and Flex CAD Map (web) do not honor the Module.CAD.MobileCADFilter setting. MAP-1427	This issue has been fixed.

14.3
Records

This section lists the issues resolved for Records.

Table 47: Records Update Resolutions

Issue	Issue Resolved
Reopen a NJ Citation report that was submitted to the state will overwrite the unit code with the officer who opens it. LAW-1794	Once a ticket is submitted to the state and someone reopens the ticket, the unit code will remain to be the original officer who submitted the ticket.
Users are able to modify law incident records in agency partitioning when they only have the access permission to the incidents in the agency partitioning. LAW-1788	Users' partition permission to the law incidents are honored such that they cannot modify the law incident records and the involvements without the modify permission.
Push to command central using up synxtids when handling invalid transaction messages. LAW-1778	Egress transform and push to CommandCentral changes were made to avoid the synxtid skipping issue.
The Traffic Violations Bureau Address is not populated on the 2020 OH Citation form. LAW-1772	The enhancement is made to allow the court address to be populated with the appropriate translation admin mapping change.
Users receive the submission errors from the state sporadically when the DOB of the person is greater than the crash date. LAW-1771	We fixed the DOB format to be passed to the broker server per the state required format.
Glasses field in state link return is not translated when importing statelink return to Flex. LAW-1767	Updated the translation admin to allow agencies to map the Flex value with the state glass value.
NJ transit and NJ state police can't submit citations because the state expects a different agency ID for the court system. LAW-1760	Changes were implemented to enable statewide agencies to pass the correct agency ID upon the citation eSubmission.
Non-custody screen is not showing workflow options. LAW-1753	We resolved the layout issue to allow the workflow fields to be shown on the non-custody screen.
Users receive the state submission error due to the field sobriety character limit issue with the UT citation/DUI. LAW-1734	Fix the issue of the extra XML markup so users can submit the citation with the field sobriety narrative up to 3000 characters.
The NCIC number is only populated on the first page of the California crash form but not other pages. LAW-1709	Populate the NCIC number when the form is initially loaded.

14.4
Jail

This section lists the issues resolved for Jail.

Table 48: Jail Update Resolutions

Issue	Issue Resolved
ONVIF Camera fine movement for one pixel moves too far. JAIL-6825	Adjusted the calculation to closer reflect a single pixel worth of movement for ONVIF cameras.
Resolved an issue where the system menu may not populate correctly. JAIL-6812	This issue has been resolved.
Resolved an authentication issue when trying to connect to an Avigilon H5A camera. JAIL-6809	Fixed an issue that caused authentication to fail when using the ONVIF profile S connection protocol.
Resolved an issue where CommandCentral Jail crashes when closing the adminutil screen while having a Jail module screen open. JAIL-6792	This has been fixed.
The client can crash shortly after logging in. JAIL-6784	This issue has been resolved.

14.5
Interfaces

This section lists the issues resolved for Interfaces.

Table 49: Interfaces Update Resolutions

Issue	Issue Resolved
Customer wants to be able to map messages in all vendors. IF-3917	Enable Custom Message Mapping for Broadcast Group, Pre-Alerts, Vesta vendors.
Intellicomm not using tbnatur.calltype when importing case updates. IF-3846	This is fixed so that when the Incident is modified due to options provided on APCO interface the callType will also get updated.
Rapid Notifications did not support email integration with Office 365. IF-3840	Added additional checkbox **Use SSL for SMTP for all SMTP vendors**. This should be unchecked in case of using Office365 e-mail accounts.
After importing ripnrun configuration data calls are creating a large amount of duplicate messages being sent to the same recipient. IF-3815	"Duplicates" were only a perception. It was due to multiple units being assigned the same SMTP address. The interface logic was adjusted to make sure to only send one message per SMTP address instead of one message per Unit.
Rapid Notification 2.0 Audit Logs not showing in application manager. IF-3806	Skip the malformed audit file and write error to the logs.
Rapid Notification Web app crashes with "Not Enough Memory to Load' error. IF-3749	Implemented pagination for all kinds of recipients and groups (BroadcastGroup, RapidNotification, Pre-Alerts, RuntimeReports, Vesta vendors).
Instead of updating "Transaction Log Position" manually, We automated the process. IF-3377	Updating the Transaction Log Position field to "now"

14.6
IBR

This section lists the issues resolved for IBR.

Table 50: IBR Update Resolutions

Issue	Issue Resolved
LA-IBR User can't use '90I' and can't fix validation error for using14:67 with 23G. IBR-3640	This issue has been resolved.
OK-IBR does not report Group B only incidents. IBR-3634	This issue has been resolved.
NJ-IBR The user can't fix NJ815.48 validation error. IBR-3633	This issue has been resolved.
OK-IBR The 06 - Lovers' Quarrel is not correct in 'Assault Homicide Circumstances'. IBR-3632	This issue has been resolved.
NY-IBR missing none loss property record with a 220 and 290 offense and only damaged property involvement. IBR-3622	This issue has been resolved.
WV-IBR throws error on multiple drug property records having the same drug type. IBR-3619	This issue has been resolved.
Clery Audit/Annual do not match for Criminal Arrests, Disciplinary Action, and Criminal Offenses. IBR-3618	This issue has been resolved.
Clery Bias Motivation field showing when isClery is not checked. IBR-3617	This issue has been resolved.
NJ-IBR User can't fix validation error 065 and 075 for the incident with Group B offense only. IBR-3609	This issue has been resolved.
NJ-IBR error NJ808.2 given when State Police select any Municipality besides 2200. IBR-3603	This issue has been resolved.
IL-IBR User can't fix the Group B arrest validation error on address fields. IBR-3596	This issue has been resolved.
OK-IBR The narratives are not recorded in the submission. IBR-3590	This issue has been resolved.
OH-IBR User can't fix DE_20.81 error when the property exists for 90Z. IBR-3582	This issue has been resolved.
IL-IBR User can't fix the statute validation error in IBR. IBR-3569	This issue has been resolved.
OK-IBR No valid date check on OK-IBR Incident Occurred To value allowing future dates to submitted in error. IBR-3567	This issue has been resolved by adding a valid date check that prohibits future dates to the Incident Occurred To date value.
TN-IBR The Domestic Violence field does not show for victim to offender codes XC and XR. IBR-3566	This issue has been resolved.

Issue	Issue Resolved
OH-IBR User can't resolve IL_1.a and DE_40f validation error when using 2919.22 statute. IBR-3565	This issue has been resolved.
KS-IBR Domestic Violence getting error K211a and occurred time of 00:00:00 giving state error. IBR-3561	This issue has been resolved.
OK-IBR User received XSD Failure: Element "FBINum" error. IBR-3559	This issue has been resolved.
IL-IBR not allowing different statutes tied to the same offense code. IBR-3557	ILIBR will be allowing different statutes tied to the same offense code with the change done for this task.
SC-IBR An exception was thrown while confirming an IBR report that caused the confirm to fail. IBR-3554	Additional data validation was added to prevent errors.
NY-IBR The user can't fix NY_176 when the Exceptional Clearance Date is used. IBR-3553	This issue has been resolved.
OH IBR - DE_40.TG error needs to be revised for a couple situations. IBR-3551	Keep this error message as it is as it may impact proper entry of the data if it is not applied.
NJ-IBR vehicle make and model throwing IBR errors that can't be fixed. IBR-3548	This issue has been resolved.
NJ-IBR Some IBR Error messages contained victim to offender relationship of XR. IBR-3547	XR has been removed from error messages as it is not supported by NJ which supports NIBRS 2017.
OK-IBR Cannot validate incident with 240 and 120 offenses. IBR-3545	This issue has been resolved.
NY-IBR arrests are valid but not reported when they are not linked to the incident. IBR-3541	This issue has been resolved.
NY-IBR Get various IBR errors from the state upon IBR submission. IBR-3539	This issue has been resolved.
MO-IBR User received property errors (b_306_descr) from submission. IBR-3538	This issue has been resolved.
IL-IBR If there is a troff record without a corresponding tboff record submission with fail. IBR-3537	Fixed the statute upload logic to consider this scenario.
NY-IBR The User can't fix NY_690 validation error. IBR-3536	This issue has been resolved.
NY-IBR throws NY_790 error on Time Window incident. IBR-3534	This issue has been resolved.
OH-IBR user can't fix validation error when there are 2921.33 and 2921.331A offenses. IBR-3533	This issue has been resolved.
OH-IBR Users get validation errors when the Eye, Hair, and Height info are not provided. IBR-3532	This issue has been resolved.
OH-IBR Users can't use statute correctly in some cases. IBR-3531	This issue has been resolved.

Issue	Issue Resolved
CA-IBR The assault/homicide circumstances dropdown was not displaying the CA specific values. IBR-3529	We were loading the NIBRS version of this table, when we should have been loading the CA version. This was changed.
OH-IBR users can't resolve DE_20.e validation error. IBR-3526	This issue has been resolved.
OH-IBR The error 601.4 received from the submission. IBR-3522	This issue has been resolved.
NE-IBR The user can't fix NE_604.2 validation error. IBR-3518	This issue has been resolved.
NY-IBR User can't upload the NY laws Excel file. IBR-3517	This issue has been resolved.
CA-IBR The arrest offense screen was showing the offense values instead of the statute values. IBR-3513	Updated the arrest offense screen for CA to display the statute values instead of the offense values.
OH-IBR Received Unknown Offender relationship error from submission. IBR-3507	This issue has been resolved.
OH-IBR State getting errors from addresses with aliases. IBR-3506	This issue has been resolved.
OK-IBR Not allowing 80 series offenses with criminal offenses. IBR-3505	This issue has been resolved.
OH-IBR The IBR offense is blank after offense is changed in law. IBR-3502	This issue has been resolved.
AL-IBR Synopsis report is not working for AL state. IBR-3498	Synopsis report is fixed for AL state.
NJ-IBR Users received "Server Error" in arrest validation for Group B offense with additional victim. IBR-3492	This issue has been resolved.
CA-IBR When an incident has exceptional clearance, validation is not recognizing race code 1-9. IBR-3488	This issue has been resolved.
SC-IBR Users can't correct SC_104.1 and SC_207.1 validation errors. IBR-3487	This issue has been resolved.
OK-IBR submission error for Unidentified ID. IBR-3485	This issue has been resolved.
Clery Campus and General Location required for save if Location is filled in. IBR-3482	This issue has been resolved.
NJ-IBR Domestic Violence in IBR not allowing users to fill in victim to offender relationship. IBR-3480	This issue has been resolved.
AL-IBR An Arrest is required on any incident with a Case Disposition of 'Cleared by Arrest'. IBR-3479	Added the validation: Arrest is required on any incident with a Case Disposition of 'Cleared by Arrest'.
Clery Bias not showing for Clery offenses on Offense screen. IBR-3476	This issue has been resolved.

Issue	Issue Resolved
NV-IBR reported arrest charge does not have a matched NV Offense Code. IBR-3474	This issue has been resolved.
OK-IBR Generate Report fail when guardian has letter in name number. IBR-3473	This issue has been resolved.
TN-IBR The TN23 and TN24 have Empty Link and Blank message. IBR-3470	This issue has been resolved.
There was no way to enter credentials for multiple agencies on the state IBRProcessor webpage. IBR-3468	This functionality was moved to the Flex client. The client will now prompt for the username/password info at the time of agency validation, so it will be agency specific info, which will not be stored anywhere.
GA-IBR Users received FVF-45-00 and FVF-46-00 errors from state submission. IBR-3463	This issue has been resolved.
Getting server error when validating IBR. IBR-3462	This issue has been resolved.
Incidents having occurred date of first second on first day of the month are appearing in the previous months IBR report. IBR-3454	This issue has been resolved.
CO-IBR Errors from state 648_CO and 701 when submitting file. IBR-3451	This issue has been resolved.
WV-IBR throws 704.45 and 760 errors when validating arrests. IBR-3438	This issue has been resolved.
AL-IBR The error message for error check AL154.9 has been fixed. IBR-3431	The error message for error check AL154.9 has been fixed.
AL-IBR misc2 is not updated by the statute update tool if the misc2 field is modified. IBR-3430	Fixed the issue statute upload tool logic to update misc2 field every time NIBRS code is changed.
The arrest display is not the same when validating agency more than one time. IBR-3420	This issue has been resolved.
WA-IBR Exceptional Clearance and its date is getting blanked out in IBR data. IBR-3415	This issue has been resolved.
Arrest Circumstances not transferring to IBR Arrest Weapons collection. IBR-3376	This issue has been resolved.
PA-IBR Bad checks not getting Classified as fraud in the UCR reports as it should. IBR-3041	This issue has been resolved.

14.7 Administration

This section lists the issues resolved for Administration.

Table 51: Administration Update Resolutions

Issue	Issue Resolved
If a user with an underscore in their username logs into Touch2, calls fail to load for Touch2	This issue has been resolved.

Issue	Issue Resolved
users and Flex Map users until the Mobile webapp is restarted. HUB-3504	
The active directory webapp fails to establish a connection of ldaps. HUB-3485	In some scenarios the active directory webapp can fail to establish a connection using ldaps to the Active Directory server. This issue has been resolved.
Certificate Manager - a warning message about expiration for the Flex Server Certificate is not sent by mail. HUB-3422	Fixed notifications about certificate expiration of the server certificate.
Flex Command windows vertical size is not saved between sessions. HUB-3401	The issue has been resolved.
Flex Server Diagnostic Tool can't be accessed on port 4443. HUB-3388	The Flex Server Diagnostic Tool is now configured so it can be accessed on port 4443.
Usernames over 15 characters cannot log into cad due to cdassign error. HUB-3383	This issue has been fixed.
Using 2 monitors with different resolutions could result in drop down selections to appear in a different location than expected. HUB-3369	Window maximize was fixed as well since it is related issue. Now maximize works correctly for summit screens on second monitor.
Data Replication Tool can stop replicating if its SQL connection gets terminated. HUB-3360	Data Replication Tool automatically establishes a new SQL connection if it gets closed for some reason.
Maint: update javascript libraries with reported vulnerabilities in scan. HUB-3359	Updated Angular libraries.
Spinning Circle upon opening empty involvement list. HUB-3357	If there are no records in the table, we get an error and stopping the spinner does not work. Problem fixed.
Implemented new type encrypting password for Active Directory. HUB-3355	Implemented new type encrypting password for Active Directory.
InSight server has a memory leak. HUB-3344	In some conditions, InSight will not release memory leading to an out of memory error. This issue has been resolved.
Reports no longer taking focus during the preview. HUB-3303	The issue has been resolved.
If a user belongs to more than 32 groups not all the privileges are honored. HUB-3283	This issue has been resolved.
Unable to upload files through the Flex help in webapp manager. HUB-3183	Removed unnecessary step in the creating file. Issue was resolved.
The datareplication tool was not sending emails for errors that were showing up on the webapp error view. HUB-3180	Fixed sending emails with errors in DataReplicationTool.
When adding an involvement, Use control puts list to background. HUB-3082	This issue has been fixed.

14.8
CAD

This section lists the issues resolved for CAD.

Table 52: CAD Update Resolutions

Issue	Issue Resolved
When using an alarm in the call taker screen an address may not be validated correctly if it contains a prefix. CAD-4816	This issue has been fixed.
CAD Incident comments are not updating when ActiveMQ lost connection for the SSL connection. CAD-4793	The issue has been resolved.
Opening traffic stop incident without specified address causes screen to be in invalid state. CAD-4790	The issue has been resolved.
In the CAD Incident screen, the How Received field does not honor e911 data. CAD-4787	The issue has been resolved.
CAD Incident screen window crashes intermittently when trying to load recommendation plan. CAD-4786	Fixed CAD incident window crash.
In the CAD Incident screen, the address field loses geovalidation mark when switching between tabs. CAD-4765	The issue has been fixed.
The CAD Incident Address reverts while switching between discipline tabs. CAD-4764	The issue has been resolved.
The CAD system does not find a response plan in the last valid minute. CAD-4760	The issue has been resolved.
The Call priority is changed on the discipline tab of the CAD Incident screen after switching between tabs. CAD-4739	The problem has been resolved.
After encountering an error in the CAD incident screen, calls can no longer be created or modified. CAD-4734	This issue has been resolved.
Address in CAD Incident screen can be reverted if two users are working on the same call simultaneously.	This issue has been resolved.
When Reported value could be missing if specifying an address via the quick command. CAD-4731	This issue has been resolved.
In the CAD Incident screen, while adding an E type to LF call caused data corruption. CAD-4698	This issue has been resolved.
Outgoing CAD2CAD XML does not format the call taker name field properly. CAD-4694	This issue has been resolved.

Issue	Issue Resolved
The XA command is not working from the CAD Command line. CAD-4691	The issue has been resolved.
The CAD Incident Screen created from traffic stop based on invalid demographics values doesn't allow to edit them. CAD-4685	The issue has been resolved.
Unsuccessful call update causes CAD server cache getting out of sync and other caching issues on new call screen for users logged into the CAD later. CAD-4681	The issue has been resolved.
Dispatcher unable to modify empty address field of traffic stop incident in case when it was created without specified address. CAD-4678	The issue has been resolved.
Traffic stops without an address are not getting a zone assigned. CAD-4675	This issue has been resolved.
The mobile cache cap fails to be enforced causing performance issues. CAD-4662	The mobile options.xml NovoCacheCapSize setting sometimes fails to be honored causing excess records in msmain and msdata which leads to performance issues in the mobile client. This issue has been resolved.
License plate querys can't be run from discipline specific call comments due to extra spaces being inserted in the text selection. CAD-4659	This issue has been resolved.
Searching for names alerts in the CAD Incident Screen can cause slowness. CAD-4653	This issue has been resolved.
For the ECW/Flex CAD ICC, the Remember Me feature wasn't supporting the storing ECW credentials for multiple Flex users if working under the single Windows user account. CAD-4648	The problem has been resolved.
When a dispatcher opens the call with empty address it is sometimes populated with other call's address. CAD-4644	This issue is resolved.
In the CAD Incident screen, the Phone Number field populated with extra digits cannot be changed. CAD-4643	On the server side, returned the division into number and extension, when fixing the problem CAD-3713 everything was combined into a number. On the client side, added the ability to display and edit extension.
Memory usage of the FlexClient process continues to grow when using the CAD incident screens. CAD-4640	This issue has been resolved.
The responding units may disappear from the CAD incident screen. CAD-4634	This issue has been resolved.
Flex CAD makes an unencrypted connection to the ActiveMQ service. CAD-4627	A standard Flex patch will resolve this. If a patch is not available or cannot be completed, a new Novo.zip and Cad.war will be necessary. Along with this, you will need to update a stunnel-session.conf file and the activemq.xml file and restart both Stunnel and ActiveMQ.

Issue	Issue Resolved
The CAD incident screen gets disabled after CAD Mobile locks up. CAD-4625	The issue has been resolved.
The CAD system becomes unresponsive, CAD calls can't be accepted or dispatched. CAD-4621	The issue has been resolved.
In the CAD Incident screen, the zone field becomes read only after city change and resetting geovalidation of the address. CAD-4617	The issue has been resolved.
Slowness in Call Taker Screen can occur when there are a lot of expired codes in code tables. CAD-4613	This issue has been resolved.
The record selector screen visually extends beyond the columns on radio list screen. CAD-4611	The issue has been resolved.
There is "No response plans found" message when a user verifies existing response plan. CAD-4610	The issue has been resolved.
Occasionally, more than one vehicle record per cad call is being inserted into the cdinvveh table, which prevents the call from being dispatched. CAD-4606	The issue has been resolved.
Dispatcher cannot change incident address using MC command if zone assigned to a new address is not in tbzones table. CAD-4605	This issue has been resolved.
Flex CAD occasionally stops responding when completing call. CAD-4599	The issue has been resolved.
DC CAD Command Intermittently going to Classic Call Screens instead New CAD Incident screen. CAD-4464	The issue has been resolved.
Sometimes the CAD Incident screen displays long term and short term call numbers incorrectly. CAD-4463	The issue has been resolved.
In the New CAD Incident screen, the phone number field intermittently disappears instead of being saved. CAD-4440	This issue has been resolved.
In the New CAD Incident screen, the blank call comment screen appears intermittently. CAD-4433	This issue has been resolved.
The incident history tab could show an incorrectly sorted list of incidents for a given address. CAD-4407	The incident history tabs now show the most recent incidents according to date reported.
In the New CAD Incident screen, a user was able to see only natures for one discipline while running the MT command. CAD-4389	The issue has been resolved.
In the New CAD Incident screen, the AT CAD command doesn't populate zone field automatically. CAD-4333	The issue has been resolved.

Issue	Issue Resolved
The Back and Forward buttons on the list screen for Radio Log History, are incorrectly being disabled. CAD-4242	The issue has been resolved.
For the Alarm tracking, the rpatfsr.x1 report is showing "[NO V" in the Fee field if there are no Law or Fire fee types in the attbfeet table. CAD-4202	The issue has been resolved.
In the New CAD Incident screen, a user is unable to update zone for the traffic stop incidents if originally assigned zone is invalid. CAD-4154	The issue has been resolved.
Potential CAD Incident duplicates being partially detected and then preventing users from accepting a CAD incident. CAD-3548	The problem has been resolved.

14.9

Mobile/Touch

This section lists the issues resolved for Mobile and Touch.

Table 53: Mobile/Touch Update Resolutions

Issue	Issue Resolved
Database context will be removed after strict rules. APPS-892	1. If this context was created more one hour ago, it will removed. 2. If the pool of database context for Touch2 increases over allowed on 0.8 (72*0.8=57), it will removed.
Touch/WEB: file attachments with unreadable symbols. APPS-883	From the Touch Web version side: If the file has one of the next extensions: .doc, .docx, .xls, .mp3, .mp4, .wav., after a click on one of them that file will be automatically downloaded on the user PC.
Pasting into the comments field removes any typed text. APPS-864	Fixed incorrect logic in the paste process.
Touch2 performance problem when on a server with lots of involvements and searching incidents. APPS-863	This issue has been resolved.
Searching in Touch2 causing ctree to nearly exhaust CPU. APPS-786	Removed 'syinvolv' query from the call detail screen.
Touch2 app stops displaying call details after 30 minutes of inactivity. APPS-565	Removing unnecessary database context. issue has been resolved.

Chapter 15

Release 2021.3

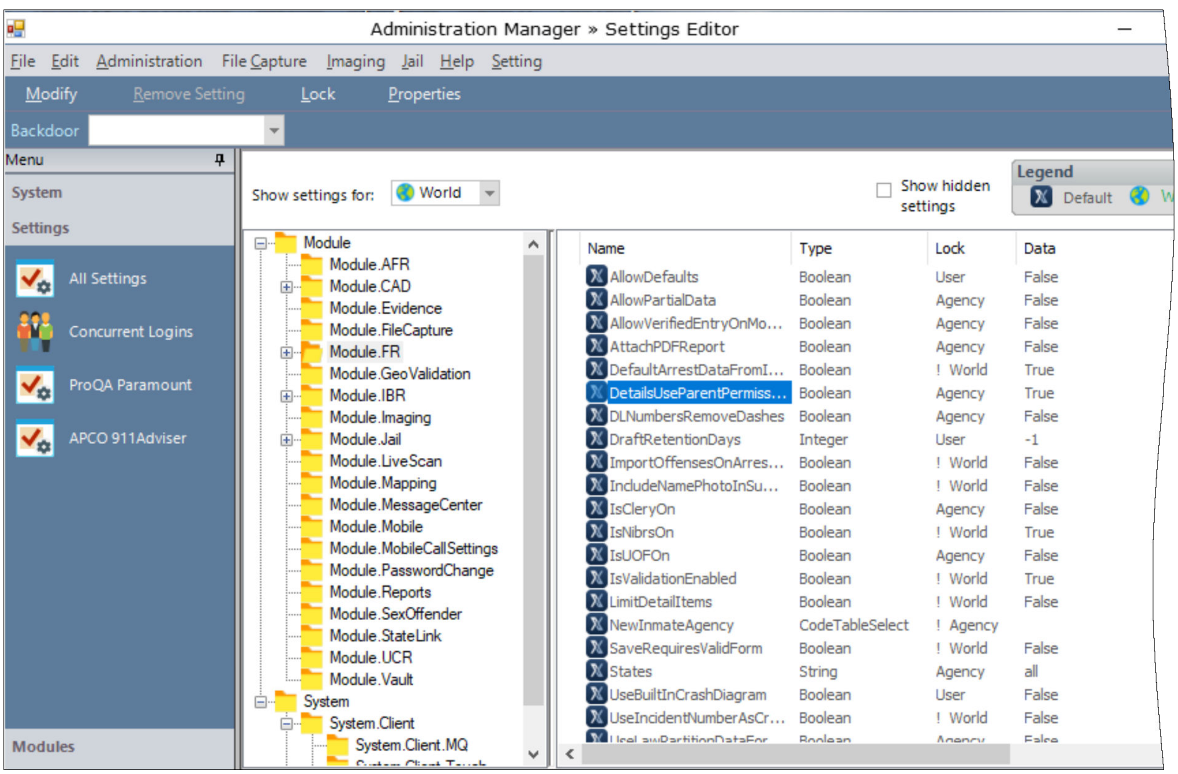
This chapter presents changes made to Flex for the 2021.3 release.

15.1 Records

15.1.1 (Admin) RMS: New Setting for Enabling Detail Controls of Mobile Screens Based On Detail Table's Partition

The new `Module.FR.DetailsUseParentPermissions` setting allows agency administrators to decide if users' privilege to any detail table should follow their privilege to the parent tables or not. By default, the value of the setting is set to `True`, so a user's privilege to any detail table on mobile screens is based on the user's privilege to the related parent table. If the agency administrator sets the setting to `False`, then the users are able to manage the partition of the parent and the related detail tables separately. This functionality is now available in the 2021.1 and newer releases.

Figure 314: The Module.FR.DetailsUseParentPermissions Setting



15.1.2
(Admin) RMS: New Setting for Read-Only Access to Incident Screens with Agency Partitioning

The new `System.Client.PartitionedIncidentsReadOnly` setting allows administrators to decide if users from an agency who do not have the Modify permission to another agency's law incident records with agency partitioning can only read the other agency's law incident records in the agency partitioning in Flex and Mobile, and cannot modify the law incident records and involvements. By default, the setting is set to `False`, which means that the read-only limitation is inactive.

The introduction of this limitation is associated with changes to the relevant screens. The changed screens are: Flex involvement screens, Field Incident Reporting screens in Mobile, IBR Incident screen in Mobile. These changes are applicable to 2021.2 (beginning with the build released July 27, 2021) and newer releases.

15.2
Jail

15.2.1
Jail Application Enhancement with Inmate Movement Feature

The CommandCentral Jail application has been enhanced to include the ability to move inmates by scanning barcodes on their wristbands and scanning a location, or selecting to return the scanned inmates to their assigned housing location.

Features of the CommandCentral Jail Application

- Scan location barcodes as rounds are completed
- Scan bed barcode when performing cell checks and note the inmate status and capture notes
- Manage inmate movement (introduced in the 2021.3 release)
- Native Android application

NOTE: This document describes the inmate movement feature. For information about the other features see the *Flex Release 2021.2*, *CommandCentral Jail Management Administrator Manual*, and *CommandCentral Jail Management User Manual*.

Requirements

- Wi-Fi connection to log in and upload completed scans
- Datalogic barcode scanner: Memor 10 or Memor 20

15.2.1.1
Managing Inmate Movement

Using a barcode scanner you can easily move record of the inmate from one location to another so the inmate's location is always up to date.

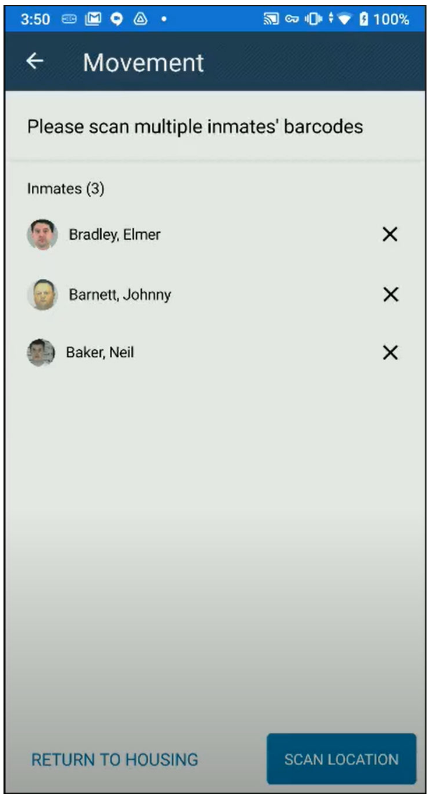
Procedure:

1. On the CommandCentral Jail main menu screen, select **MOVEMENT**.

   The **Movement** screen appears and the scan mode activates.

2. Scan barcodes of all inmates who are ready to be moved.

   Figure 315: List of Inmates to be Moved

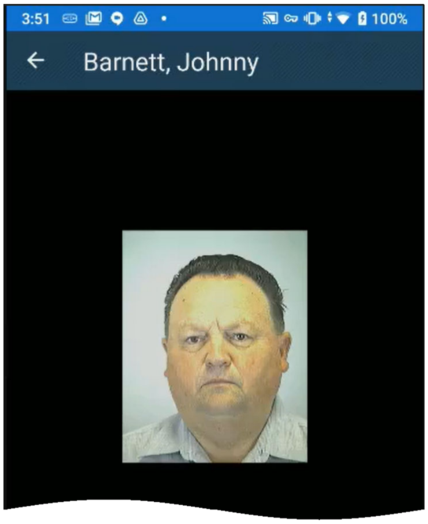
   

   A list of the inmates' names appears on the screen, with a thumbnail photograph to the left of each name.

   NOTE: Thumbnails only show if the scanner has a network connection when the scan is completed.

3. Optional: To see the full-size photograph of an inmate, tap the relevant thumbnail.

Figure 316: Full-size Photograph of a Selected Inmate



To return to the list of inmates, tap the back arrow next to the name, or use the device back button.

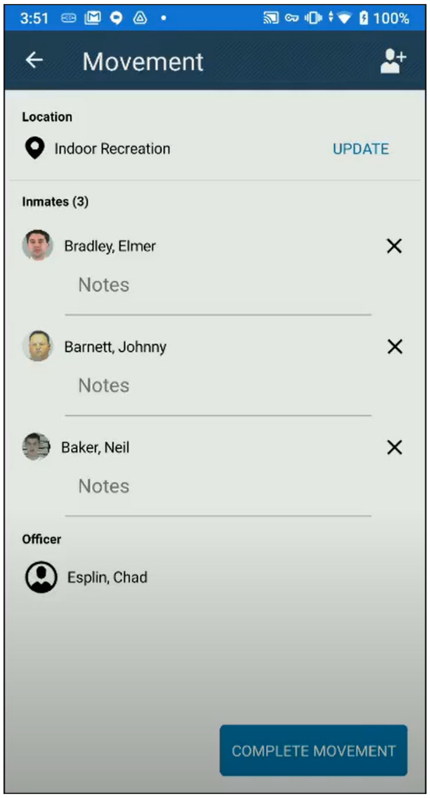
4. To move the inmates in the list to a new single location, select **SCAN LOCATION**, and scan the barcode of that location.

   The **RETURN TO HOUSING** option to the left of the **SCAN LOCATION** tab returns all inmates to their assigned housing location.

5. On the screen showing the new **Location**, verify the list of the inmates and optionally add notes to some of their names.

   If the location is not correct, you can change it by tapping the **UPDATE** button and scanning another location.

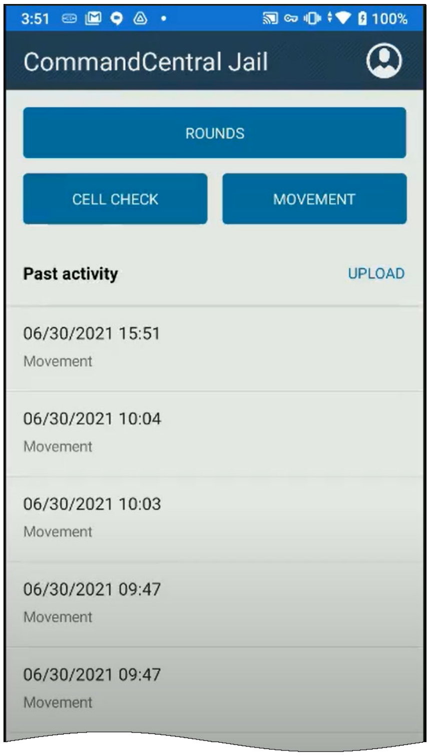
Figure 317: The Target Location with the List of Inmates



6. Tap **COMPLETE MOVEMENT**.

   Once a scan record is saved to the server, it is no longer viewable on the device. The date and time of the completed Movement appear at the top of the **Past activity** list (see the following figure).

Figure 318: Main Menu Screen with the Past Activity List



NOTE: The scanner requires a Wi-Fi connection to both log in and to upload the movement. If the device does not have a Wi-Fi connection, the activity is stored on the device until there is a Wi-Fi connection available. You can attempt to upload any activities that are stored on the device and have not been uploaded to the server by tapping the **UPLOAD** button.

7. Optional: To review any Movement item from the **Past activity** list, tap the item you are interested in.

   The **View activity** screen opens. In the case of a Movement, the information includes the OFFICER, LOCATION, DATE and TIME data, and the list of inmates.

15.3 Touch

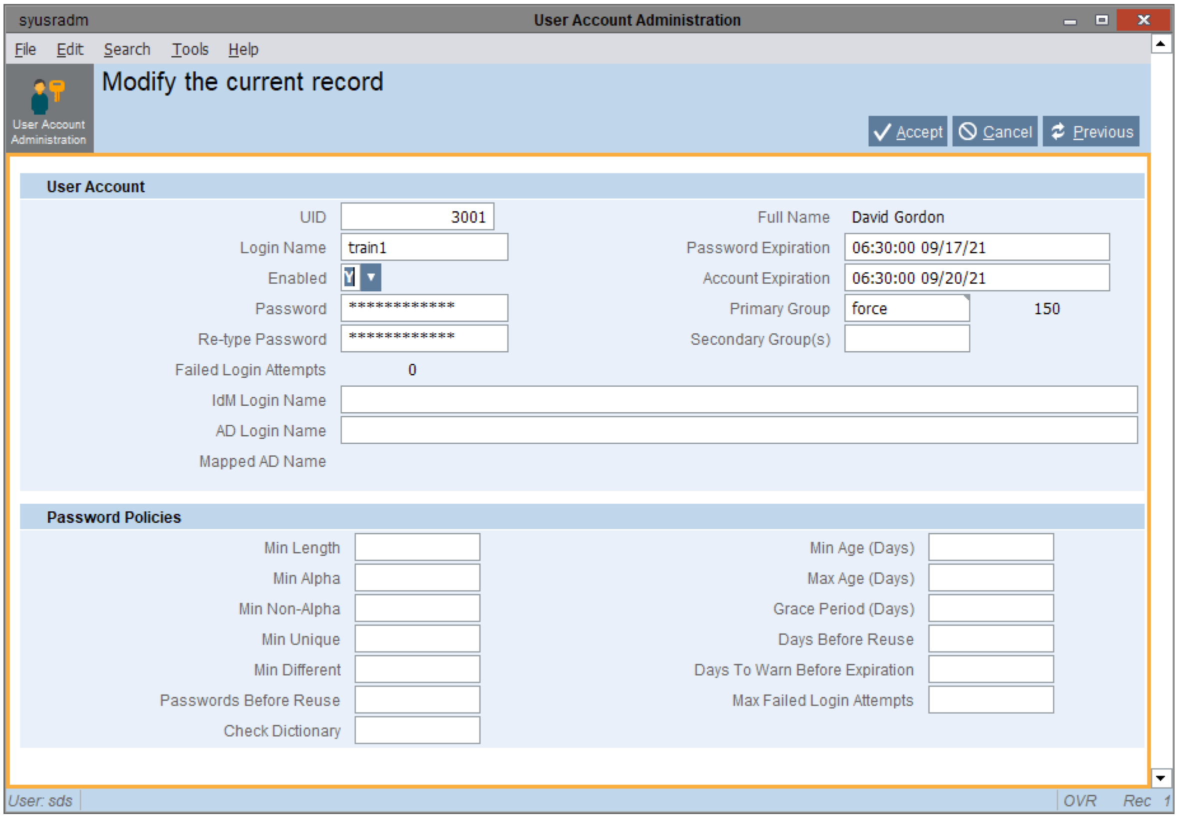
15.3.1 Notifications on Password and Account Expiration

With this feature configured, users receive password expiration notifications and are also notified when their accounts are locked.

Admin

Configure a user account in the Flex client application by entering the `syusradm` command, searching for the user, and modifying the **User Account** record with **Password Expiration** and **Account Expiration** data. In the **Password Policies** section, you can set other options, for example **Days to Warn Before Expiration**.

Figure 319: User Account Administration Window (syusradm)

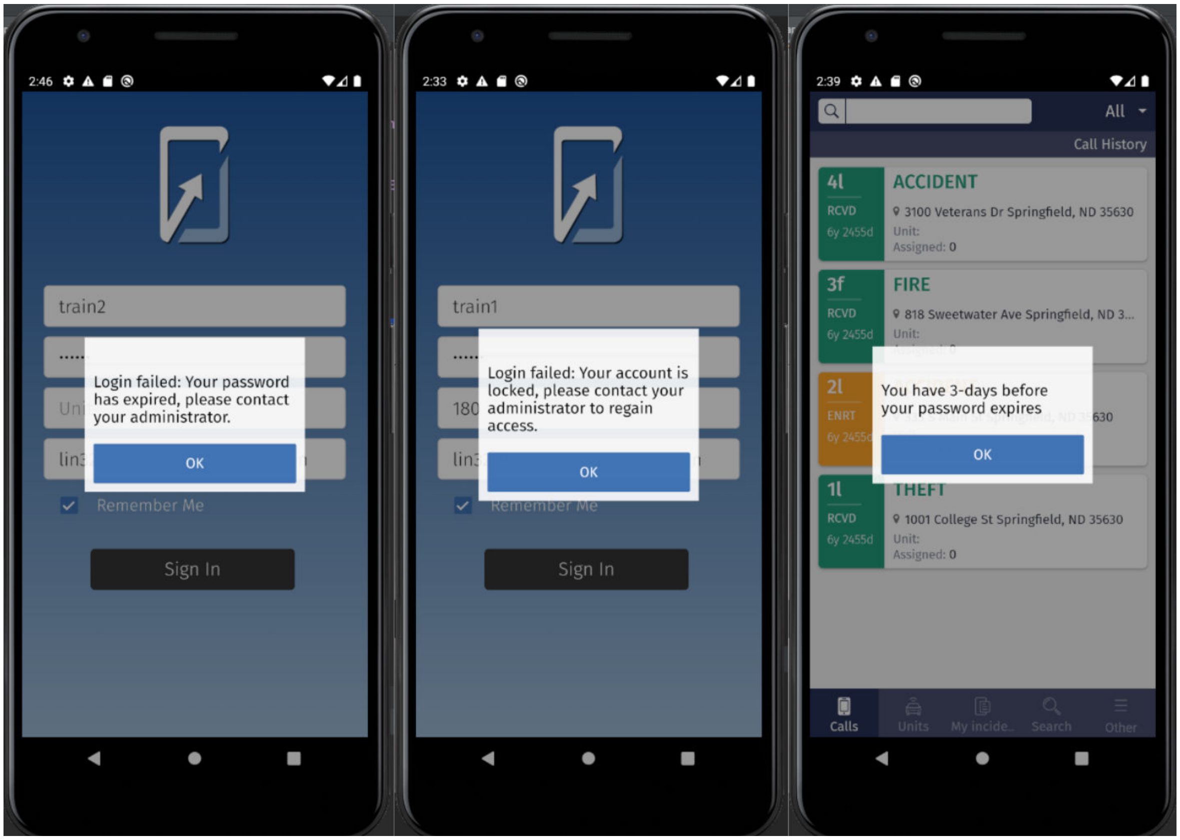


Notifications on User Devices

When the feature is configured by your administrator, you might see the following notifications on the screen of your mobile device:

- `Login failed. Your password has expired, please contact your administrator.`
- `Login failed. Your account is locked, please contact your administrator to regain access.`
- `You have X-days before your password expires.` (X represents the number of days left. The warnings begin when the number of days left is equal to or less than the value set by the administrator.)

Figure 320: New Notifications Concerning User Account and Password



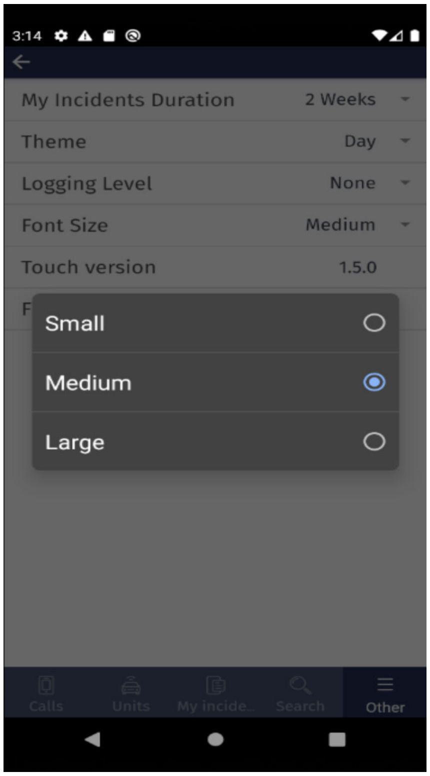
15.3.2 Adjusting the Font Size

This functionality can improve text legibility for users who do not have very good eyesight.

Procedure:

1. In the Touch application settings, select **Font Size**.

Figure 321: Font Size Choices



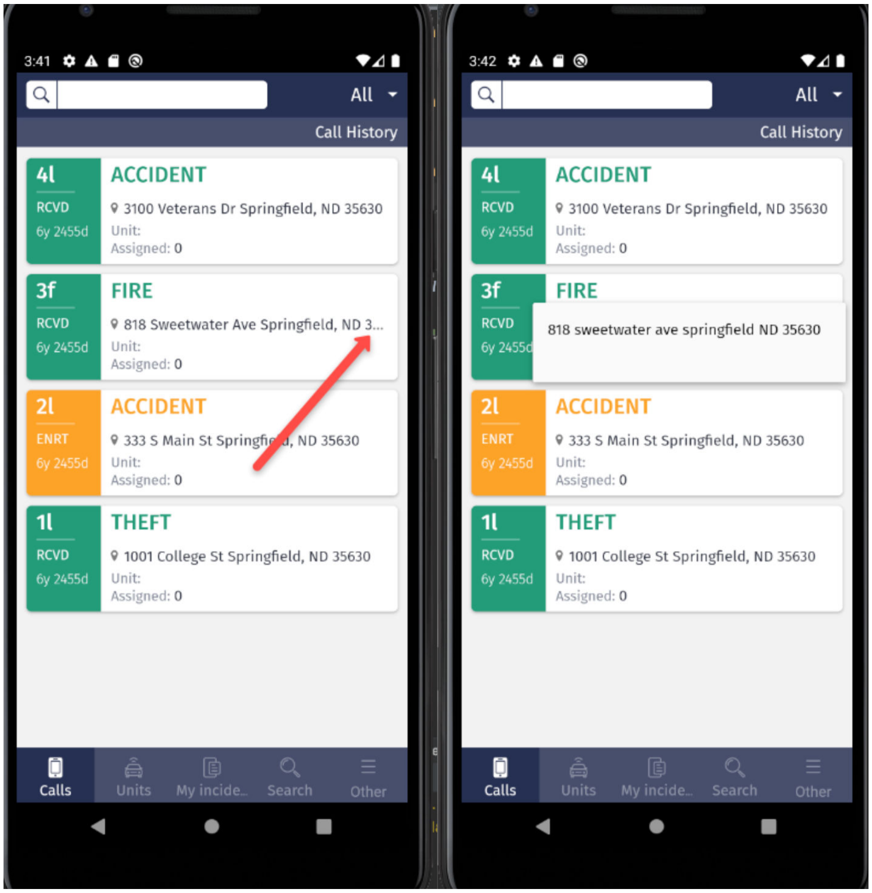
2. From the drop-down list, select your preferred font size.

To compare the font size effects, you can see iPhone 6 Screens with Different Font Size Settings on page 311.

NOTE:
The visible content of some fields can be limited to the available space, especially when you select the **Large** or **Medium** size. Incomplete information is indicated by three dots at the end of the text.

To display the full content of any field with text finishing with three dots (**...**), tap these dots. In the following figure, a case with three dots is indicated by a red arrow.

Figure 322: Incomplete Text Ending with Three Dots and Its Expansion



15.3.2.1
iPhone 6 Screens with Different Font Size Settings

Figure 323: iPhone 6 Screen with Small Font Setting

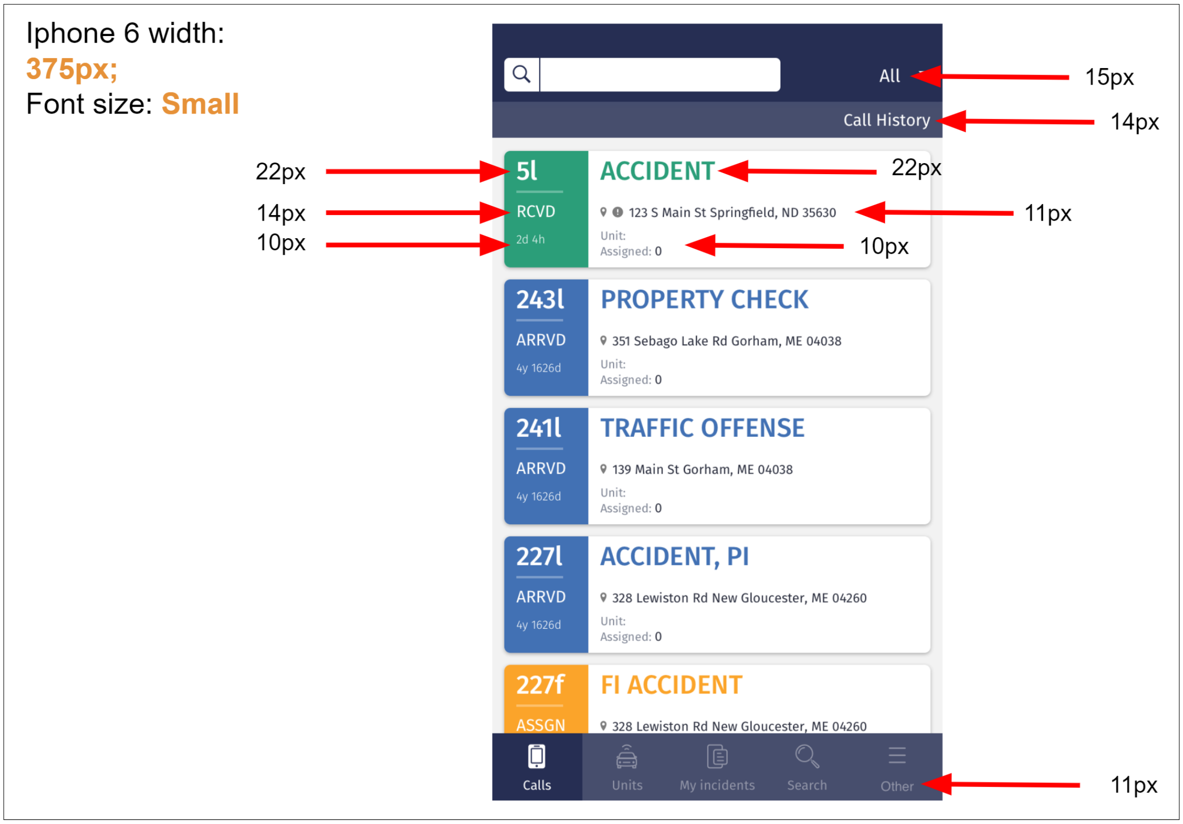


Figure 324: iPhone 6 Screen with Medium Font Setting

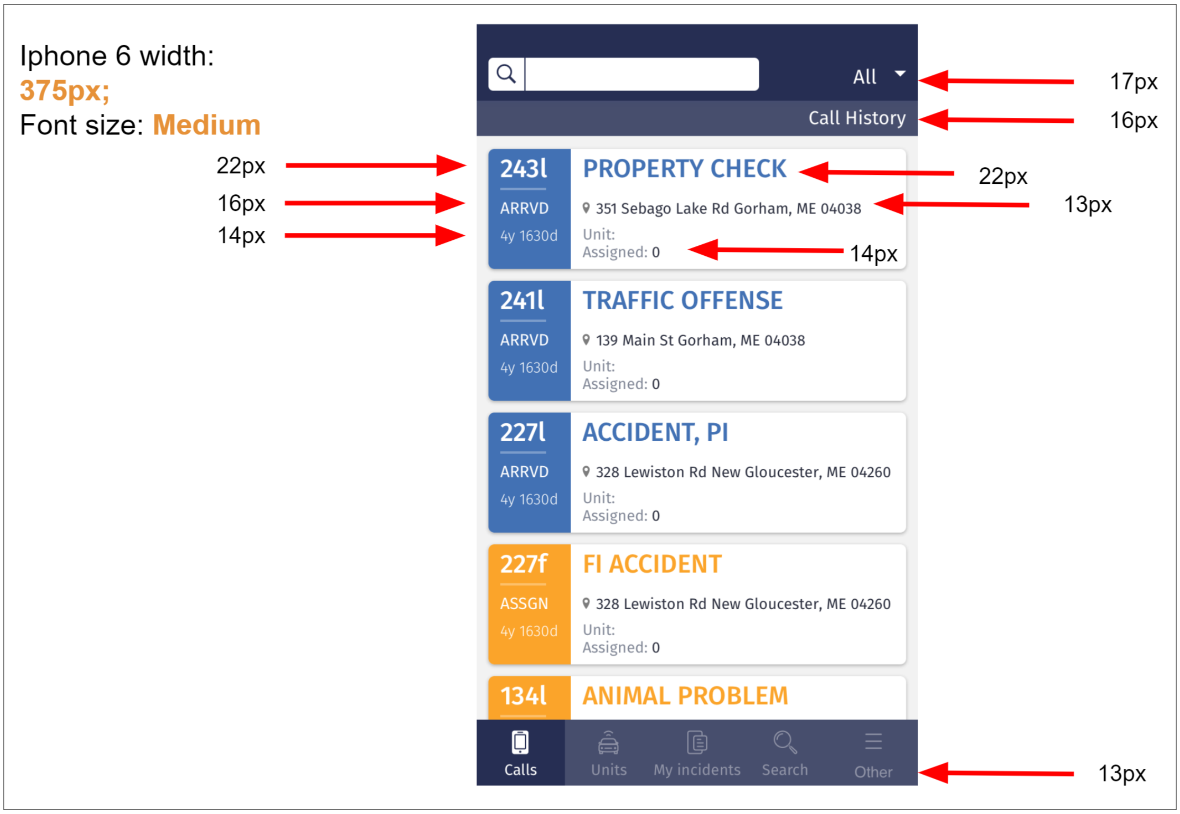
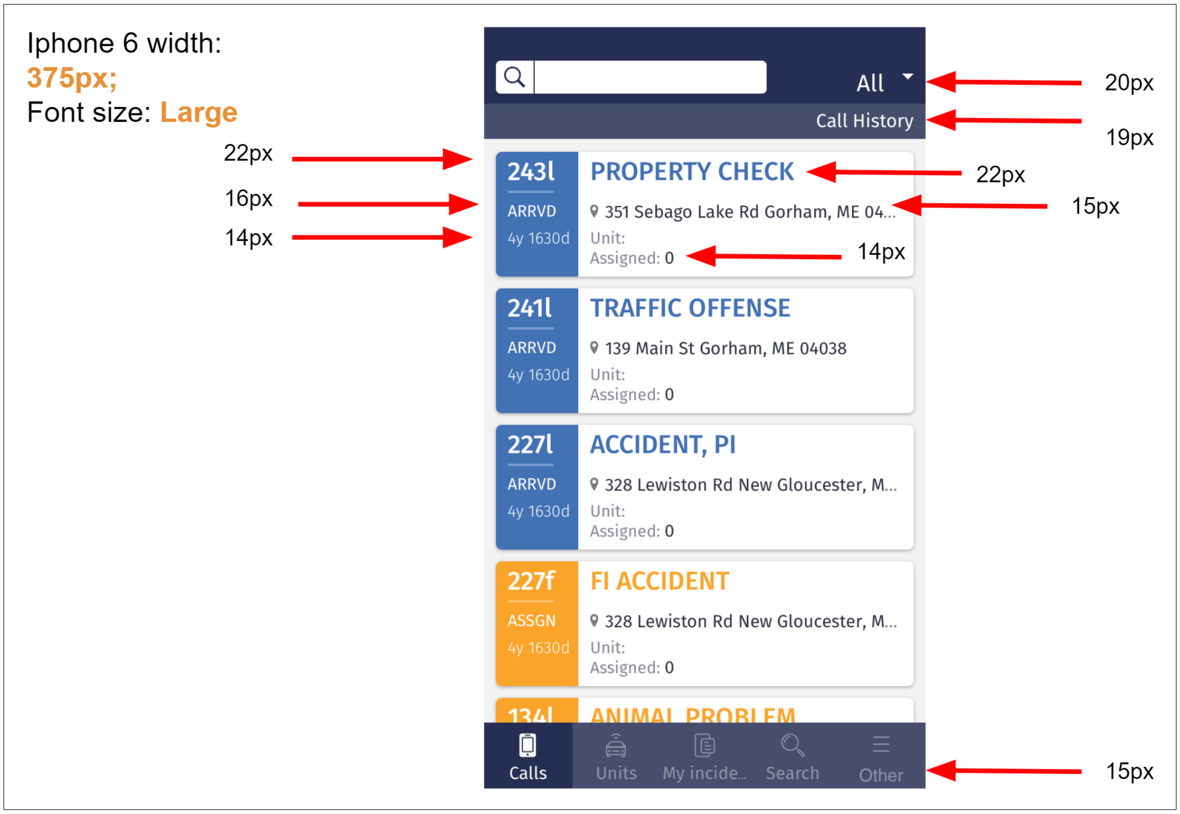


Figure 325: iPhone 6 Screen with Large Font Setting



15.3.3

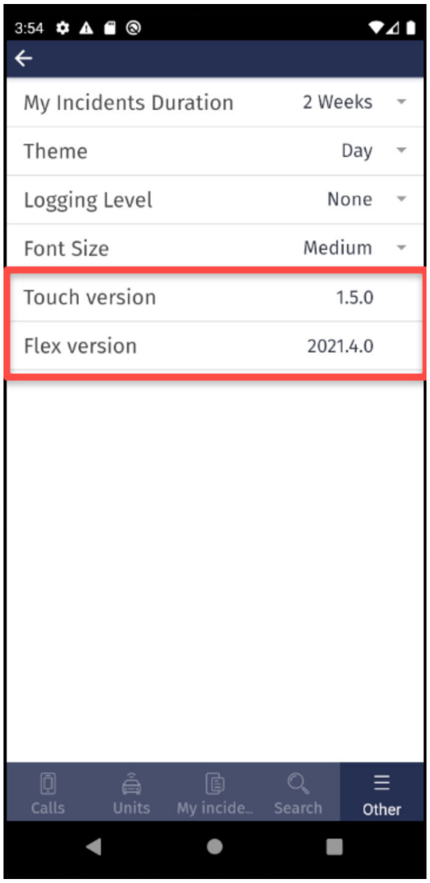
Checking Touch and Flex Versions

This functionality can improve communication between users at agencies and support teams by understanding which application and server versions are being used. It should facilitate the reporting of possible issues, as well as the development and support processes.

Procedure:

1. Log on to the Touch application.
2. In the lower right corner of the screen, tap the **Other** icon.
3. Select the **Settings** menu.

Figure 326: Touch and Flex Versions



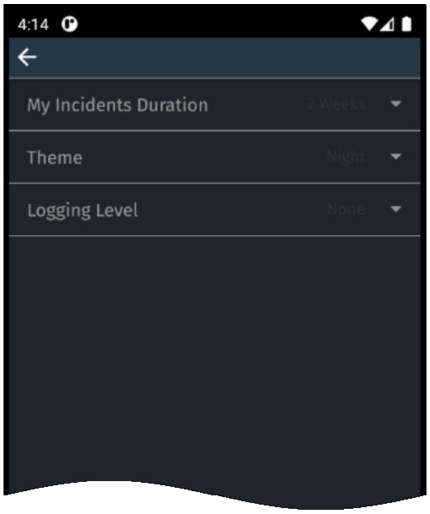
The last two fields of the screen contain the information about Touch version and Flex version (in the figure, the fields are marked with a red frame).

15.3.4

Better Clarity of Texts in the Night Mode

The operation of the application in the night (dark) mode is improved by the replacement of dark fonts, barely visible on black backgrounds, with bright fonts.

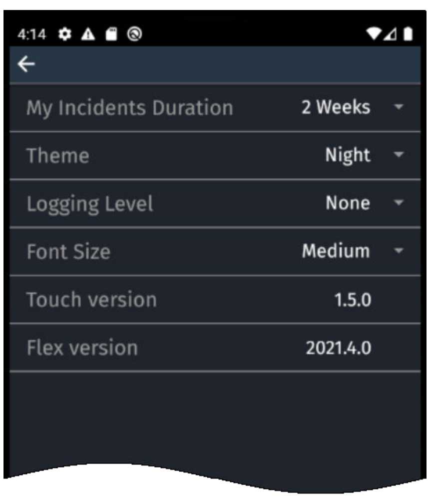
Figure 327: Poor Visibility of Dark Texts in the Night Mode Before the Change



So far, the visibility of some texts in the night mode was very poor. In the figure, the dark-gray texts in the right parts of the fields are barely visible.

With the improvement (see the following figure), users can use the application in the night more comfortably. The texts in all fields are now easily visible.

Figure 328: Improved Visibility of Dark Texts in the Night Mode



15.3.5
Enhancement of Android Platform with Taking Photographs

Thanks to this enhancement, users of Android devices can take photos within the application and attach them to Name, Vehicle, Property and other databases. Before, such a possibility was implemented only on iOS devices.

The camera feature used in the Touch application on an Android device supports the following settings:

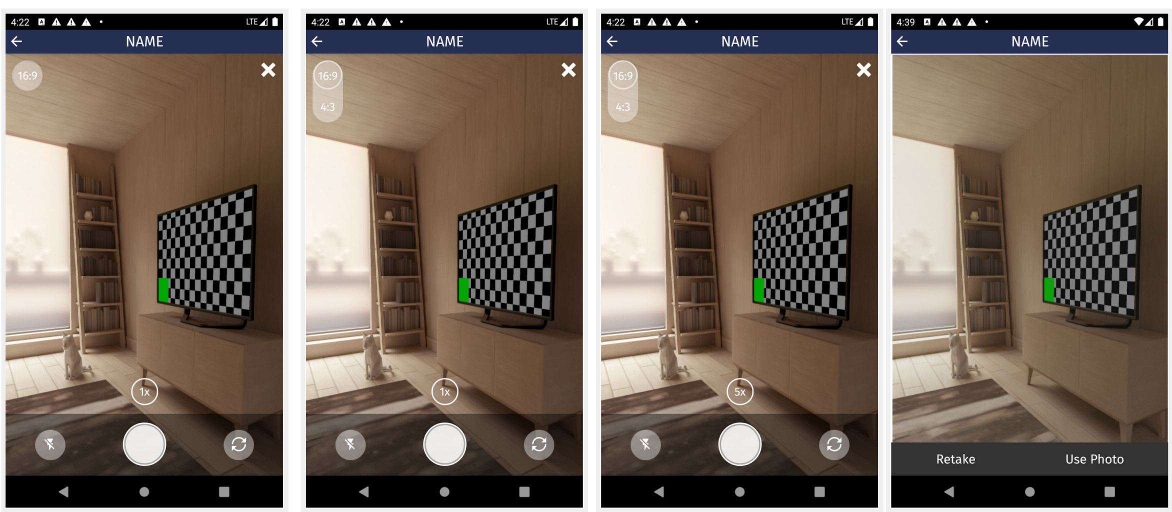
- Image aspect ratios: 4:3, 16:9, 18:9

  NOTE: The availability of the ratios depends on the type of the device used. The available options are shown as buttons at the top left corner of the image.

- Flash modes: ON, OFF, AUTO; (button at the bottom left corner of the image)
- Image scaling: 1x – 5x; (button in the center of the lower part of the image)
- Image orientation: landscape, portrait; (button at the bottom right corner of the image)

After taking a photo, the user has the possibility to retake it with the same settings (in the following figure, see the last screen on the right).

Figure 329: Photographic Options of Android Devices in the Touch Application



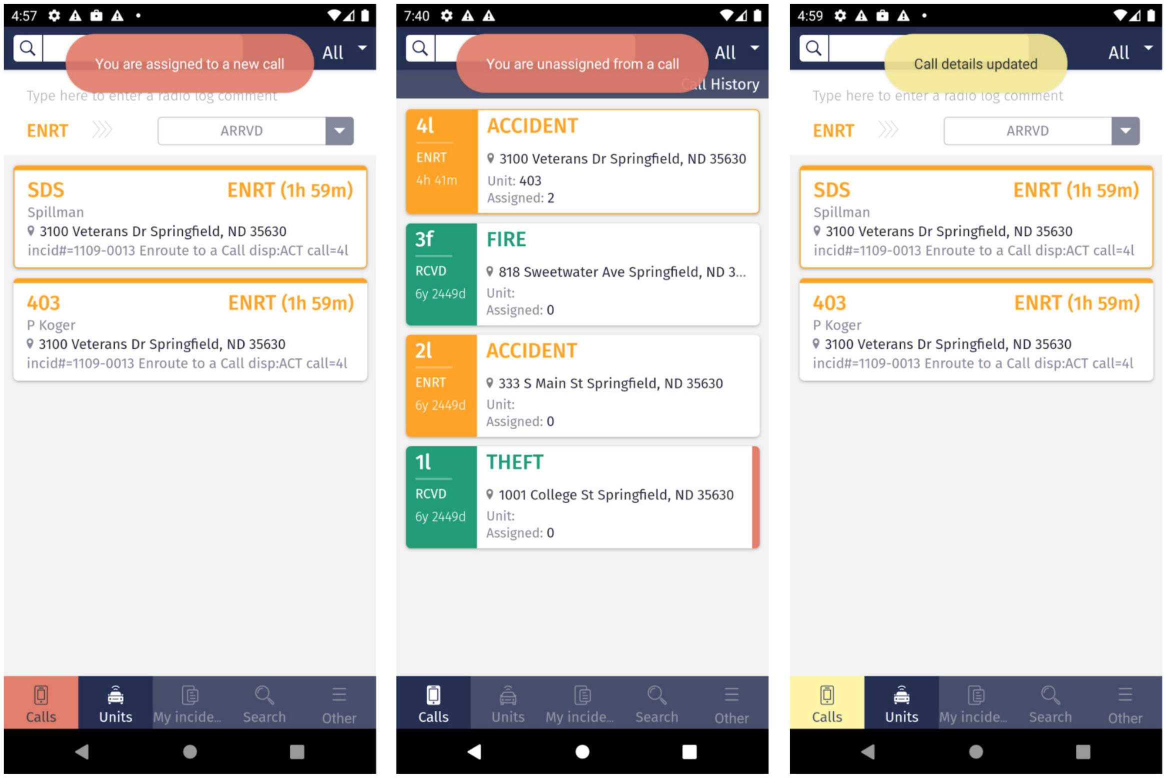
15.3.6
In-App Notifications

The purpose of In-App notifications is notifying users that they are assigned to new calls, unassigned from some calls, or they have updates to the assigned calls. From the notifications, users can access the new and updated information.

Users can see this type of notifications during the active use of the iOS or Android application as pop-up messages appearing at the top of the screen. A message disappears after five seconds or when the user taps it, initiating redirection to the new or updated information.

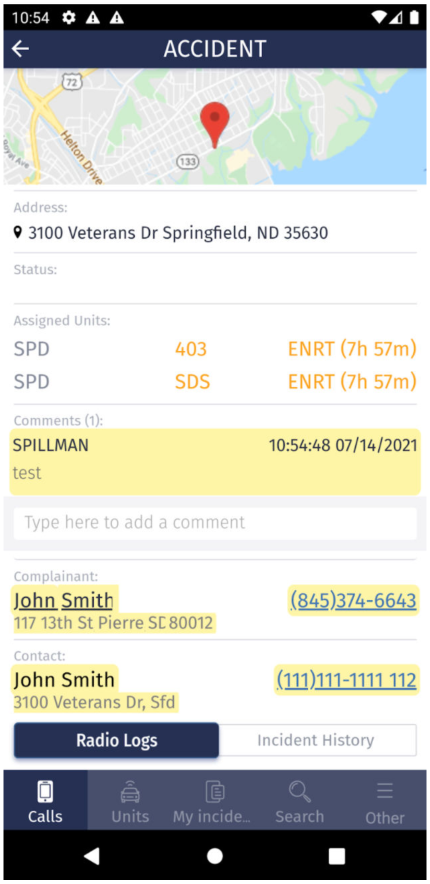
There are three types of notifications: assignment to a new call (marked with a reddish color), unassignment from a call (marked with a reddish color), and an update of an assigned call (marked with a yellow color).

Figure 330: New Call Assignment, a Call Unassignment, and Call Details Update Notifications



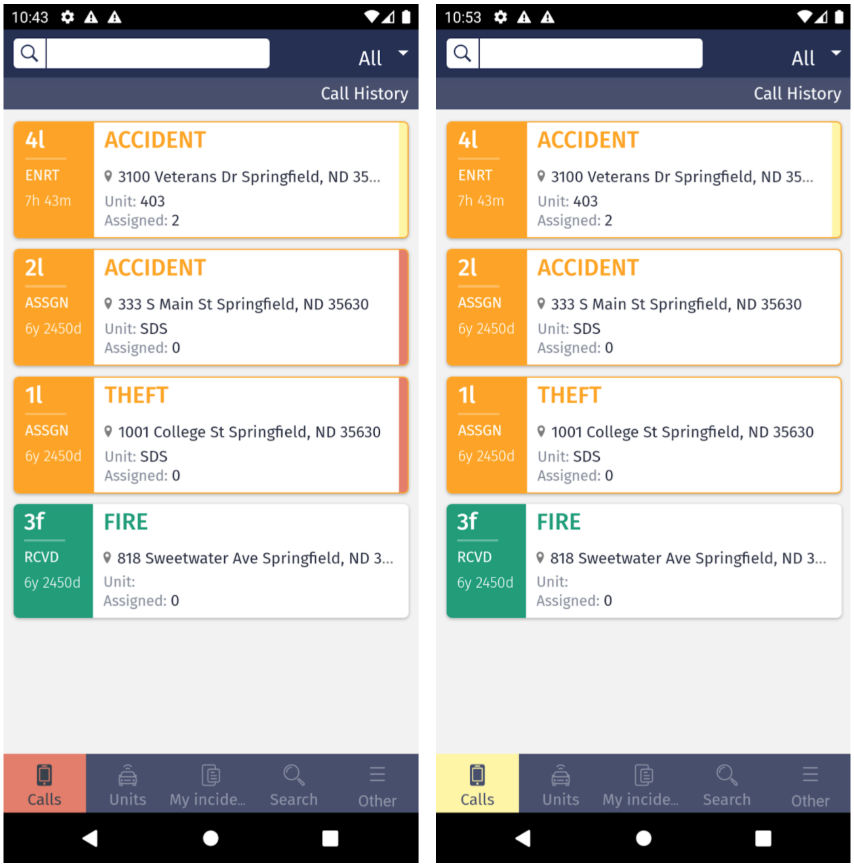
Notifications are clickable. By tapping a notification, the user is redirected to the appropriate call. In the call details screen, the highlighted fields indicate what exactly was changed (see the following figure). After reviewing the updates, the highlighting disappears.

Figure 331: Highlighted Updated Details



Users can review all missed changes. The existing missed assignments/unassigments and updates are indicated by a reddish or yellow color of the **Calls** tab. A reddish background indicates some missed assignments or unassignments, and yellow background indicates some missed updates. With missed both assignments and updates, the information about assignments has a higher priority, so the **Calls** tab has a reddish background. The assignments/unassignments and updates are also marked in the Call History list, with a reddish or yellow right-side borders, respectively.

Figure 332: Call History Lists with Notification Markers



15.3.7 Push Notifications in the Background Mode

The purpose of Push notifications is notifying users that they are assigned to new calls, unassigned from some calls, or they have updates to the assigned calls. From the notifications, users can access the new and updated information. Push notifications are accompanied by a sound effect.

Examples of Push notifications:

Figure 333: A New Call Push Notification

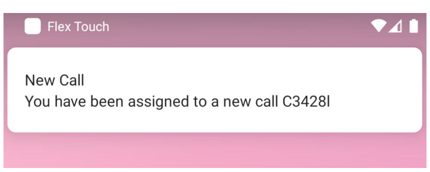
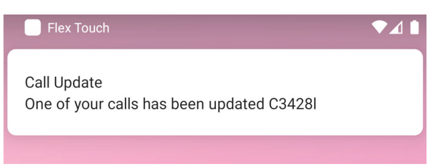


Figure 334: A Call Update Push Notification



Push notifications are clickable. By tapping a notification, the user is redirected to the appropriate call. In the call details screen, the highlighted fields indicate what exactly was changed (analogically to the In-App Notifications on page 316). After reviewing the updates, the highlighting disappears.

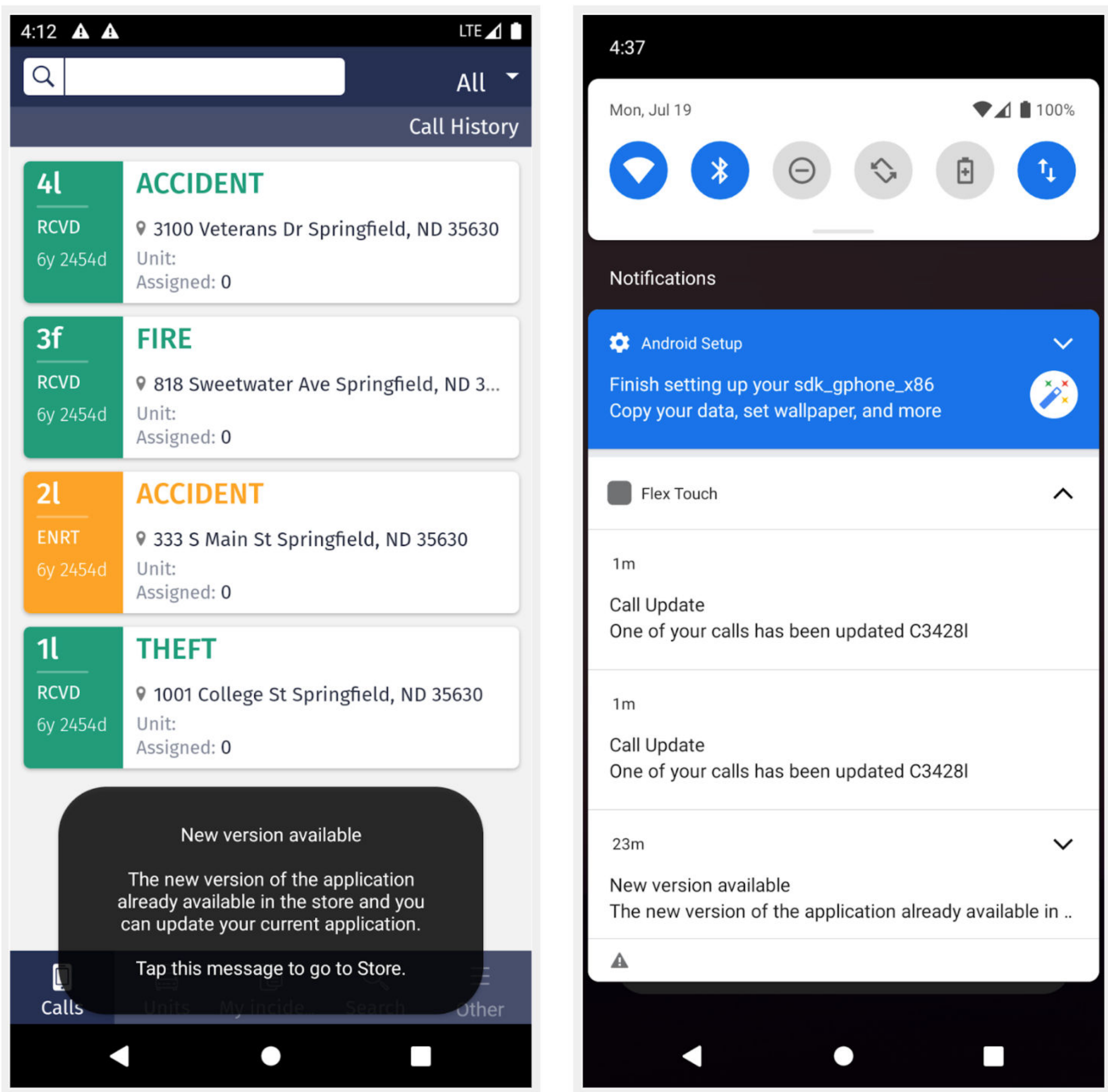
NOTE: Both on the Android and iOS platforms, users can be notified about new/updated call information only through the sounds. This customization is beyond the scope of this document.

15.3.8
Push Notifications about New Application Version

After publishing a new version of the Flex Touch application, users might get push notifications about the available version update, both on the iOS and Android platforms.

The push notifications reach devices in the active and background mode. By tapping the notification, the user of the device is redirected to the application's download page in the relevant store.

Figure 335: Push Notification about New Application Version on an Android Device



Chapter 16

Release 2021.2

This chapter presents changes made to Flex for the 2021.2 release.

16.1 CAD

16.1.1 Admin: Displaying Jurisdiction Information for a Geo-Validated Address

Use this procedure if you want to display the jurisdiction information in your agency. By default, this feature is switched off.

Procedure:

1. In the Administration Manager (`adminutil`), in the **Module.CAD** folder, set the value of the `IncidentScreenShowJurisdictionLink` setting to `True`

   The setting determines whether to show below the **CAD Incident Address** the information with codes of **Law**, **Fire**, **Med** (EMS), and **Misc** type agencies in the dispatching zone. The default value is `False`.

2. Ensure that the `tbzones` table contains a code for every zone of every agency that uses the software.

   For more information about setting up code tables, see the *Flex Administrator Manual*.

   For more details about jurisdiction information, see the Jurisdiction Information for a Geo-Validated Address on page 321.

16.1.2 Jurisdiction Information for a Geo-Validated Address

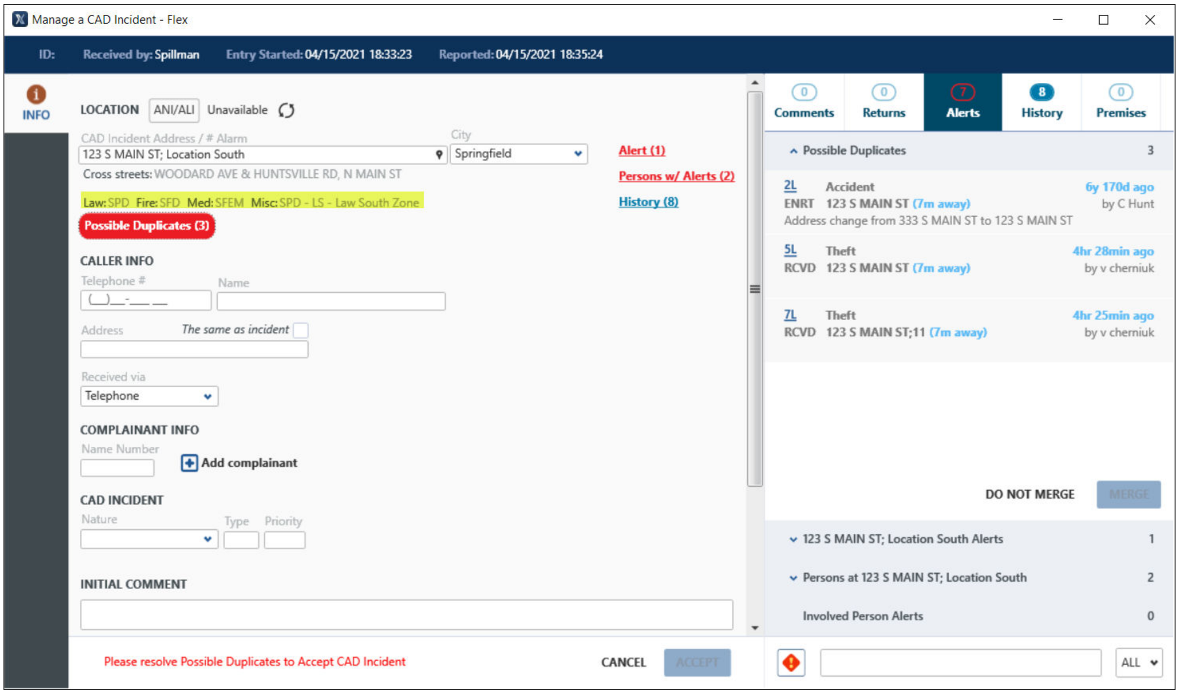
When your agency uses the GeoValidation module and ArcGIS to create a Geographic Information System (GIS) of street and address information about jurisdictions, your administrator can enable displaying jurisdiction information. This feature allows you to save time when making a decision on transferring the phone call.

If the displaying of jurisdiction information is enabled and the `tbzones` table contains zone codes of adequate agencies, some CAD Incident screens can provide you with a range of jurisdiction information about a geo-validated address.

The jurisdiction information, if exists, is displayed below the **CAD Incident Address** field containing a geo-validated address, under the **Cross streets** information. If the address is changed, the system will display a new set of data available for the new address.

In the following figure, the jurisdiction information is additionally marked with a yellow highlighting. In the case of **Possible Duplicates** message, its red field is located just under the jurisdiction information.

Figure 336: Location of the Jurisdiction Information on the INFO Tab



The jurisdiction information is based on zones and may include:

- **Law**: *Law agency code*
- **Fire**: *Fire agency code*
- **Med**: *EMS agency code*
- **Misc**: *Miscellaneous agency code - Dispatch zone code - Zone description*

NOTE: The *Zone description* of the **Misc** type can be modified by your administrator to include, for example, name of the fire inspector or other suitable information.

If there is no data available about a type of agency dispatching the address, the system skips the respective section in the jurisdiction field. For example, when a fire agency is missed, then only the **Law**: *Law agency code*, **Med**: *EMS agency code*, and **Misc**: *Miscellaneous agency code - Dispatch zone code - Zone description* information is displayed, without the label and agency code for a fire department. If no data is available, the system does not display anything in the jurisdiction field.

The jurisdiction information, if exists, is also displayed on discipline tabs, as shown in the examples in the following figures.

Figure 337: Jurisdiction Information on a CAD Incident Screen (Law Nature)

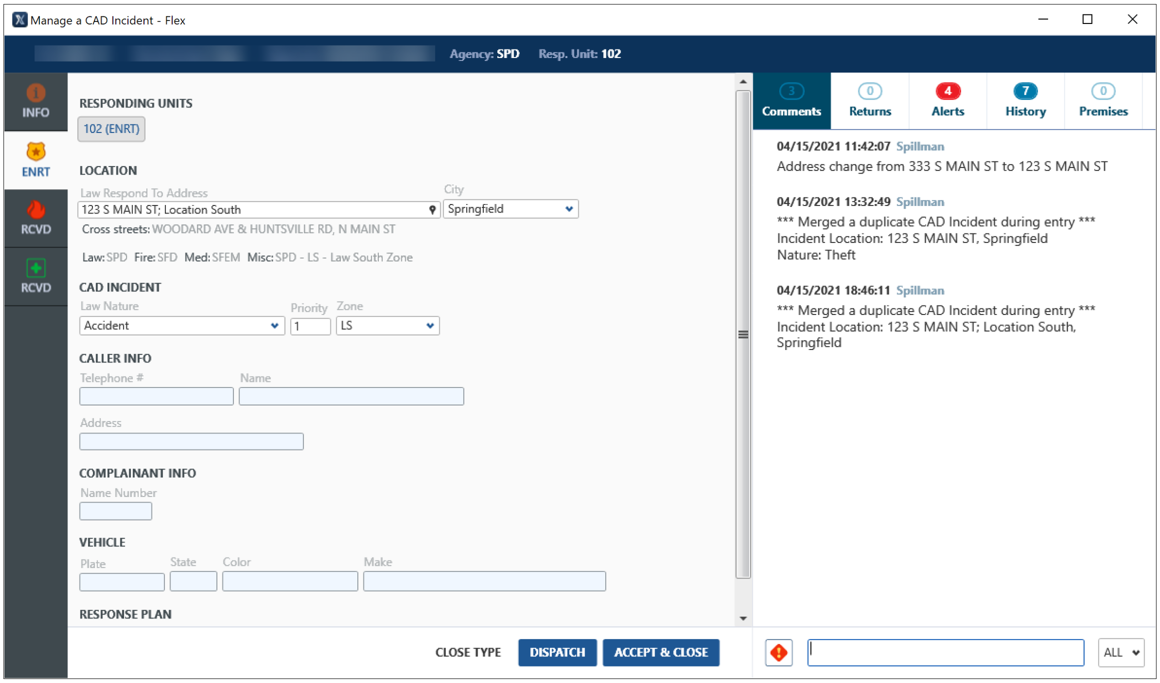


Figure 338: Jurisdiction Information on a CAD Incident Screen (Fire Nature)

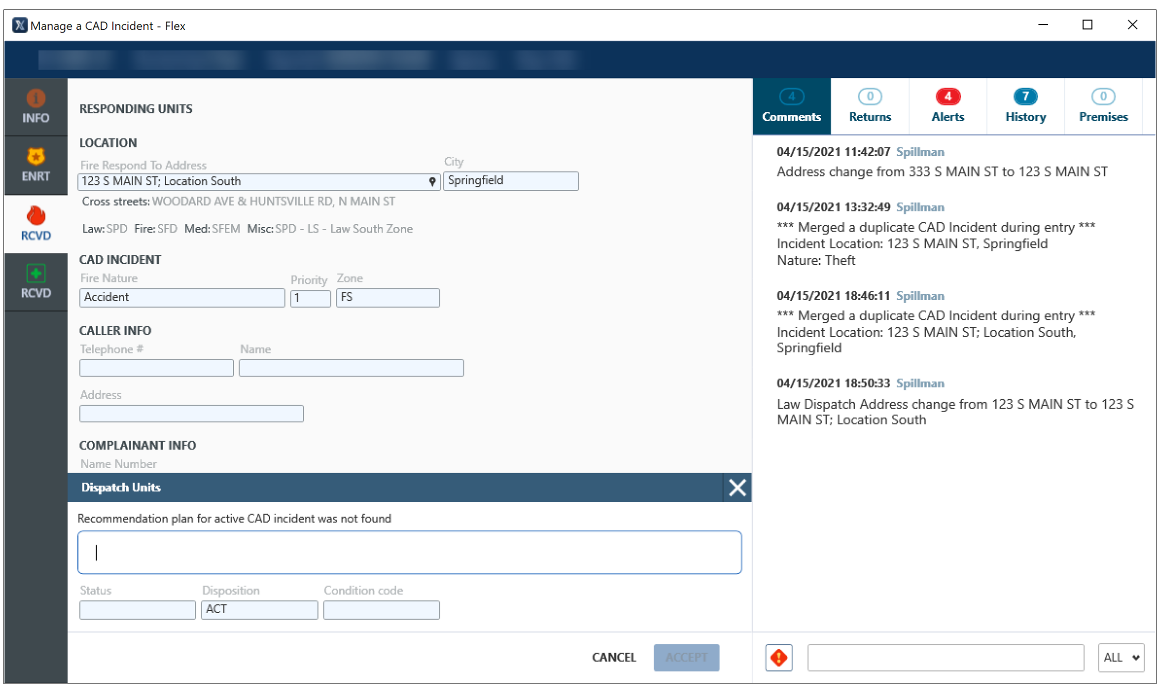
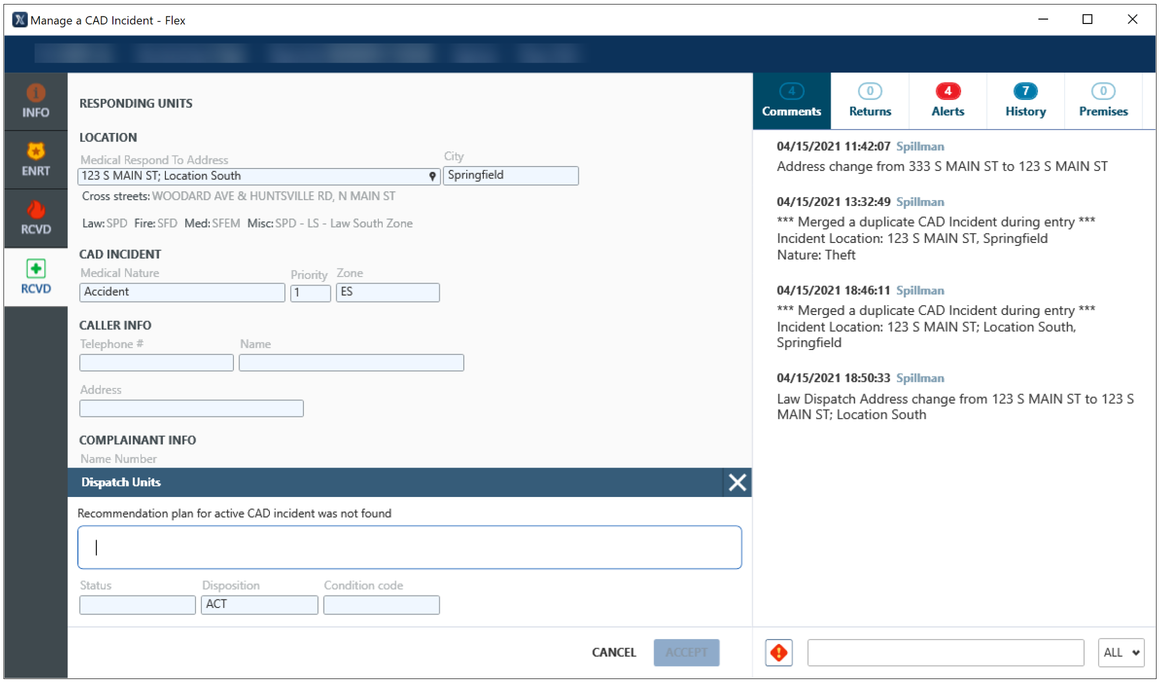


Figure 339: Jurisdiction Information on a CAD Incident Screen (Medical Nature)



16.1.3

Admin: Configuring CAD for Use in California

Use this procedure to enable your Californian agency to operate according to the new CLETS rules.

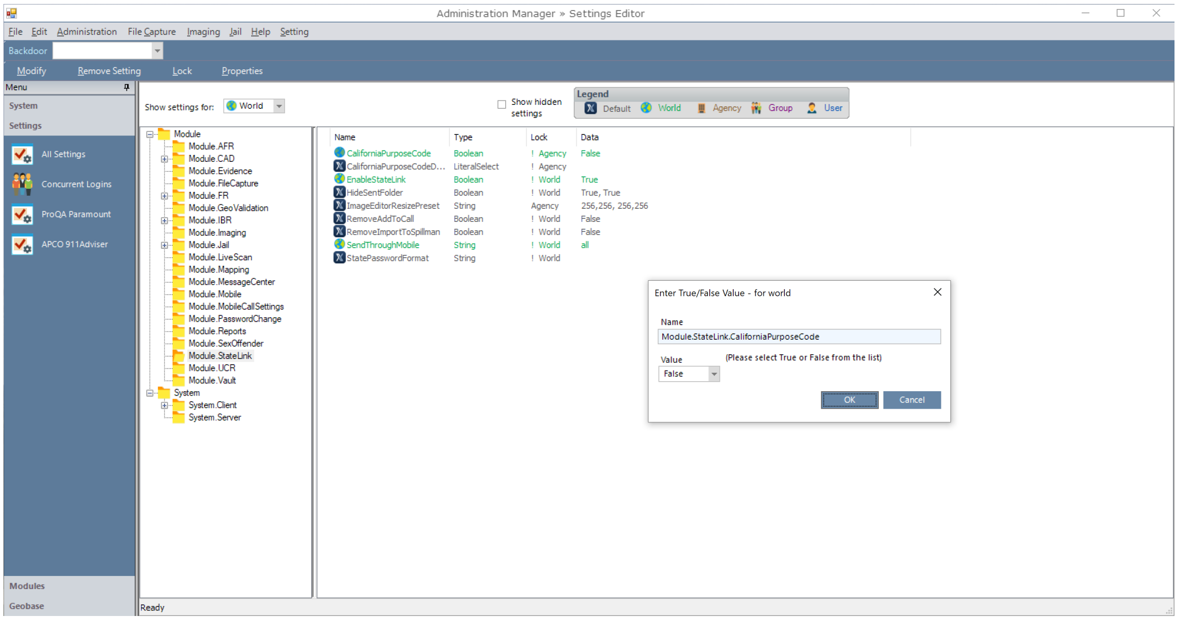
Due to new statutory restrictions and requirements governing the use of the California Law Enforcement Telecommunications System (CLETS), commencing July 1, 2021, any inquiries submitted through the CLETS will have to include a reason for the inquiry. It applies to `DQ`, `DQA`, `DQL`, `OSC`, `RQ`, `RQV`, and `TS` commands. For more information, see California: Purpose Code in Some CAD Commands on page 325.

Procedure:

1. On the command line, enter `adminutil`
2. From the **Settings** menu group, click the **All Settings** menu item.
3. In the **Show settings for** field, enter `World`
4. In the tree menu on the left, use the **Module** menu to locate the **Module.StateLink**.
5. In the setting window on the right, locate the `CaliforniaPurposeCode` setting and double-click it.

   The **Enter True/False Value - for world** dialog box opens, with the `False` default **Value** of the `Module.StateLink.CaliforniaPurposeCode` setting.

Figure 340: Flex Settings Editor Window with Module.StateLink.CaliforniaPurposeCode dialog Box



6. Set the **Value** to `True` and click **OK**.

   The software saves the new setting value.

   NOTE: When the `Module.StateLink.CaliforniaPurposeCode` setting is set to `True`, the system prevents automatic queries for license plates from CAD Incident comments, regardless of the value of the `Module.CAD.Calltaking.AutorunPlatesFromComments` setting.

16.1.4

California: Purpose Code in Some CAD Commands

In California, starting July 1, 2021, any inquiries submitted through the California Law Enforcement Telecommunications System (CLETS) will have to include a reason for the inquiry. To meet the California State requirements, a set of Flex CAD commands and workflows is modified, allowing Californian agencies to operate in compliance with the state law. These changes do not affect the operation of the software in other states.

Purpose Code parameters are required in California for a set of Flex CAD commands. One of the three parameters is necessary for execution of any of these commands.

California Purpose Code

The implementation of the Purpose Code is connected with the California Values Act. The statement from Government Code Section 15160: "Commencing on July 1, 2021, any inquiry for information other than criminal history information submitted through the system shall include a reason for the initiation of the inquiry." sets additional conditions for California law enforcement agencies.

NOTE: It is the role of the administrator of your Californian agency to configure the system to be ready for the new rules.

The new valid Purpose Codes will be:

- `C` = Criminal Justice
- `I` = Immigration Enforcement
- `U` = Investigate Violations (of Title 8, section 1325 of the United States Code)

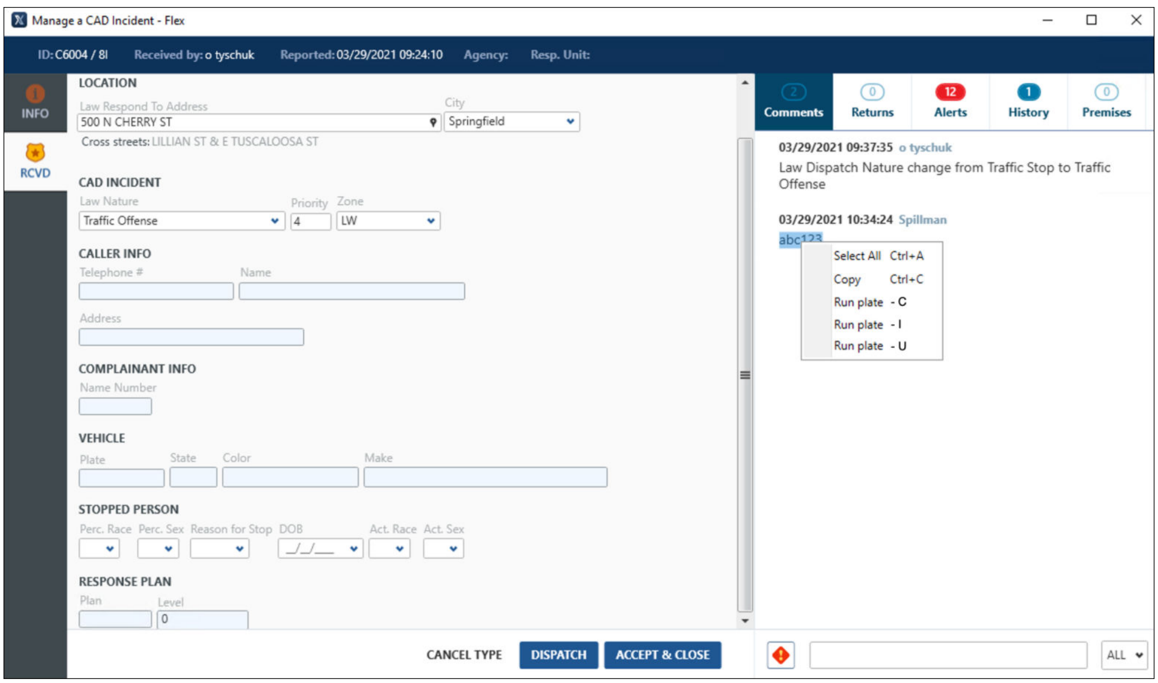
To be valid, each of the CAD commands that require the California Purpose Code must include as the first parameter one of these values: `C`, or `I`, or `U`. If the value of this parameter is different, the system will warn you with the following message: `Command is invalid, wrong purpose code.`

NOTE: Some queries with `OSC` and `TS` commands can be performed with an empty value of the Purpose Code entered as one or two double quotation mark(s): `"`, or `""`. For more information, see descriptions of these commands in California: CAD Commands that Require a Purpose Code.

The **Usage** tip will remind you of entering a suitable Purpose Code as the first parameter of the command. The components of the Flex CAD commands are not case-sensitive. For more information about CAD commands, see the *CAD User Manual*.

NOTE: In the new configuration for Californian agencies, automatic license plate queries from CAD Incident Comments are not supported. To manually run a query for a license plate number entered in the **Comments** tab, right-click the number, and from the pop-up menu select the appropriate option: `Run plate - C`, or `Run plate - I`, or `Run plate - U`.

Figure 341: Purpose Code Selection Menu for License Plate Query from Comments



16.1.4.1

California: CAD Commands that Require a Purpose Code

The implementation of the Purpose Code is connected with the California Values Act. The statement from Government Code Section 15160: "Commencing on July 1, 2021, any inquiry for information other than criminal history information submitted through the system shall include a reason for the initiation of the inquiry." sets additional conditions for California law enforcement agencies.

This is a preview of CAD commands that, when used in California, are subject to the California Purpose Code requirements. For general information about each of these commands see the relevant description in this manual, especially in CAD Commands: Complete Reference.

The valid Purpose Codes are:

- `C` = Criminal Justice
- `I` = Immigration Enforcement

- U = Investigate Violations (of Title 8, section 1325 of the United States Code)
  To be valid, each of the CAD commands that require the California Purpose Code must include as the first parameter one of these values: C, or I, or U. If the value of the parameter is different, the system will warn you with the following message: `Command is invalid, wrong purpose code.`

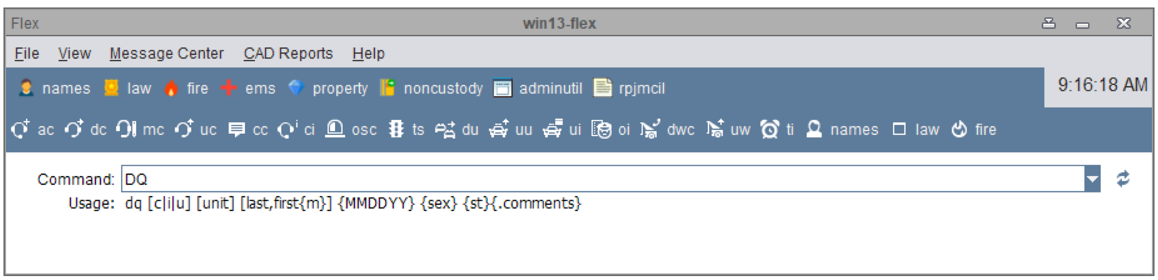
  The **Usage** tip will remind you of entering a suitable Purpose Code as the first parameter of the command. The components of the Flex CAD commands are not case-sensitive.

  CAUTION: In the new configuration for Californian agencies, automatic license plate queries from CAD Incident Comments are not supported. To manually run a query for a license plate number entered in the Comments tab, right-click the number, and from the pop-up menu select the appropriate option: `Run plate - C`, or `Run plate - I`, or `Run plate - U`.

The **Usage** tip will remind you of entering a suitable Purpose Code, `c`, or `i`, or `u` as the first parameter of these commands. The `OSC` and `TS` commands can optionally accept an empty value of the Purpose Code entered as one or two double quotation mark(s): `"`, or `""`. If the value of the Purpose Code parameter is different, the system will warn you with the following message: `Command is invalid, wrong purpose code.`

DQ Command

Figure 342: DQ Command with California Purpose Code Options

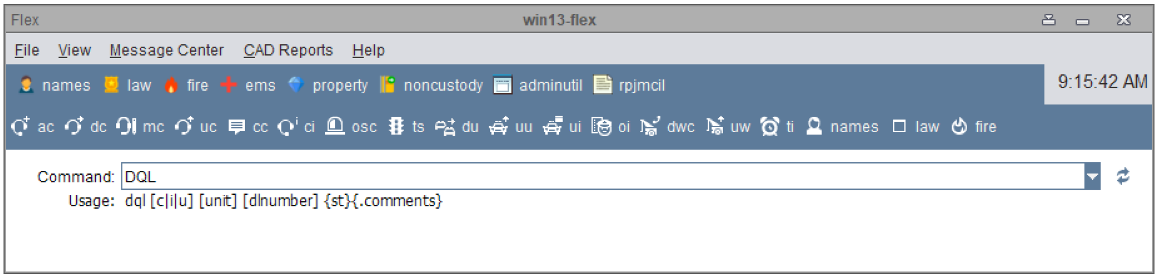


DQA Command

Figure 343: DQA Command with California Purpose Code Options

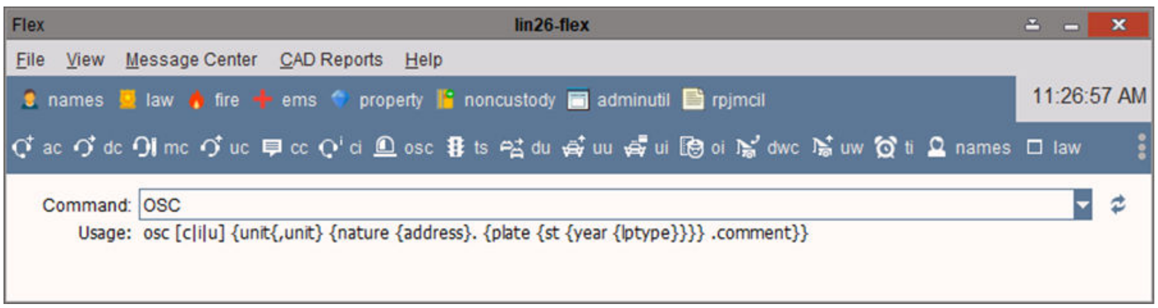
DQL Command

Figure 344: DQL Command with California Purpose Code Options



OSC Command

Figure 345: OSC Command with California Purpose Code Options



The `OSC` command can optionally accept an empty value of the Purpose Code entered as one or two double quotation mark(s): `"`, or `""`.

By clicking the **OSC** button on the toolbar, or entering the `OSC` command from the **Command** field without a parameter, you open the **Onsite Call Command** window. The window includes the **Purpose Code** field with selectable options. The `c`, or `i`, or `u` Purpose Code is necessary for any StateLink query. If the **Lic Plate** field is left blank, selecting a **Purpose Code** is optional.

NOTE: When the `OSC` quick command is used with **Purpose Code** value `"` or `""`, and the **Lic Plate** field is filled in, the system will **not** run the StateLink query and will **not** create a CAD Incident. At the bottom of the **Onsite Call Command** window an error message will be displayed.

Figure 346: Onsite Call Command Window with Purpose Code Field

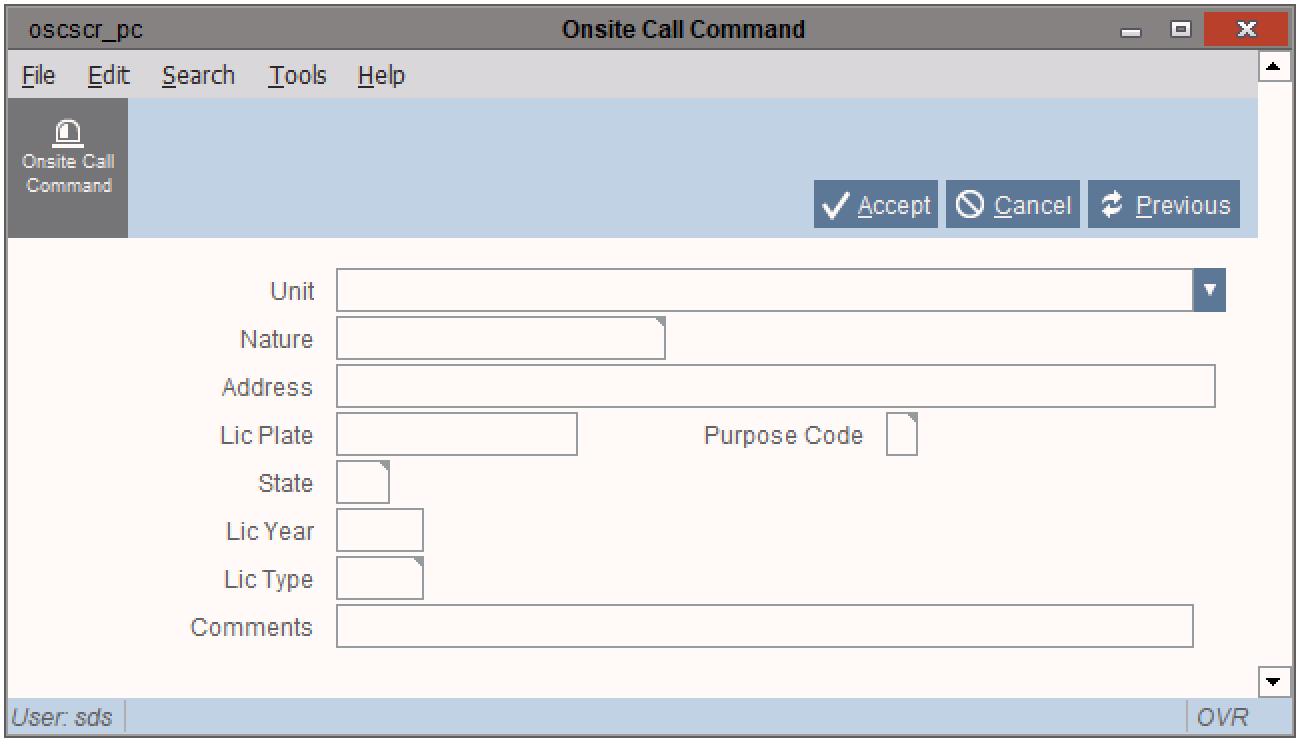
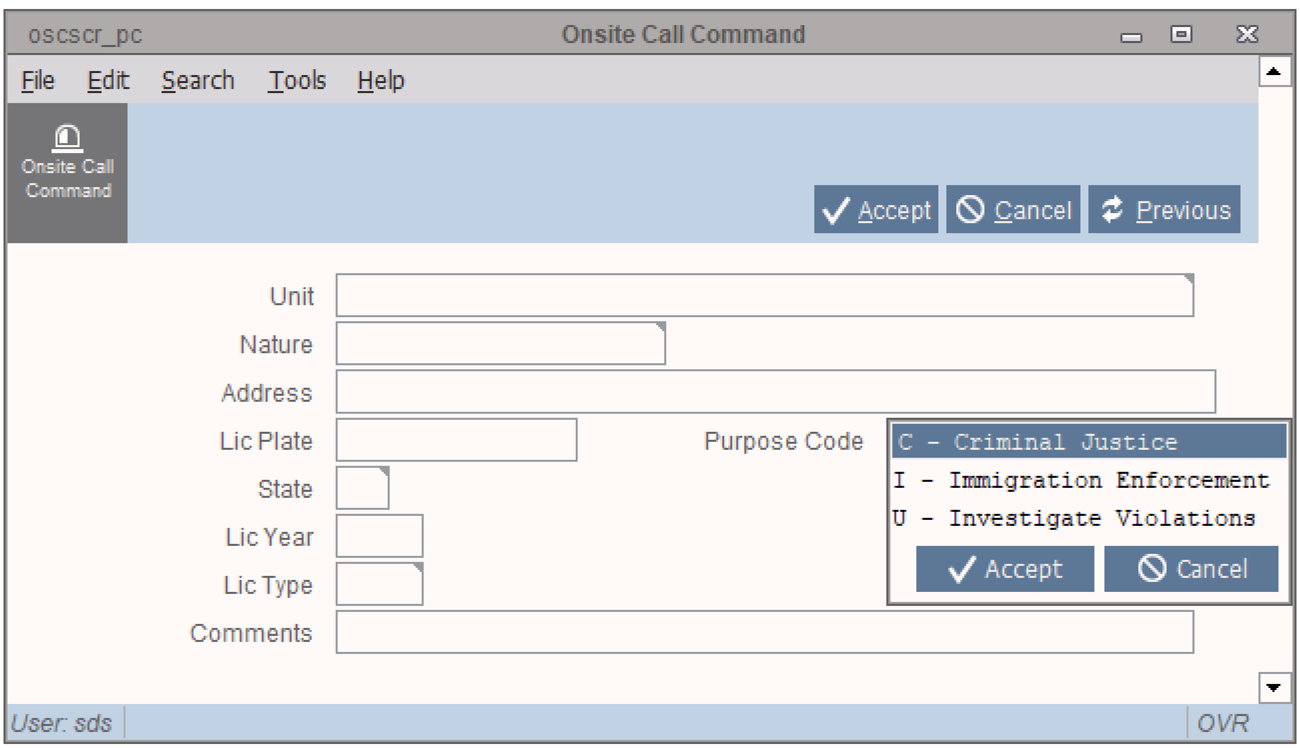


Figure 347: Onsite Call Command Window with Purpose Code Field Options

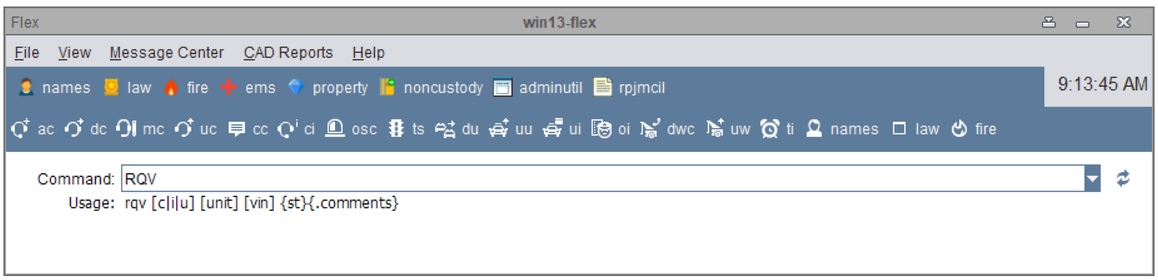


RQ Command

Figure 348: RQ Command with California Purpose Code Options

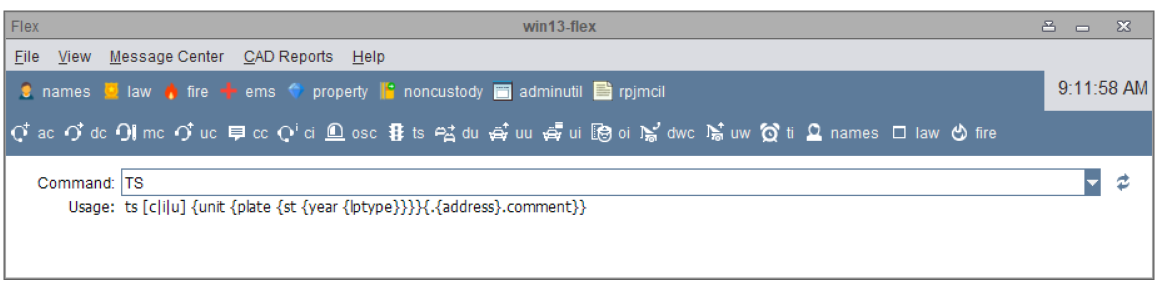
RQV Command

Figure 349: RQV Command with California Purpose Code Options



TS Command

Figure 350: TS Command with California Purpose Code Options



The `TS` command can optionally accept an empty value of the Purpose Code entered as one or two double quotation mark(s): `"`, or `""`.

By clicking the **ts** button on the toolbar, or entering the `TS` command from the **Command** field without a parameter, you open the **Traffic stop** window. The window includes the **Purpose Code** field with selectable options. The `c`, or `i`, or `u` Purpose Code is necessary for any StateLink query. If the **Lic Plate** field is left blank, selecting a **Purpose Code** is optional.

NOTE: When the `TS` quick command is used with **Purpose Code** value `"` or `""`, and the **Lic Plate** field is filled in, the system will **not** run the StateLink query and will **not** create a CAD Incident. At the bottom of the **Traffic stop** window an error message will be displayed.

Figure 351: Traffic Stop Window with Purpose Code Field

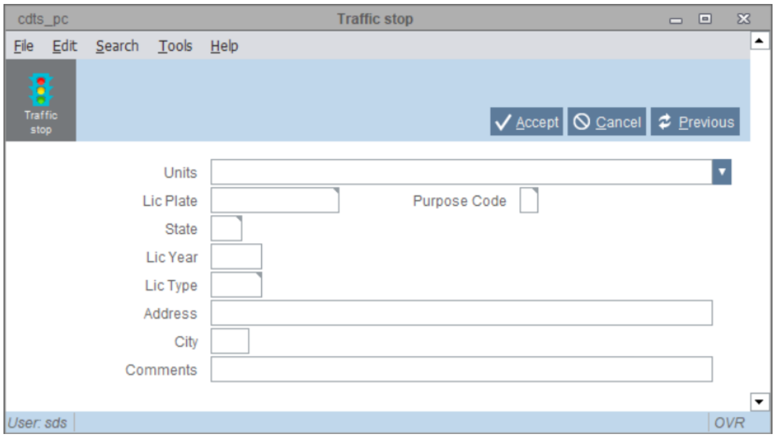
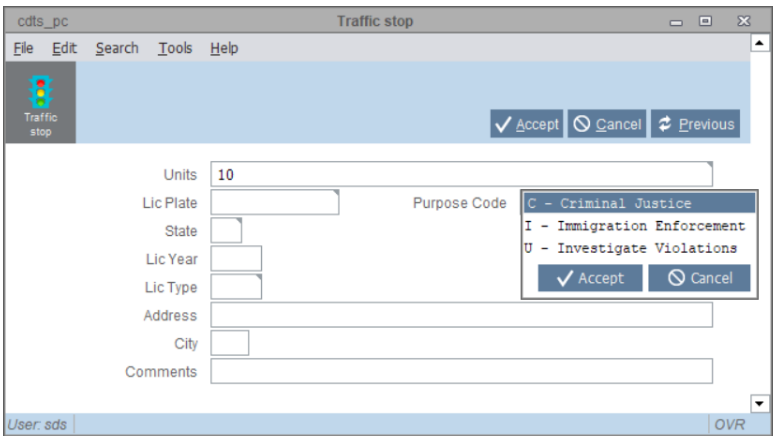


Figure 352: Traffic Stop Window with Purpose Code Field Options



16.2
Records

16.2.1
RMS: Detail Controls of Mobile Forms Based On Detail Table's Partition

With this change, by default, the detail controls of Mobile forms are editable by users based on their privileges to the detail table's partition and not the parent table's partition. Users are able to manage the partition of the parent and the related detail tables separately. This functionality is now available in the 2021.1 and newer releases.

16.3
Jail

16.3.1
Jail Application

Jail Application eliminates paper logs when performing cell checks and rounds by using a cell-phone-sized device to capture the information. The log information is then available as log records in CommandCentral Jail.

Features

- Scan location barcodes as rounds are completed
- Scan bed barcode when performing cell checks and note the inmate status and capture notes
- Native Android application

Requirements

- Wi-Fi connection to log in and up to upload completed scans
- Datalogic barcode scanner: Memor 10 or Memor 20

16.3.2
Performing Rounds or Cell Checks

To complete the jail rounds or cell check, you can use the scanner to efficiently record and share the data.

Procedure:

1. From the scanner **Main Menu**, select **Rounds**.

   The **Rounds** menu appears and the scan mode activates. You can now scan the locations.

2. Scan the barcode for each location as rounds are performed. Once finished, select **Complete Rounds**.
3. For cell checks, select **Cell Check**. After each bed is scanned, select the status of the inmate. You can also add Notes.

   NOTE: The Inmate Activity List needs to be populated with the statuses the agency would like for officers to select from when performing cell checks. To set up the statuses, see Admin: Setting Up Statuses for Cell Checks on page 333.

   The scanner displays the number of locations scanned.

4. When finished, select **Complete Cell Check**.

   NOTE: The scanner requires a Wi-Fi connection to both log in and to upload the rounds and cell check scans. If a user has a Wi-Fi connection, the activity is uploaded when it is completed. If the device does not have a Wi-Fi connection, the activity is stored on the device until there is a Wi-Fi connection available.

   A Log record is created for each scanned location or bed. The Log records use the **Event Type** value set by your administrator:

   - For rounds, the **Inmates Involved** tab lists any inmates who were in the location, according to the **Current Location** values on the Inmate records.

- For cell checks, the **Inmate Involved** tab lists the inmate assigned to the bed. The **Notes** tab lists the bed number and the status of the inmate.

16.3.3
Admin: Setting Up Statuses for Cell Checks

The status options for Cell Checks are configured in the BarcodeScanner web application by the Administrator.

Procedure:

1. Navigate to: https://***<servername>***:4444/BarcodeScanner
2. Select the **Properties** button.
3. In the **Cell Check Activities List** field, enter the inmate status values to be available when performing cell checks, each status on its own line.

   Example statuses:

   - Resting
   - Sleeping
   - Exercising
   - Other
4. Select the **Update** button to save your changes.

   The next time the user logs into the Jail application on the scanner, the new cell check status codes are available.

Chapter 17

Release 2021.1

This chapter presents changes made to Flex for the 2021.1 release.

17.1 CAD

CAD was enhanced in the following ways:

- Deleting Comments and Erasing Comment History on page 334
- Understanding Updates to the Emergency Call Works Integration on page 335
- Admin: Using ProQA Determinant Codes on page 336

17.1.1 Deleting Comments and Erasing Comment History

Flex CAD was enhanced so that you can delete comments and erase the history of comments. This feature only works with the CAD Incident screen and the Comments window. The CAD Incident record associated with the comments must be saved before you can delete comments or erase comment history.

Your admin can give you permission to erase comment history, to erase comment history and delete the comment completely, or to do neither. The ability to delete comments and to erase comment history exists so that you can follow any applicable laws in your jurisdiction about expunging information. Do not casually delete or erase comments.

When you delete a comment, Mobile CAD notifies users. If someone attempted to update the deleted comment from Mobile CAD, the changes are ignored.

17.1.1.1 To delete a comment:

Procedure:

1. In the **Comments** tab on the **CAD Incident** screen or the **Comments** window, rest your mouse pointer over the comment to delete.

   The **Delete** button appears.

2. Click **Delete**.

   A prompt opens, asking you to confirm the delete action.

3. Click **Delete** to delete the comment and erase its history.

17.1.1.2

To erase the history of a comment:

Procedure:

1. In the **Comments** tab on the **CAD Incident** screen or the **Comments** window, rest your mouse pointer over the comment to erase.

   The **Erase History** button appears.

2. Click **Erase History**.

   A prompt opens, asking you to confirm the erase history action.

3. Click **Erase History** to erase the comment history.

17.1.1.3

Admin: Setting Up Deleting and Erasing Comments

To allow specific users to delete comments and erase comment history, you must set the `DeleteFlexComments` setting, located in the **Module.CAD.Calltaking** setting folder.

You can configure this setting at an agency, group, or user level. Depending on what you want to allow, you can configure the setting with any of the following values:

- `Erase`: Allows the user to erase the history of comments, while keeping the most recent version of the comment.
- `Delete & Erase`: Allows the user to erase comment history, and to completely delete the comment.
- `No`: Does not allow the user to delete or erase comments. This value is selected by default.

The ability to delete comments and to erase comment history exists so that your users can follow any applicable laws about expunging information. Remind your users that they should not casually delete or erase comments.

17.1.2

Understanding Updates to the Emergency Call Works Integration

The DL command, which works with the Emergency Call Works integration, was enhanced in the following ways:

- Once the phone number is dialed, a confirmation message appears under the command line.
- When you use the DL command, the software ignores the following characters:
  - opening and closing parentheses ( )
  - spaces
  - hyphens -
- Additional parameters were added to specify whether you are entering a unit to call or a phone number. The format of the DL command is:

  `dl [u|p] [unit#|phone#]`

  where `unit#` is the unit number and `phone#` is the phone number. For example to call unit L12, enter `dl u l12`. To call the phone number 555-1234, enter `dl p 5551234`.

17.1.3
Admin: Using ProQA Determinant Codes

CAD was enhanced with a change to the ProQA interface and the valid ID range. If your agency uses the ProQA interface, when you enter determinant codes in the Determinant Code table (`tbpdterm`), the recommended format for the **Determ ID** field value is `A0000` where A is a capitalized letter, and `0` is a digit. For example, `B3452`. The recommended range of values is `A0000-Z9999`. You can use the determinant code as a record's ID when the length is not more than 5.

17.2
Hub

Hub was updated with the following changes:

- Admin: Enhancement of the Flex Server Diagnostic Tool on page 336
- Admin: Limiting the Number of Records on the Customizable List on page 343
- Evidence Management: Flex Evidence Mobile Application on Datalogic Memor 10 Scanner Device with Android OS on page 344

17.2.1
Admin: Enhancement of the Flex Server Diagnostic Tool

The enhanced Flex Server Diagnostic Tool extends the range of diagnostic and maintenance functions that help to prevent and solve potential server issues. The new features are available under the **SYSTEM CHECK** tab.

17.2.1.1
Using SYSTEM CHECK Tab

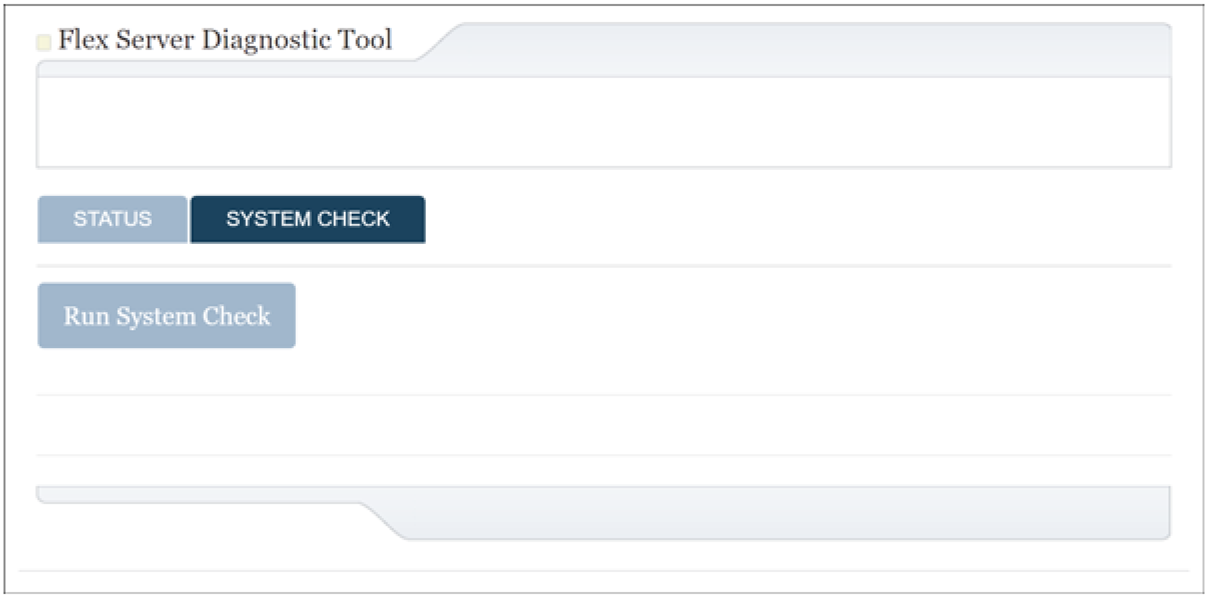
Use the **SYSTEM CHECK** tab to get information on the system components and processes, including issues that might need your attention or intervention. The screen has two main areas, **Info Checks**, for informative and optimization purposes, and **Health Checks**, for system health monitoring and maintenance.

Procedure:

1. Open the Flex Server Diagnostic Tool. For more information, see the *Flex Administrator Manual*.
2. Select the **SYSTEM CHECK** tab.

   The SYSTEM CHECK start screen opens.

Figure 353: SYSTEM CHECK Start Screen



3. On the SYSTEM CHECK start screen, click **Run System Check**.
4. Wait until `System Check Complete!` message appears.

Figure 354: Upper Part of the SYSTEM CHECK Screen

Once the system check is completed, a message appears, stating that the system check is complete and displaying the date and time the check was run. The header also contains information about the operating system, Flex version, time zone, and uptime.

17.2.1.1.1
Using Info Checks

The items in the **Info Checks** area are mainly for information purposes. The green color of an item in the list means that the featured element is in normal/optimum state. The red color indicates that you can optimize the system by performing actions concerning this element. However, the optimization of the element is not critical for system operation. After expanding the item, read the information highlighted by a pink background. Based on your knowledge about the system, you can decide whether to take some actions.

Procedure:

To use the Info Checks feature, do one of the following:

- If an item is in red color, open its **Description** by clicking the relevant chevron.

  Read the point or points highlighted by a pink background and decide about actions to take.

  If the description directs you to contact Technical Services, decide whether to contact them.

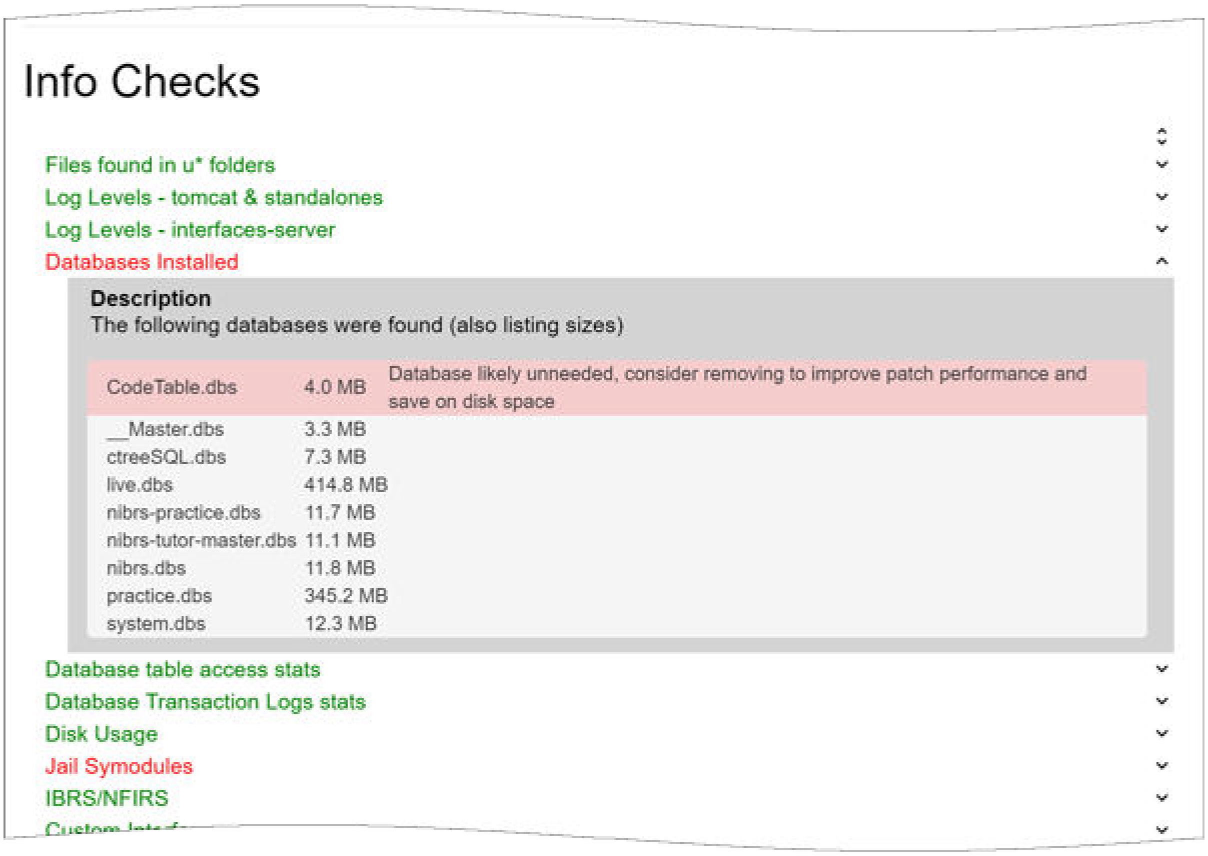
  If you or Technical Services successfully complete actions that address all the causes of the highlighted points, after the restart of the system check, the item appears in green color. Otherwise, the item remains in red color.

- If an item is in green color and you want to know more about it, open its description by clicking the relevant chevron.

  Details about the item appear. No action is needed.

You can also expand/collapse descriptions of all items at once by clicking the pair of chevrons at the top of the **Info Checks** list. You may collapse each description individually by clicking the relevant up chevron. By clicking **Download Report** at the bottom of the screen, you can access all descriptions both from the **Info Checks** and **Health Checks** areas, in the form of a PDF file.

Figure 355: Part of the Info Checks List with an Item Description Open



17.2.1.1.2
Understanding Health Checks

The items in the **Health Checks** area are vital for the system operation. The green color of an item in the list means that the featured element is in normal state. The red color indicates that you must take an action to fix the issue that poses a risk of system malfunction or failure.

An item in red color belongs either to the administrator-repairable or non-administrator-repairable category. You can distinguish the repairable items by check boxes on the left side of them. The related issues are not fixed automatically so that you can take into account the specifics of the system used by your agency. After you expand an admin-reparable item, the description contains details and the recommended solution (**Fix**). Use the **Fix** consciously. If in doubt, contact Technical Services for help, which you must always do in the case of any non-admin-repairable items.

Figure 356: Lower Part of the SYSTEM CHECK Screen – Health Checks

17.2.1.1.3
Using Health Checks

Procedure:

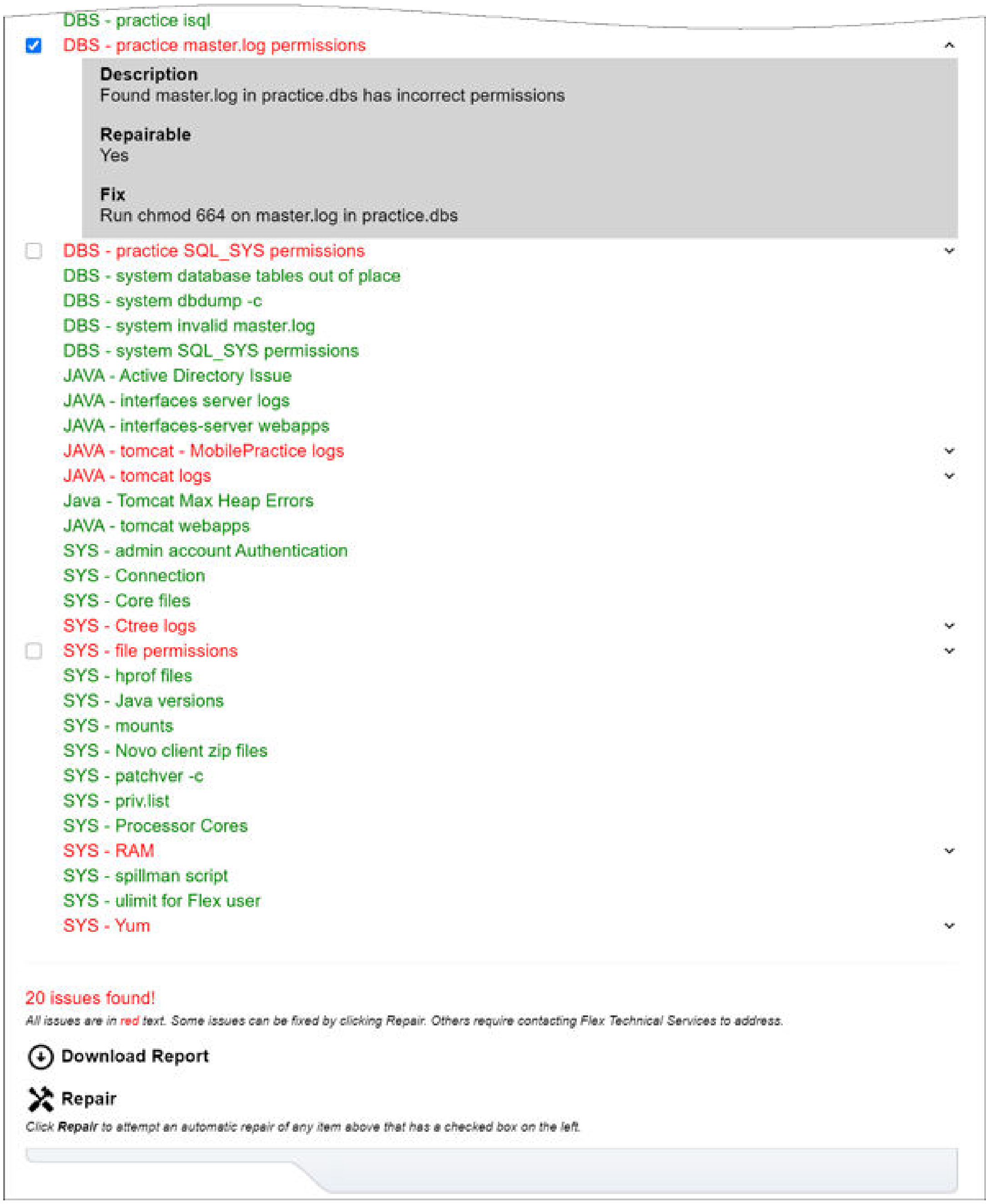
- If an item in red color is preceded by a check box, open its description by clicking the relevant chevron.
  1. Read the description to be aware of actions initiated by the recommended **Fix**.
  2. To set the **Fix**, select the check box on the left side of the item.
  3. To apply the **Fix**, at the bottom of the screen, click **Repair**.

  The SYSTEM CHECK screen reloads. If the **Fix** is successfully applied, the item appears in green color.

  NOTE: By selecting the check box at the top of the **Health Checks** list, you can attempt to fix all repairable items at once. However, Motorola recommends that you read all descriptions beforehand.
- If an item in red color is not preceded by a check box, open its description by clicking the relevant chevron.
  1. Read the description and contact Technical Services for help.

  You can also expand/collapse descriptions of all items at once by clicking the pair of chevrons at the top of the **Health Checks** list. You may collapse each description individually by clicking the relevant up chevron. By clicking **Download Report** at the bottom of the screen, you can access all descriptions both from the **Info Checks** and **Health Checks** areas, in the form of a PDF file.

Figure 357: Health Check List with a Repairable Item Selected for Repair



17.2.2

Admin: Limiting the Number of Records on the Customizable List

The **System.Client.CustomizableListMaxRecordsToLoad** setting on the Settings Editor screen of the Administrator Manager (**adminutil**) determines the maximum amount of records that can be loaded into memory at once. Setting a limit helps agencies with large amounts of records (over 100,000) to prevent memory issues and possible system crash. The default value of this setting is 100000. When the limit is reached, the following message appears.

Figure 358: Message about Reaching the Limit

If your agency needs a lower limit, enter a lower value in the setting. If your agency needs more records loaded into the customizable list at once, ensure that your clients can handle a higher volume, and then enter a higher value in the setting.

17.2.3

Evidence Management: Flex Evidence Mobile Application on Datalogic Memor 10 Scanner Device with Android OS

The Datalogic Memor 10 scanner device running Android OS replaces the Datalogic Memor X3 model based on Windows OS. By using the Flex Evidence mobile application installed on the Memor 10 scanner, you can perform evidence audit and movement. A touch screen, popular mobile OS with intuitive user interface, and data transfer over Wi-Fi, help you to perform the audit procedures more quickly and easily.

NOTE: For information about how to configure and operate the Datalogic Memor 10 scanner, see its Quick Start Guide and User's Manual.

17.2.3.1

Using the Flex Evidence Mobile Application

Use the Flex Evidence mobile application to audit and move inventory and then transfer inventory data to the Evidence Management screen. For more detailed information on using the Flex Evidence application, see the *Flex Evidence Manual*.

Prerequisites:

- Your agency purchased the Evidence Audit module with the Datalogic Memor 10 scanner.
- Motorola Solutions installed the necessary software on your agency server.
- The Flex Evidence application is installed on the scanner by downloading the latest APK file.
- Users have the Flex client login credentials needed to log on to the Flex Evidence application.

17.2.3.1.1

Starting the Flex Evidence Application

Procedure:

1. On a Home screen of the Datalogic Memor 10 scanner, locate the Flex Evidence application and open it by tapping its icon.

Figure 359: The Flex Evidence Scanner Application Icon

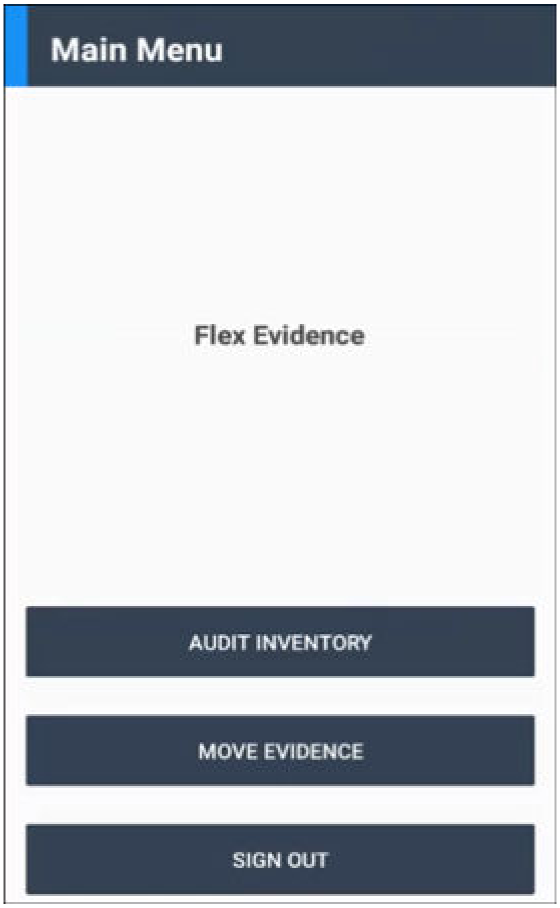
2. On the login screen, log on to the Flex Evidence Scanner application by entering your Flex **Username** and **Password**.

Figure 360: Flex Evidence Scanner Login Screen

3. Confirm your credentials and tap **SIGN ON**.

   The **Main Menu** screen appears.

Figure 361: Flex Evidence Scanner Main Menu Screen

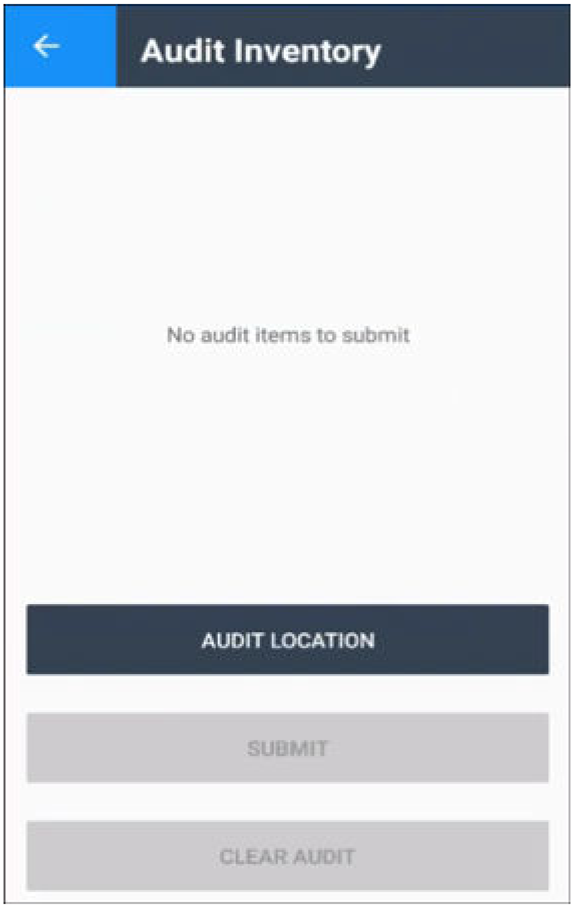


17.2.3.1.2
Using the Audit Inventory Screen

Use the Audit Inventory screen to scan barcodes of evidence items to confirm the accuracy of current evidence records.

To access the Audit Inventory screen, from the Main Menu screen, tap **AUDIT INVENTORY**.

Figure 362: Audit Inventory Screen



17.2.3.1.2.1

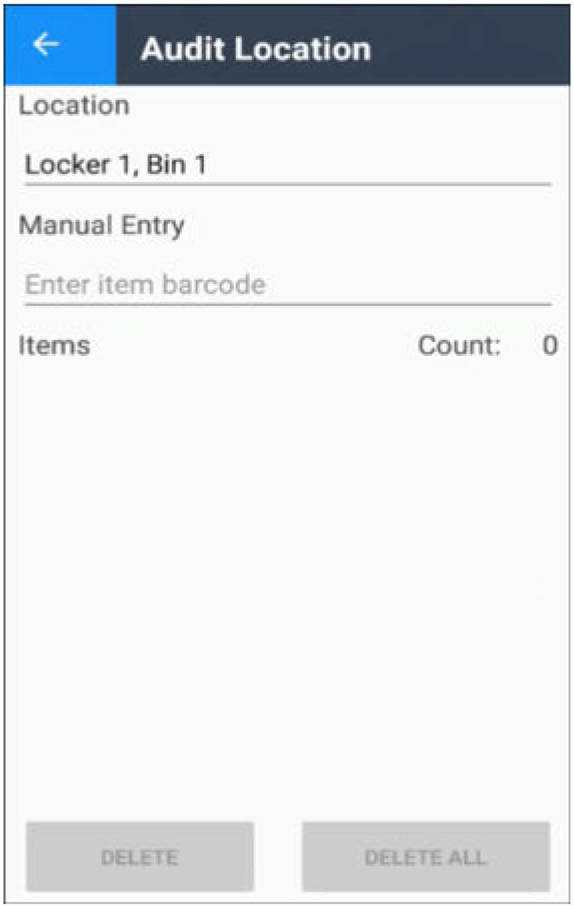
To scan barcodes of evidence items:

Procedure:

1. For a required location, from the Audit Inventory screen, scan the barcode of the location.

   A similar screen appears.

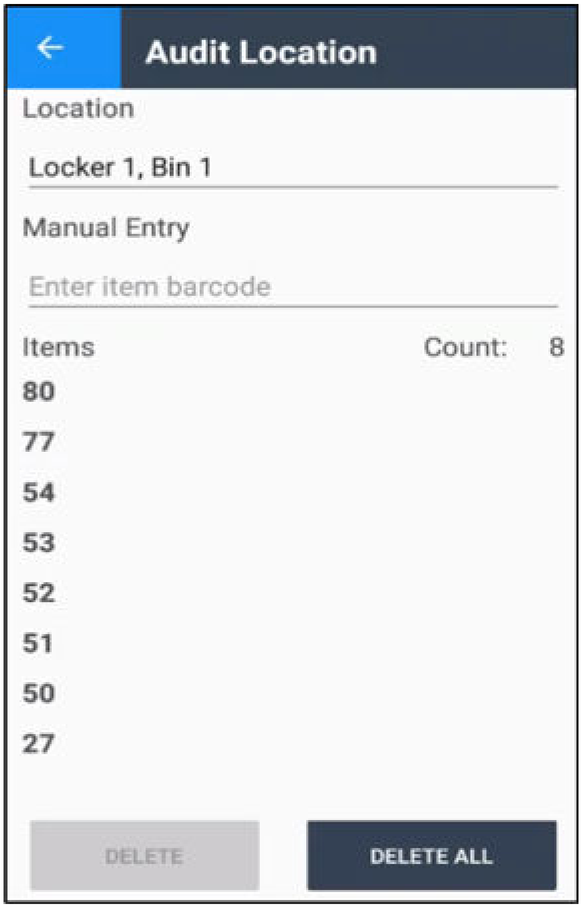
Figure 363: Audit Location Screen



2. Scan items barcodes in this location.

   NOTE: If you need to enter a barcode manually, tap the **Manual Entry** field and enter the barcode.

Figure 364: Example of Scanning Results in a Location

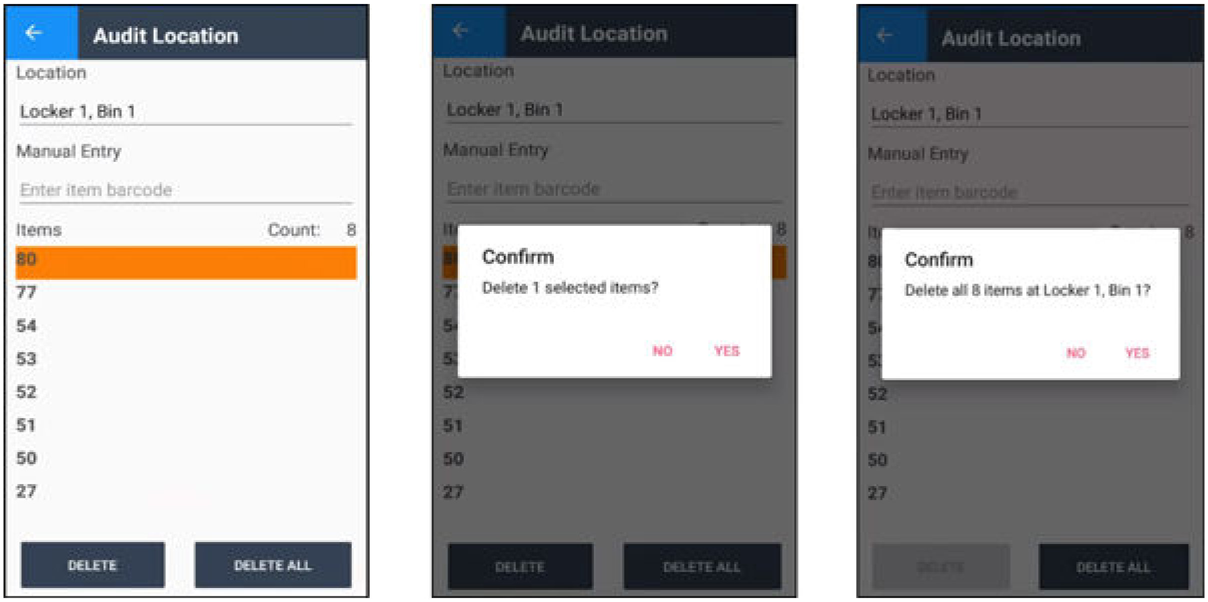


3. When you finished scanning all of the items, from the Audit Location screen you can delete some or all items that were scanned wrongly.

   By deleting an item, you remove it from the audit submission on the Audit Inventory screen.

   - If you want to delete all items at once:
     a. Tap **DELETE ALL**.
     b. In the Confirm box, confirm the deletion by tapping **YES**, or cancel this action by tapping **NO**.
   - If you want to delete one or some of the items, delete each item separately:
     a. Tap an item you want to delete, and then tap **DELETE**.
     b. In the Confirm box, confirm the deletion by tapping **YES**, or abort this action by tapping **NO**.
     c. Repeat steps a – b for each item you want to delete.

Figure 365: Selecting a Single Item or All Items for Deletion in a Location



4. If you need to scan barcodes in other locations, for each location repeat steps 1 – 3, until you complete scanning inventory in all the required locations.

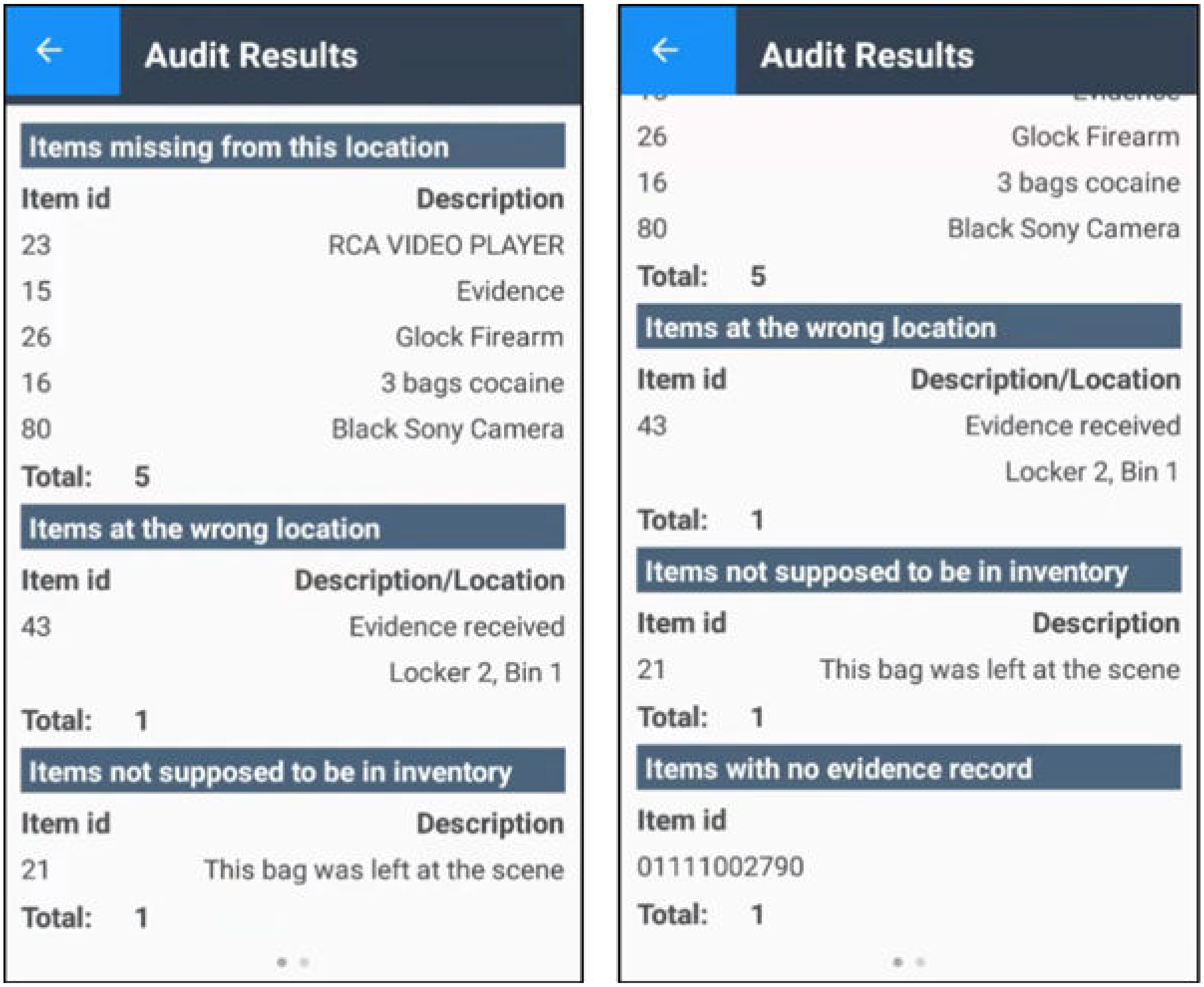
17.2.3.1.2.2 To review the audit results:

Procedure:

1. After you completed scanning inventory in all the required locations, from the Audit Inventory screen, tap the back button on the top right corner to return to the Audit Inventory screen.
2. On the Audit Inventory screen, tap **SUBMIT**.

   The Audit Results screen appears. With more than one audit location, the darker dot at the bottom of the screen indicates the displayed screen from among all the scanned locations.

Figure 366: Examples of Audit Results with Various Errors



3. With multiple locations, to view audit results from a required location, select that location by swiping the screen left/right.
4. Fix possible errors that are shown in the Audit Results.

   For example, in the case of items at a wrong location, or missing from a location, you can use this procedure: Using the Move Evidence Screen on page 352.
5. When you finished audit transactions and submitted the data, clear all the data by tapping **CLEAR AUDIT**.
   - If you want to confirm the clearance of the data, in the Clear Audit Data confirmation box, tap **YES**.
   - If you decide to withdraw from this action, in the Clear Audit Data confirmation box, tap **NO**.

   NOTE: If you do not clear the data, the next user logged into the application will see your transactions.

17.2.3.1.3
Using the Move Evidence Screen

Use the Move Evidence screen to move evidence between locations. To access the Move Evidence screen, from the Main Menu screen, tap **MOVE EVIDENCE**.

Procedure:

1. From the Move Evidence screen, tap **MOVEMENT**.
2. Scan the barcode of the location where the items are currently stored.

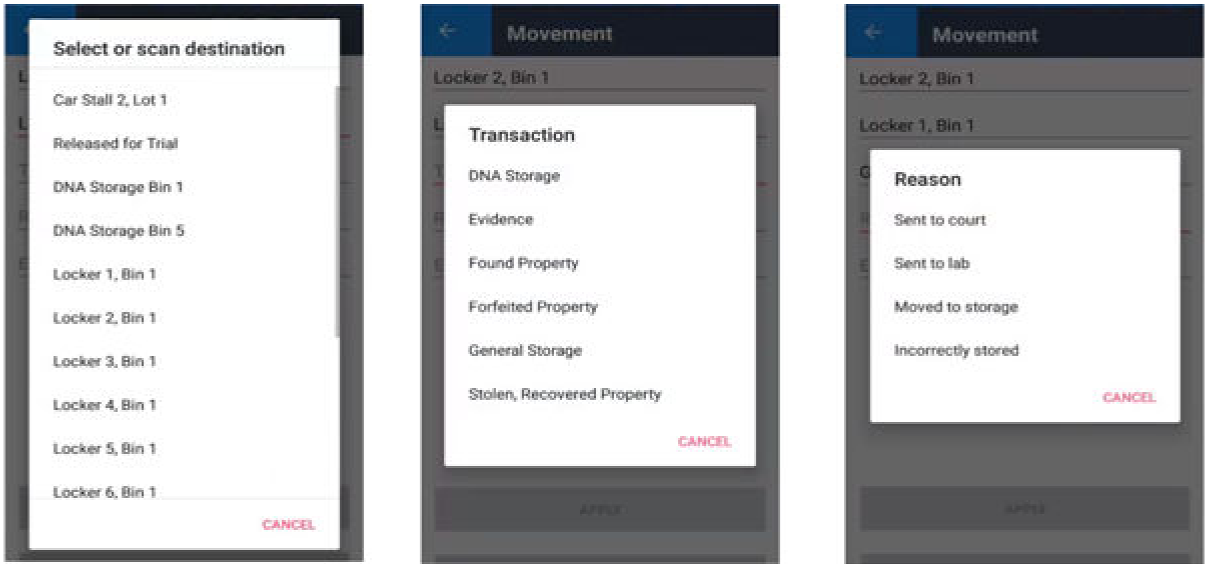
   The Movement screen displays the current location.

   Figure 367: A Movement Screen of the Current Location

3. Scan the barcode of the destination, or tap the **Select or scan destination** field and select the destination manually.
4. Tap the Transaction field, and from the displayed list select a transaction value.
5. Tap the Reason field, and from the displayed list select a movement reason.

Figure 368: Examples of the Destination, Transaction, and Reason Boxes

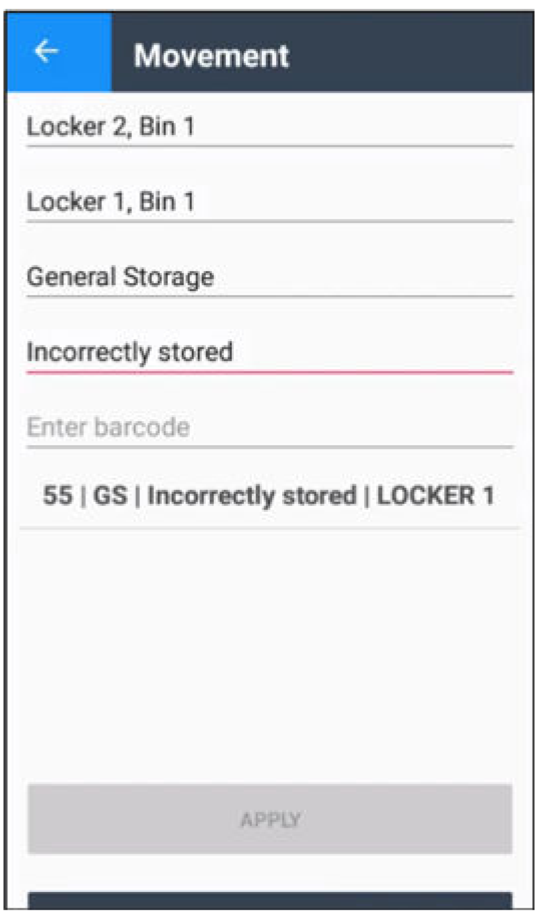


NOTE: The lists in the Transaction and Reason boxes are configurable by your administrator.

6. Scan all the items in the current location that you want to move to the same destination.

   If you need to enter a barcode manually, tap the Enter barcode field and enter the barcode manually.

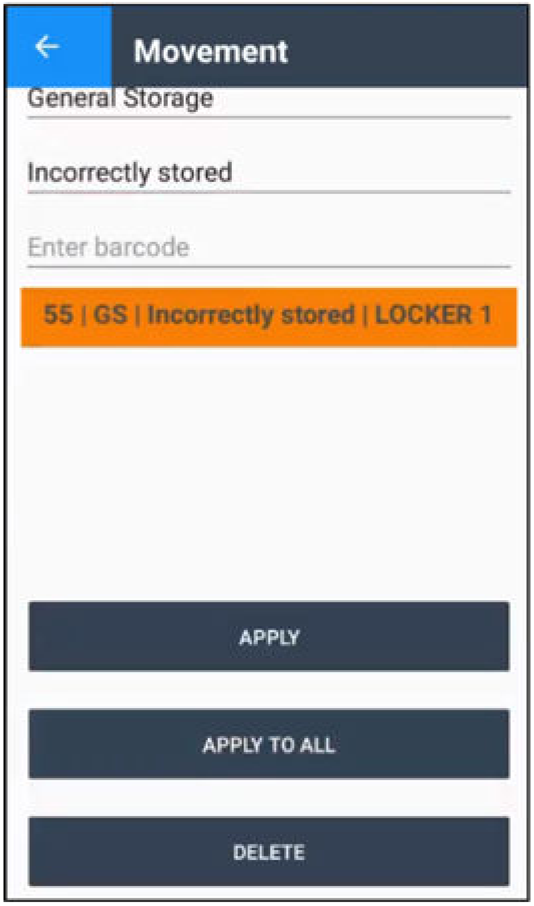
   Figure 369: Example of a Movement Screen with a Single Item and the Reason Selected



7. Perform one of the following actions:
   - To prepare for the movement submission of all the items, tap **APPLY ALL**.
   - To prepare for the movement submission of an individual item, select that item and tap **APPLY**.

   In the following figure, there is only one item to be moved.

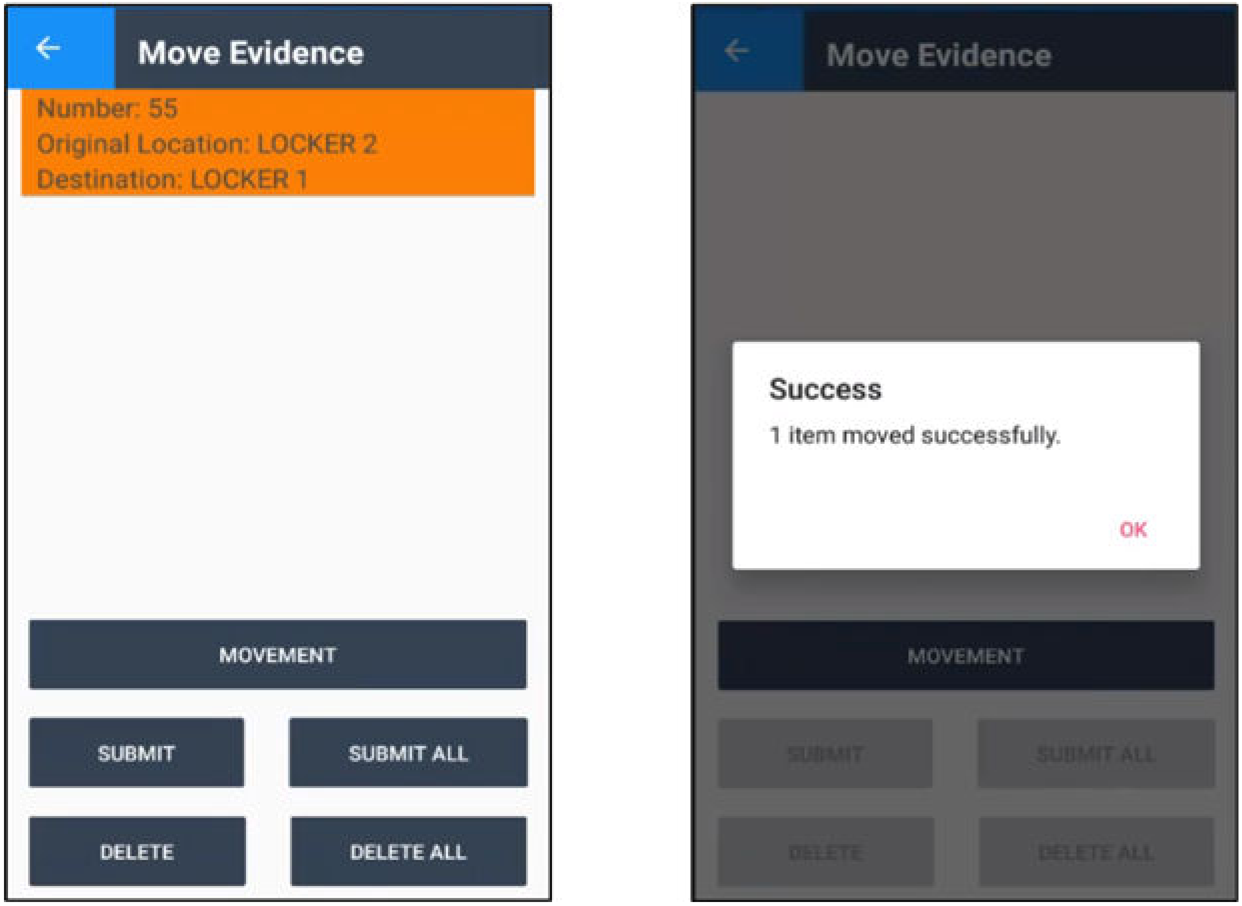
   Figure 370: The Item to be Moved



   Once the action is applied, the Move Evidence screen appears.
8. On the Move Evidence screen, perform one of the following actions:
   - If you want to move all items at once, tap **SUBMIT ALL**.
   - If you want to move a selected item, tap **SUBMIT**.

   A successful movement transaction is confirmed by a Success message. When multiple items are submitted for movement, the items without an error are moved, and the remaining items with errors are left on the screen with specific error messages.

Figure 371: Example of a Successful Movement Submission



17.3
Mapping

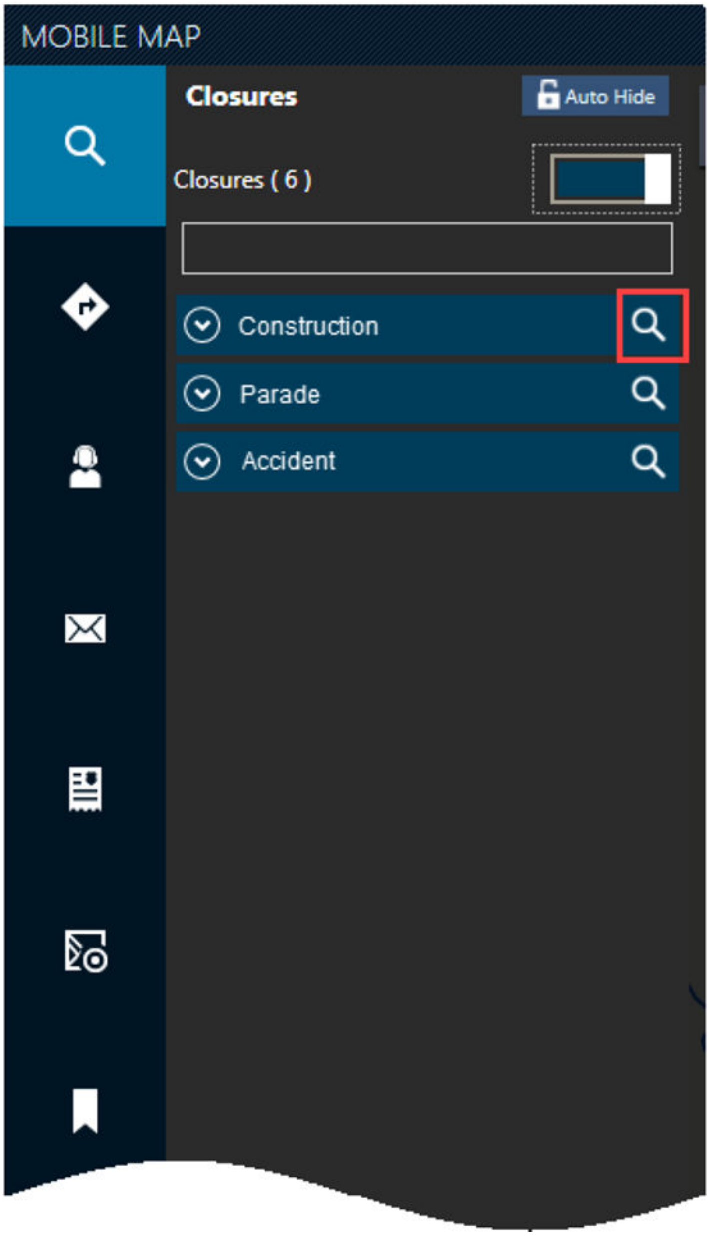
Flex Mapping was enhanced in the following ways:

- Viewing All Barriers For a Closure on page 355
- Admin: Configuring the Refresh Interval for the Map on page 356

17.3.1
Viewing All Barriers For a Closure

The map was enhance with the **Zoom to Closure** button. Click the button to view all barriers associated with a closure on the map.

Figure 372: Zoom to Closure Button



17.3.2
Admin: Configuring the Refresh Interval for the Map

The Map Configuration page was enhanced with the ability to configure the refresh interval for services that support automatic refreshing. When you add or edit the Feature, ArcGIS Dynamic, or ArcGIS Tiled services, you can use the **Refresh Interval In Seconds** field to indicate how often the service refreshes.

Chapter 18

Release 2020.4

This chapter presents changes made to Flex for the 2020.4 release.

18.1 CAD

CAD was enhanced in the following ways:

- Using CAD Paging with the Rapid Notification 2.0 Interface on page 357
- Understanding Updates to the Traffic Stop Screen on page 358
- Understanding Updates to the ECW Integration on page 358
- Understanding Response Plans on the CAD Incident Screen on page 358

18.1.1 Using CAD Paging with the Rapid Notification 2.0 Interface

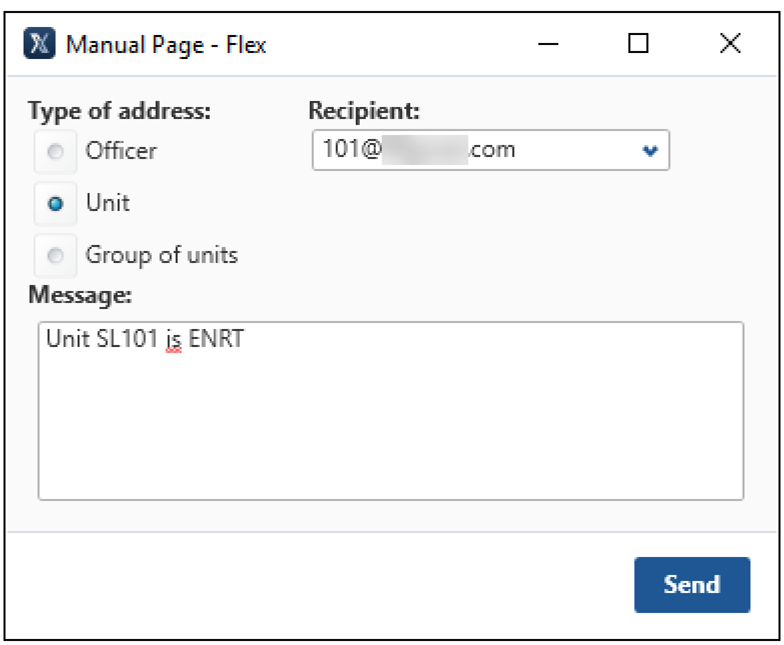
If your agency uses the Rapid Notification 2.0 interface as a paging solution, then when you page someone in CAD, be aware of the following changes:

- You can use the updated Manual Page screen to send pages.

  To send a page with the Manual Page screen:

  1. Open the Manual Page screen by entering `page` at the command line.

     Figure 373: Manual Page Screen

  2. Select the type of recipients for the page (an officer, a unit, or a group of units).

3. From the list, select the specific recipient for the page.
4. Enter the message.
5. Click **Accept** or press Ctrl+Enter or F3 to send the page.

- When you use the PAGE command to send pages, if you use the pipe symbol (|) in the message, all text after the pipe symbol is not added to the message. Remember that when the usage line under the command line shows the format of a command, the pipe symbol indicates that you can pick one of the listed options. The format for the PAGE command is:

  `page {-n {name} | -u {unit} | -g {group}} {message}`

  where `name` is the name of the officer, `unit` is the unit number, `group` is the group name, and `message` is the message. For example, to page unit 101 with the message “Unit SL102 is ENRT,” enter `page -u 101 Unit SL102 is ENRT`.

18.1.1.1
Admin: Setting Up CAD Paging with the Rapid Notification 2.0 Interface

If your agency wants to use CAD Paging with the Rapid Notification 2.0 interface, then you must set the `UseRapidNotification2ForManualPaging` setting, which is located in the **Module.CAD** setting folder, to `Yes`. If you do not want to use the interface for CAD Paging, configure the setting with the value `No`. For more information on configuring settings, see the *Flex CAD Administrator Manual*.

18.1.2
Understanding Updates to the Traffic Stop Screen

If your agency collects vehicle information on the Traffic Stop screen, then be aware that the order of the fields changed. The order of the fields is now **Plate**, **State**, **Color**, Make instead of color, make, plate, state. This change helps the Traffic Stop screen match the TS command and puts the important information first. These fields only appear if your admin has configured CAD to show them. For more information, see the *CAD User Manual*.

18.1.3
Understanding Updates to the ECW Integration

Normally, when you finish entering an address in the **Address** field and move to a different field or click a button, the Address Validation window opens. However, for the Emergency CallWorks integration, if you click a call control (such as **Hold** or **Mute**), even if you were typing in the **Address** field immediately before, then the Address Validation window does not open.

18.1.4
Understanding Response Plans on the CAD Incident Screen

Be aware of the following clarifications about using response plans and recommended units on the CAD Incident screen:

- Currently, in the **Dispatch Units** area, the units that are required by the response plan appear in the header (in the **Reqs** field). The actual units that the system recommends appear underneath, in the **Dispatch** field. Sometimes, if the required unit is not available, but a covering unit is defined and the covering unit is available, the system selects that unit. As a result, the list of required units might be different from the list of recommended units. When you make dispatch decisions, rely on the recommended units in the **Dispatch** field, as those are the units that are dispatched when you click **Accept**.

- **Admin**: If your agency is using response plans with the CAD Incident screen, and dispatchers are never seeing any recommended units, check the sort parameter for the target discipline. The parameters to check are `firesort emssort`, and `lawsort`. Look for the value `STS` (sort by status). If your agency is using that value, and the Recommended Units Status Order table (`cdrustat`) — which contains hierarchies of unit statuses that indicate units are available for recommendations from the most to least available—has no values, then that is the reason dispatchers are not seeing recommended units. To fix the issue, do one of the following:
  - If your agency is not using recommended units (only response plans), then you can remove the `STS` value from the sort parameters.
  - If your agency is using both recommended units and response plans, and your agency wants to use `STS` as a sorting value, then you must define a sequence of statuses in `cdrustat` for response plans or recommended units to function. For more information, see the *CAD Administrator Manual*.

18.2
Hub

Hub was updated with the following changes:

- Admin: Addition of Certificate Manager on page 359

18.2.1
Admin: Addition of Certificate Manager

Flex was enhanced with Certificate Manager feature to allow agencies for convenient management of security certificates.

When you or someone from the Admin group first logs in after the patch, a prompt might open, stating that the certificate your agency is using is not unique and a new certificate needs to be generated. The message provides you with the server address to the Certificate Manager feature.

You can use the Certificate Manager feature any time when you need to audit, add, create, validate, implement, or update security certificates, as well as configure automatic email alerts about upcoming expiration dates to required recipients.

To manage certificates properly, you must know general rules concerning security certificates in public key infrastructure (PKI) systems, and be aware of the importance of installing trusted CA certificates obtained from a Certificate Authority (CA).

18.2.1.1
Opening the Certificate Manager Interface

Procedure:

In a browser, enter the following URL:

`https://localhost:4080/Spillman/CertificateManager.html`

where localhost is the name of your server.

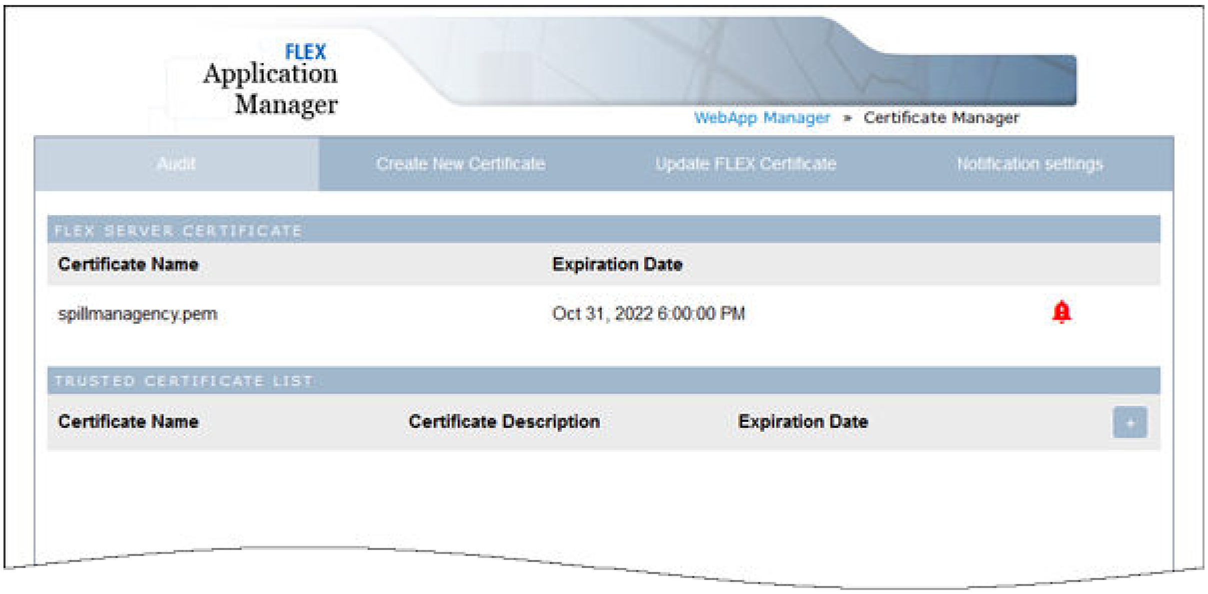
The Certificate Manager page opens.

18.2.1.1.1
Using the Audit Screen

Use the Audit screen to view and audit the certificate currently used by the Flex server, as well as upload and add a range of certificates, for example, those previously generated with a CA. When you add the certificates to the TRUSTED CERTIFICATE LIST, you can give them names and use the certificates in the future for applications within the Flex suite. This centralized repository of security certificates enables you to easily manage all the certificates.

To open the Audit screen, click the **Audit** tab in the Certificate Manager interface.

Figure 374: Flex Application Manager Audit Screen



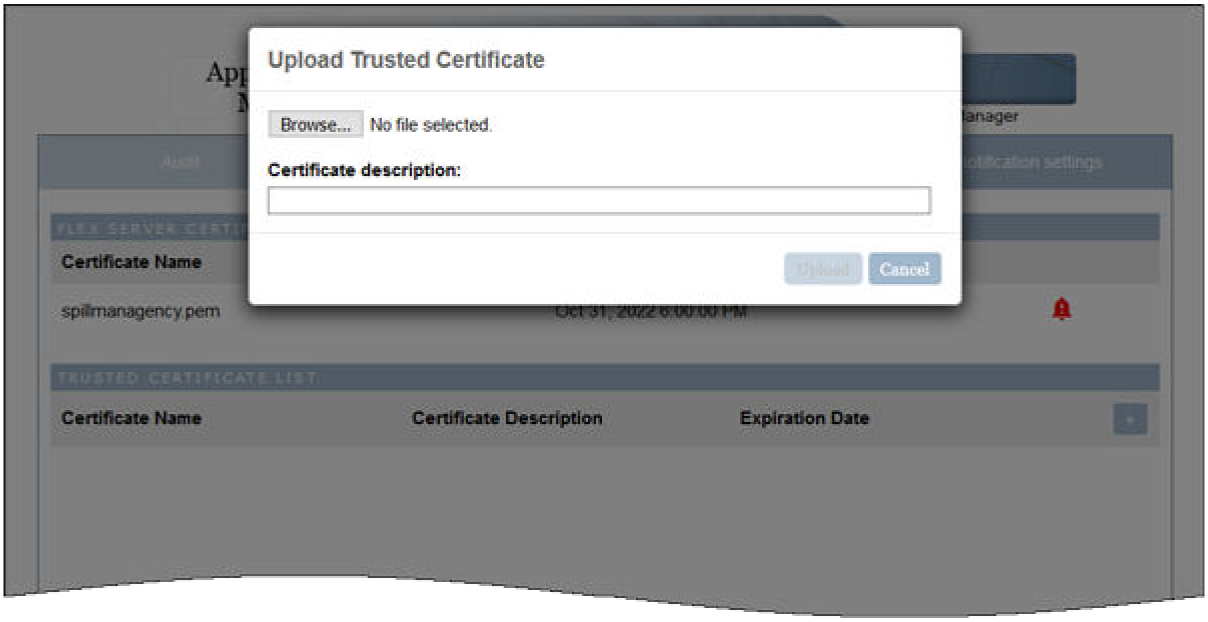
When you first open the Audit screen, the *spillmanagency.pem* certificate might appear in the FLEX SERVER CERTIFICATE pane. This certificate is only a placeholder that must be replaced by a proper certificate. As being not unique, the placeholder certificate does not comply with CJIS policies, which is indicated by the warning bell icon.

NOTE: When you see any alert in the Audit screen, rest the mouse pointer on the alert icon to view a ToolTip that explains the alert. For example, `This certificate is not unique`. Other warnings appear if the current date is close to or exceeds the expiration date of the certificate.

18.2.1.1.1.1
Adding a Trusted Certificate

If your agency has a valid certificate previously generated with a CA, which you want to use within the Flex suite, you must add it to the Trusted Certificate List.

Figure 375: Upload Trusted Certificate Window



Procedure:

1. In the TRUSTED CERTIFICATE LIST pane, click the plus button.

   The Upload Trusted Certificate window opens.
2. In the Upload Trusted Certificate window, click **Browse**.
3. Select the appropriate file on your machine.
4. In the Certificate description field, add a meaningful description.
5. Click **Upload**.
6. If your agency has several certificates that can be used for Flex applications, repeat steps 1–4.
7. If you want to remove a certificate from the list, click the minus button at the end of the certificate line.

18.2.1.1.2

Using the Create New Certificate Screen

Use the Create New Certificate screen if you need to generate a new trusted certificate. To open the screen, click the **Create New Certificate** tab on the Certificate Manager screen.

Figure 376: Create New Certificate Screen

Procedure:

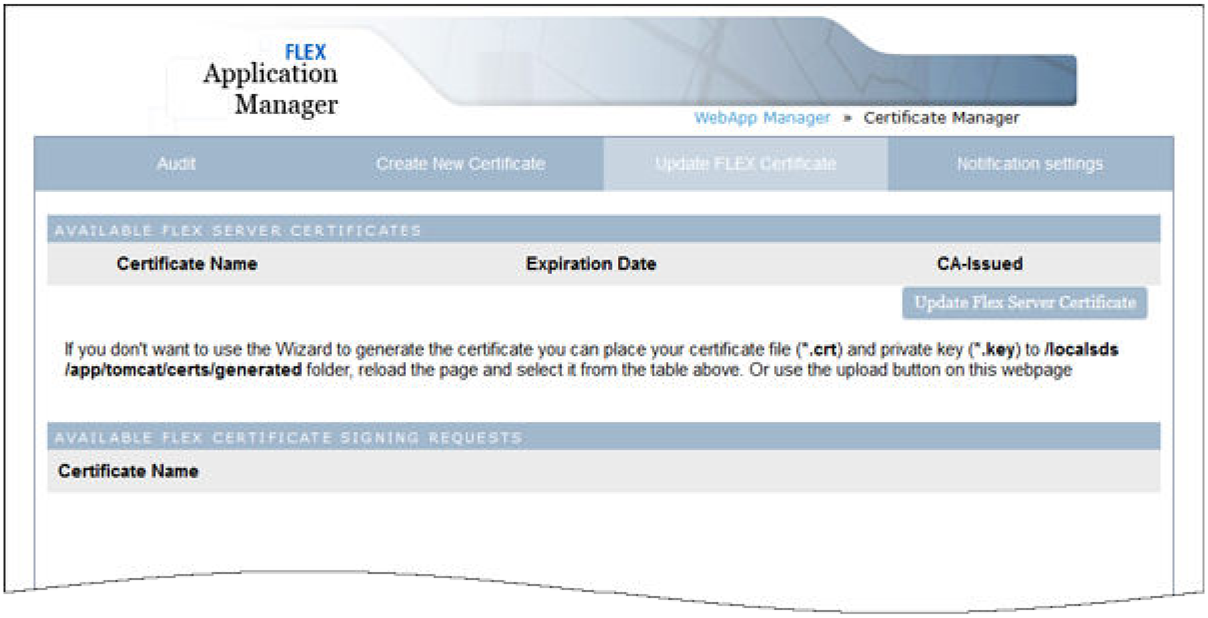
1. Fill in all obligatory fields (marked with red asterisks) with information unique for your agency.
2. Optional: Add the required validity period of the certificate.
3. Optional: Add Subject Alternative Names (for example: DNS, IP address, additional email address) by performing the following actions:
   a. In the Subject Alternative Names line, click the chevron and select one of the items.
   b. In the input field, enter information relevant to that item and click plus.
   c. If you want to add another alternative name, repeat steps a – b.
   d. If you want to remove an alternative name, click minus at the end of its line.
4. Click **Generate Certificate Signing Request**.
5. To complete the process of signing your agency's certificate by a Certificate Authority, contact that authority for further proceedings.

   ⚠ **CAUTION:** The use of the **Create Self-Signed Certificate** option, although possible, is not recommended. Motorola Solutions recommends using only signed certificates from certificate authorities to ensure your agency's users cannot be tricked into using a non-genuine certificate. Using a self- signed certificate risks the security of your agency's communications because users are put into a situation where they are adding a certificate to their machine after patching. If users see prompts to add certificates to their machine, they might be more likely to accept a malicious certificate later on because they might not be able to distinguish a genuine certificate from a malicious certificate.

18.2.1.1.3
Using the Update FLEX Certificate Screen

If you want to update the Flex server certificate, you can use the Update FLEX Certificate screen. To open the screen, select the **Update FLEX Certificate** tab in the Certificate Manager interface.

Figure 377: Update FLEX Certificate Screen



The AVAILABLE FLEX SERVER CERTIFICATES and AVAILABLE FLEX CERTIFICATE SIGNING REQUESTS panes are empty because nothing was posted on the server. Without HTTPS connection, the screen also lacks the plus button that is used for adding a certificate. With HTTPS connection, that button is located past the CA-Issued column title.

18.2.1.1.3.1
To upload an existing certificate:

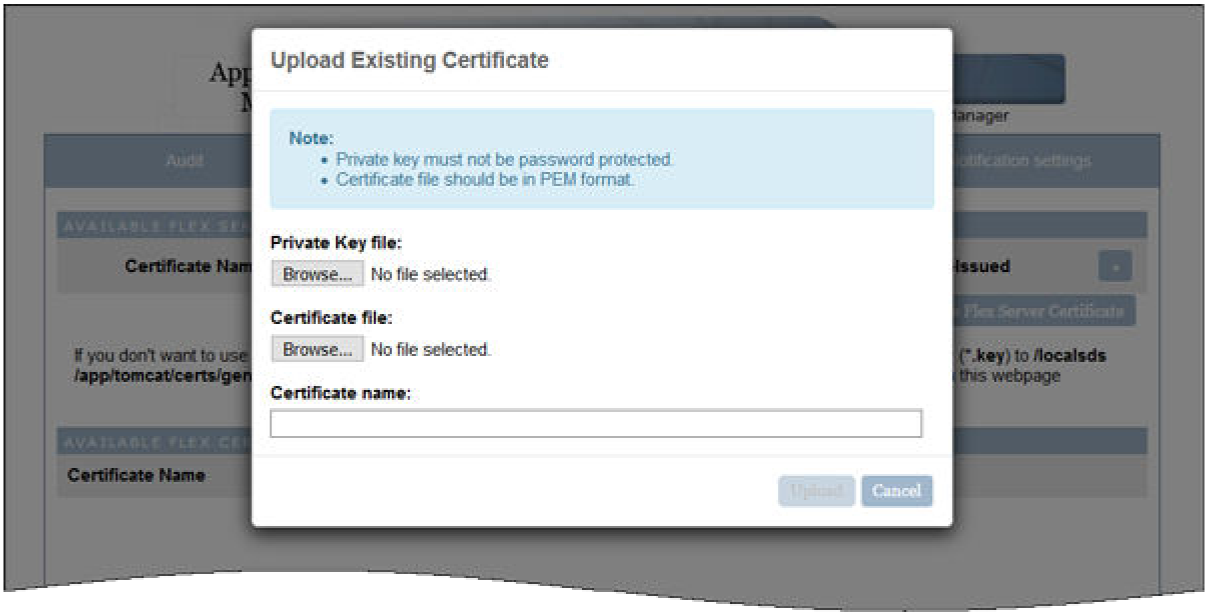
Procedure:

1. Ensure that you are using HTTPS connection.
2. Click the plus button.

   The Upload Existing Certificate window opens (the button clicked is visible in the grayed out area to the right of the window).

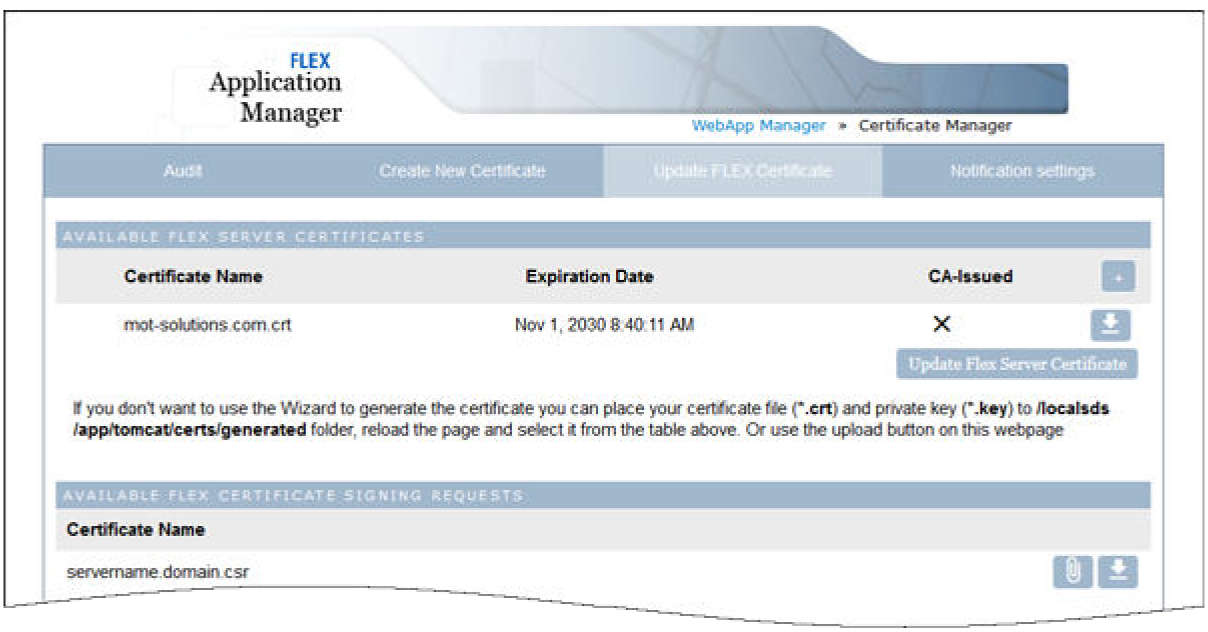
3. In the window, browse for the appropriate Private Key file and Certificate file.
4. In the Certificate name field, enter a meaningful name and click **Upload**.

Figure 378: Upload Existing Certificate Window



If you upload a certificate, you can view it in the AVAILABLE FLEX SERVER CERTIFICATES pane.

Figure 379: Update FLEX Certificate Screen with an Uploaded Certificate

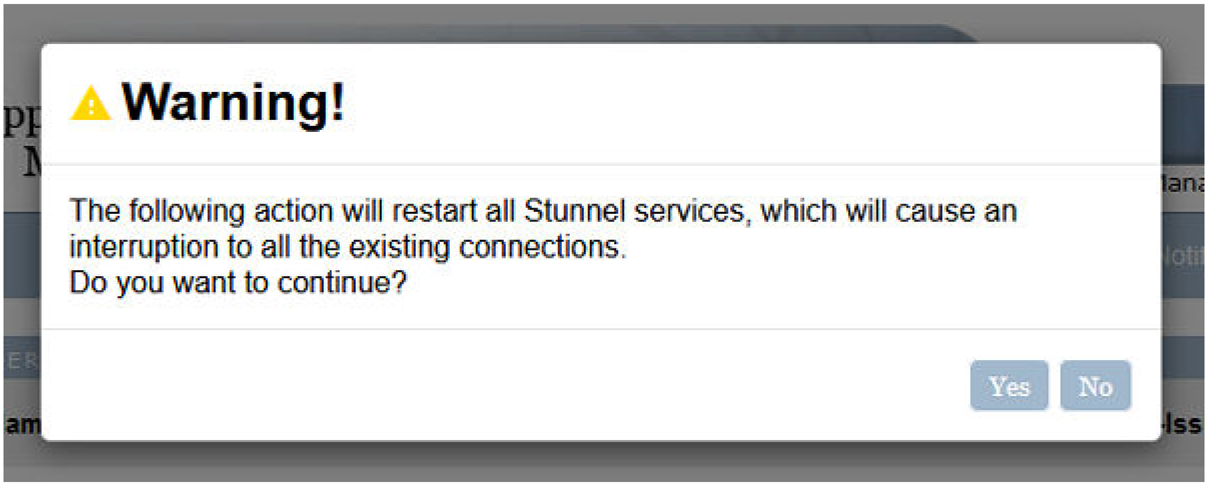


18.2.1.1.3.2 To update the Flex server certificate with an uploaded CJIS compliant FIPS validated certificate:

Procedure:

1. Click **Update Flex Server Certificate**.
2. In a warning pop-up window, decide if you accept an interruption in your agency’s connections, needed for restarting all Stunnel services.

Figure 380: Stunnel Services Restart Warning Window



3. If you can accept the interruption, click **Yes**.
4. Optional: After the restart, you can verify the result of the operation.

   In the Certificate Manager screen, click the **Audit** tab.

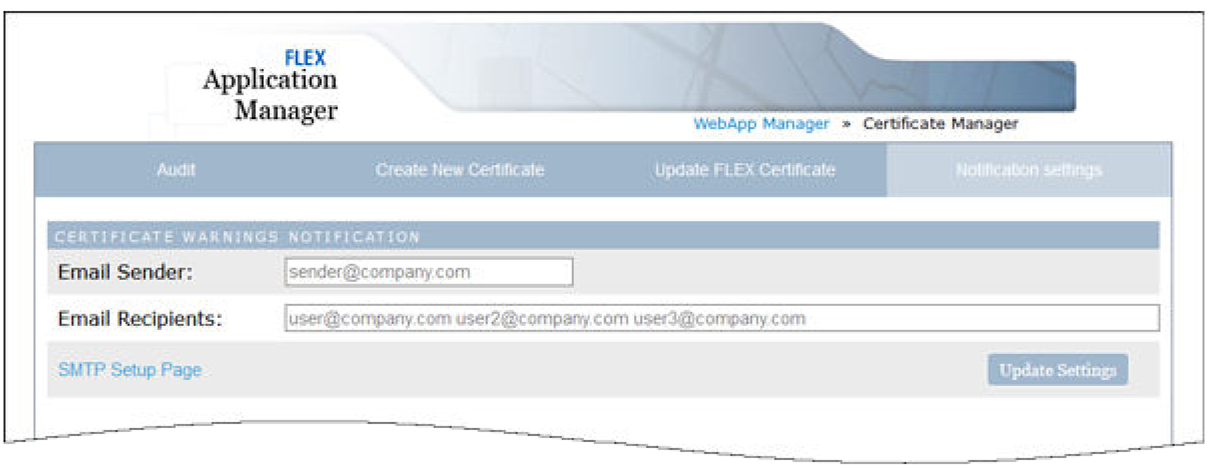
   You should be able to view the new certificate in the FLEX SERVER CERTIFICATE pane.

18.2.1.1.4

Using the Notification Settings Screen

You can select the Notification settings screen for setting up automatic email notifications on upcoming certificates expiration dates. To open the screen, click the **Notification settings** tab.

Figure 381: Notification Settings Screen



Procedure:

1. Using your agency's SMTP service, set up the Email Sender server for sending email notifications.
2. Into the Email Recipients field, enter email addresses of the required recipients, separated by spaces.
3. Click **Update Settings**.

   By configuring this function, you are sure that these recipients will be aware of upcoming expiration dates, even if they do not use the Certificate Manager for a long time.

18.3
Jail

The Jail module was enhanced in the following ways:

- Bond Fees on page 366
- Pay or Stay Sentences on page 366

18.3.1
Bond Fees

Automatically adds a fee to each bond entered for agencies that charge fees per bond. This feature is primarily applicable to Texas agencies. Two new fields have been added:

- on the Bond Screen to capture the fee
- on the Bond Payment screen to capture payment of the fee

18.3.2
Pay or Stay Sentences

This feature adds daily rate and fine amount fields to sentencing adjustments. For each day an offender stays in jail the fine amount is reduced by the daily rate. The following calculation is used: fine amount = daily rate / number of days.

Fine amount and either daily rate or number of days is required. Daily rate or number of days is calculated.

18.4
GeoValidation

The GeoValidation module was enhanced in the following ways:

- Admin: Configuring GeoValidation on page 366

18.4.1
Admin: Configuring GeoValidation

Use the `EnableSuggestions` setting, which is located in the **Module.GeoValidation** setting folder, to allow or prevent suggestions from locators. Set to `True` to allow suggestions. Set to `False` to prevent suggestions. If your agency has many concurrent users, preventing suggestions can help with network traffic. For more information about configuring settings, see the *GeoValidation Manual*.